Risk-e-business: A framework for legal risk management developed through an analysis of selected legal risks in Internet commerce

Katharine Reid

PhD

2000

STATEMENT OF ORIGINAL AUTHORSHIP

I hereby declare that this submission is my own work and to the best of my knowledge it contains no materials previously published or written by another person, nor material which to a substantial extent has been accepted for the award of any other degree or diploma at UNSW or any other educational institution, except where due acknowledgment is made in the thesis. Any contribution made to the research by others, with whom I have worked at UNSW or elsewhere, is explicitly acknowledged in the thesis.

I also declare that the intellectual content of this thesis is the product of my own work, except to the extent that assistance from others in the project's design and conception or in style, presentation and linguistic expression is acknowledged.

(Signed)…….

RISK-E-BUSINESS: A FRAMEWORK FOR LEGAL RISK MANAGEMENT DEVELOPED THROUGH AN ANALYSIS OF SELECTED LEGAL RISKS IN INTERNET COMMERCE

ABSTRACT

The research in this thesis investigates the extent to which risk management can be used in the context of legal risk. In addition, this thesis examines the usefulness of using risk management methodology for this purpose. These issues are analysed using a two step process. The first part of this thesis involves examining risk management methodology and determining whether it can be used in the context of legal risk. The research then turns to developing a framework for *legal* risk management. The second part of this thesis involves evaluating the effectiveness and usefulness of the legal risk management framework developed. This is achieved by applying the legal risk management framework developed in relation to a particular commercial activity, the conduct of Internet commerce. The research demonstrates that risk management methodology can be adapted for use in the context of legal risk. Not surprisingly, the research indicates that risk management methodology is best used when its purpose is to identify, analyse and manage legal risks affecting a specific business in a systematic and consistent way. However, the research suggests that legal risk management may have wider uses, including its use as a technique for identifying areas of true legal uncertainty and areas for which law reform is required. In relation to Internet commerce, the research showed that whilst there are several contractual risks associated with Internet commerce their impact on the conduct of Internet commerce is not as great as has been previously suggested and, moreover, the effect of these risks can often be minimised if certain risk management strategies are implemented. The overall research conclusion in this thesis is that risk management can and should be used in the context of legal risk.

RISK-E-BUSINESS: A FRAMEWORK FOR LEGAL RISK MANAGEMENT DEVELOPED THROUGH AN ANALYSIS OF SELECTED LEGAL RISKS IN INTERNET COMMERCE

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACKNOWLEDGMENTS

I wish to thank my supervisors Professor Graham Greenleaf, Professor Brent Fisse and Associate-Professor Rodger Jamieson for taking on the supervision of a multi-disciplinary thesis and for setting aside the time to provide constructive feedback despite busy and demanding work obligations. I am also grateful to various risk management professionals, lawyers and academics, Mr Rick Davis, Mr Harry Whiteside and Ms Judie Mulholland deserve a particular mention, who generously responded to my out of the blue e-mails seeking information concerning the use of risk management in the context of legal risk especially those who responded to the self-completion questionnaire. I would also like to thank the School of Law staff members, University of Canberra, who provided me with intellectual support, an office, as much part-time employment as I could handle, and moral support throughout my study. Finally, I wish to thank my family for their unwavering support and encouragement. A huge thank you goes to my mother, Dr Helen Reid, who cheerfully and skilfully undertook the Herculean task of proofreading the thesis. Finally, a special thank you goes to my very soon to be husband Curt, who has provided tremendous support and encouragement throughout the course of my research.

CHAPTER 1 INTRODUCTION

1.1 Research issue and methodology

Risk management is a process by which a business systematically identifies, analyses and manages business risk. Whilst it appears from the risk management literature that risk management is used only for specific business operations or classes of business risk, such as disaster risk, or the risks associated with trading derivatives, risk management can be used to identify, analyse and manage the entire range of risks that businesses face. This thesis examines how risk management can be used to identify and manage legal risk.

What constitutes *legal* risk management is presently not clearly defined. Judging from how some legal practitioners use the term "legal risk management" it would seem that legal risk management is simply a repackaging of what previously has been termed "compliance audits" or "due diligence". I argue that legal risk management constitutes much more and that we should draw more heavily from risk management methodology in defining what constitutes legal risk management.

This raises several questions: What is risk management? To what extent can risk management methodology be used in the context of legal risk? For what purposes can risk management be used if applied in the context of legal risk? Is the usefulness of applying risk management in the context of legal risk limited to business planning and management, or can it be used for other purposes? For example, can it be used to investigate the extent to which the law is adequate or too uncertain in relation to a particular activity, which could be useful for identifying areas requiring law reform?

The research in this thesis investigates these issues using a two step process. The first step involves examining risk management methodology and assessing the extent to which it can be used in the context of legal risk. This involves reviewing the literature on risk management and examining how risk management is used in practice by lawyers or risk managers who profess to apply risk management in the context of legal risk. In addition, in order to ascertain how risk management is used in the context of legal risk in practice, a limited qualitative survey of expert opinion was undertaken. A select number of experts who use risk management in relation to electronic commerce (2 participants), and legal practitioners or risk managers who offer legal risk management services (4) were interviewed using a self-completion questionnaire[1]. The aim of the survey was not to obtain empirical results but to obtain informed comment on the use of risk management methodology in the context of legal risk and how it is used in the marketplace. Ultimately, a model for *legal* risk management is developed. In addition, checklists and sample documentation are developed to facilitate the use of the legal risk management model.

The second part of this thesis involves determining the usefulness of the legal risk management model developed. This is achieved by applying the legal risk management model developed in this thesis in relation to a particular commercial

---

[1] The self-completion questionnaire was distributed by e-mail and responses provided by e-mail. The self-completion questionnaire is included at appendix 1 at p475. Participants were chosen on the basis of their reputation as users of risk management either in the context of electronic commerce or in relation to legal risk. Such information was obtained from articles and professional newsletters, responses to enquiries made to professional bodies including the Australian Institute of Risk Management, postings to specialist Internet newslists and upon recommendations of practitioners in the field.

activity which is commonly perceived to involve substantial legal risk, the conduct of Internet commerce. By applying legal risk management to the conduct of Internet commerce the usefulness of the legal risk management model developed is examined, and weaknesses and strengths of the model and the scope of its application is determined.

1.2 Significance of this study/ Justification for the research

The research issue and the methodology employed in this thesis are significant on several theoretical and practical grounds.

Broadly, this thesis investigates from a legal perspective two topics which have not previously been the subject of detailed research: risk management and the conduct of Internet commerce from an Australian business perspective.

More specifically, this thesis is significant for the following reasons:

- The relative neglect of legal risk management by previous researchers;
- The practical significance risk management has for legal practice;
- The contribution the research makes to understanding better certain legal issues affecting Internet commerce;
- The relative neglect by researchers to examine legal issues affecting Internet commerce *from a business perspective*; and
- The practical benefit to businesses of the evaluation and development of risk management strategies for managing certain legal risks associated with Internet commerce.

1.2.1 RELATIVE NEGLECT OF LEGAL RISK MANAGEMENT BY PREVIOUS RESEARCHERS

Very little has been written on the application of risk management in the context of legal risk with the exception of the use of risk management to manage the contractual risks associated with government procurement and outsourcing. This is in contrast with the literature available on the use of risk management by lawyers and law firms to manage the risks associated with running a legal practice. Such literature focuses on how lawyers can prevent instances of professional liability.

Moreover, a review of the existing literature reveals an often uneven approach to legal risk management with often little regard to risk management methodology. A risk management expert has, for example, commented:

> … whilst everyone says "I know and use AS4360"—very few risk managers understand it, and even if they do understand it, they don't apply or use it. This, in my view, stems from the fact that there are very few (perhaps fewer than 25) formal tertiary qualified risk managers in Australia—plenty have done "certificates", one to five day courses, are qualified in insurance, or are OH&S qualified: but such "qualifications" are not in risk management.[2]

This situation is perhaps not surprising given that legal risk management spans two disciplines, law and risk management. This thesis seeks to clarify how risk management can and should be used in the context of legal risk, and to establish a framework for legal risk management. In addition, this thesis seeks to synthesise the literature on risk management with the literature on compliance in the context of legal risk.

---

[2] Response dated 8 December 1999 to a self-completion questionnaire enquiring how the participant uses management methodology in the context of legal risk. Participants' names have not been disclosed to honour a request of some participants to remain anonymous. All responses are available on file.

1.2.2 RISK MANAGEMENT HAS SIGNIFICANCE FOR LEGAL PRACTICE

The outcome of this research will have practical significance for legal practice. A number of Australian law firms already offer legal risk management services[3]. By offering legal risk management services, law firms expand the range of services that they provide to clients and thereby create new business opportunities.

An interesting development that has taken place in the US has been the offer to businesses of reduced rates by three leading insurers provided that the insured business implements a risk management program in relation to the business's exposure to employment legal risks, part of which involves undergoing a free legal risk management audit undertaken by a particular law firm[4]. Again, this presents new business opportunities for law firms.

Legal risk management will be of particular practical significance to in-house counsel. Already, in-house counsel are taking more pro-active approaches in relation to legal risk:

> …the efforts of many general counsel are shifting from incident specific activities- such as shaping the legal aspects of major corporate transactions or responding to legal claims against corporate clients towards greater efforts to identify and reduce the legal risks raised by ongoing corporate actions.[5]
>
> …With these new demands on corporations have come new expectations of corporate general counsel. As the threat of corporate liability has expanded, the importance of minimizing that threat through proper management of corporate law compliance has grown accordingly. Where it once may have

---

3 For example, the law firms Blake Dawson Waldron and Freehill Hollingdale & Page expressly offer what is termed "Legal risk management" services.

4 Lee-Ann Gjertson, 'J & H M & M offers EPL cover, legal advice', *National Underwriter Property and Caualty/ Risk and Benefits Management*, December 8, 1997, v 101 n 49, pp 17-19.

5 Richard S Gruner, "The Randolph Thrower Symposium: The role of General Counsel: Perspective: General Counsel in an era of compliance programs and corporate self-policing", 46 *Emory Law Journal*, Summer 1997, p 1113 at p1114.

> been sufficient for a general counsel to play a traditional attorney's role in responding to a company's major legal crises and assisting with key corporate transactions, now a general counsel's role must extend beyond these tasks to encompass shaping a company's ongoing law compliance efforts and leading a legal department that aids in those efforts. As a result, today's general counsel is much more concerned with forward-looking, systematic features of corporate law compliance than his or her predecessors.[6]

The legal profession have recognised the usefulness of risk management in relation to the management of the risks associated with a legal practice, the Law Society of New South Wales regularly publishing articles in the Law Society Journal and offering courses about risk management of a legal practice[7].

The use of risk management, however, has not been widely used by lawyers in relation to the assessment of legal risk when providing legal advice to clients. Perhaps part of the reason is that law firms, influenced by the focus of Australian Standard *AS 3806 –Compliance* (which initially notes that legal compliance constitutes part of a business's overall risk management and then deals mostly with regulatory compliance), have typically placed emphasis on the notion of compliance rather than risk management. For example, the law firm Minter Ellison offers an on-line software based service called SAFETRAC for applying the Australian Standard *AS 3806 -Compliance*[8]. SAFETRAC offers Internet based compliance training in relation to the application of Australian Standard *AS 3806 - Compliance*. The

---

6 Gruner, *Emory Law Journal*, p1116.

7 For example, Ronwyn North, "Risk management education comes of age" (December 1996) 34 (11) *LSJ* 33, Ronwyn North, "Motivating yourself to manage risk more effectively in 1997" (February 1997) 35 (1) *LSJ* 41, David Taylor, "LawCover: profession responds positively to risk management", (October 1997) 35 (9) *LSJ* 44, Margaret Conners, "Risk Management: Lessons from Risk Management Education", (November 1999) 37 (10) *LSJ* 44.

8 See http://www.safetrac.com.au/.

promotional material states that SAFETRAC comprises of manuals, tutorials and tests in electronic form and a relational database that enables the effectiveness of a business's compliance program to be monitored. Gilbert & Tobin's product, on which the Minter Ellison service appears to be based, is called "ComplianceNet.[9]"

It is hoped that by establishing the extent to which risk management can be used in the context of legal risk, and, in particular, in relation to the legal risks associated with Internet commerce, that a framework for legal risk management is developed, which in turn can be used as a starting point for law firms and in-house counsel in the provision of legal risk management services.

1.2.3 THE RESEARCH OUTCOME CONTRIBUTES TO A BETTER UNDERSTANDING OF CERTAIN LEGAL ISSUES AFFECTING THE CONDUCT OF INTERNET COMMERCE

If even the most conservative forecasts about Internet commerce eventuate, Internet commerce promises substantial benefits to the Australian economy. However, there has been a reluctance by Australian consumers and businesses to use the Internet as a forum for commerce due to a perception that to conduct Internet commerce involves a high degree of legal risk.

Both government and industry players at a national and international level have identified that in order for businesses to take advantage of the opportunities presented by Internet commerce it is necessary for Internet commerce to operate in a predictable legal environment[10]. If, as suggested earlier in this chapter, legal risk

---

9 See http://www.gtcompliance.com.

10 See for example *The Emerging Digital Economy*, Report of the Secretariat of Electronic Commerce, http://www.ecommerce.gov/EmergingDig.pdf, p 21; *Electronic Commerce: Building the Legal Framework*, Report of the Electronic Commerce Expert Group to the Attorney-General,

management provides a method of identifying areas of legal uncertainty, the research in this thesis will pinpoint those aspects of Internet commerce that bring about legal uncertainty from an Australian business perspective and therefore impede the use of Internet commerce by Australian businesses. Two important effects flow from the research undertaken in this respect. Firstly, some aspects of Internet commerce for which a perception of legal uncertainty exists are analysed and whether such perception is justified is investigated. This information will be of interest to policy and regulatory advisers who seek to identify areas for which statutory regulation can facilitate Internet commerce. Secondly, by isolating those aspects of Internet commerce that actually bring about legal uncertainty we can break down the perception that Internet commerce is at present too risky a proposition for businesses to enter. If prospective businesses can see that Internet commerce, like any other forum for commerce, has its attendant risks, that these risks have been identified and that there are strategies for managing such risks, much of the basis for the perception that Internet commerce operates in an uncertain legal environment is removed.

---

31 March 1998, http://law.gov.au/aghome/advisory/eceg/ecegreport.html, para 4.01; "The Emergence of Electronic Commerce- Overview of OECD's Work", OECD Policy Brief No 1 November 1997 on Electronic Commerce, http://www.oecd.org/subject/electronic_commerce/documents; "Dismantling the Barriers to Global Electronic Commerce", An International Conference and Business-Government Forum organised by the OECD and the Government of Finland in Co-operation with the European Commission, the Government of Japan and the Business and Industry Advisory Committee, 19-21 December 1997, http://www.oecd.org/subject/electronic_commerce/documents.

1.2.4 RELATIVE NEGLECT BY RESEARCHERS TO EXAMINE LEGAL ISSUES AFFECTING INTERNET COMMERCE FROM A BUSINESS PERSPECTIVE

Several writers have focussed on the legal matters affecting the Internet from a policy and regulatory perspective. Much emphasis, therefore, has been placed on examining matters of public interest such as content regulation and privacy considerations.

At the time research for this thesis commenced few researchers had considered the legal issues associated with Internet commerce *from a business perspective* and even less has been written about this area from an Australian business perspective. Although a literature review indicates an increasing government interest in this area in Australia, the focus has tended to be on the issue of government's role in regulating Internet commerce[11]. This thesis seeks to fill this gap by investigating legal aspects of Internet commerce from an Australian business perspective.

---

[11] It should be noted that increasingly government agencies have become involved resulting in several position papers and reports written from a regulatory perspective. See for example *Electronic Commerce: Building the Legal Framework*, Report of the Electronic Commerce Expert Group to the Attorney-General, 31 March 1998, http://law.gov.au/aghome/advisory/eceg/ecegreport.html; Corporate Law Economic Reform Program, *Electronic Commerce: Cutting Cybertape- Building Business, Proposals for Reform*, Paper No 5, Commonwealth of Australia, AGPS, 1997; *Tax and the Internet*, Discussion Report of the Australian Taxation Office Electronic Commerce Project Team on the challenges of electronic commerce for tax administration, AGPS, August 1997; Steering Group of the Electronic Commerce Task Force, *Report of the Electronic Commerce Task Force to the Commonwealth Law Enforcement Board*, Commonwealth of Australia, November 1996; National Advisory Council on Consumer Affairs, *Consumer Protection in Electronic Commerce- Draft Principles and Key Issues*, National Advisory Council on Consumer Affairs, October 1997; Federal Bureau of Consumer Affairs, *Untangling the Web - Electronic Commerce and the Consumer*, Issues Paper No 3, AGPS, 1997; Australian Competition and Consumer Commission, *The Global Enforcement Challenge - Enforcement of consumer protection laws in a global marketplace*, Discussion paper, Commonwealth of Australia, August 1997.

1.2.5 THE EVALUATION AND DEVELOPMENT OF RISK MANAGEMENT STRATEGIES FOR MANAGING LEGAL RISKS ASSOCIATED WITH INTERNET COMMERCE WILL BE OF PRACTICAL BENEFIT TO BUSINESS

This thesis is also of practical significance to businesses. On a general level, this thesis provides businesses with a framework for applying legal risk management. More specifically, this thesis demonstrates how this framework can be used to identify, evaluate and manage some of the legal risks that arise in the the context of Internet commerce.

1.3 Research scope

The focus of this thesis is to investigate and determine how risk management can be used in the context of legal risk, for what purpose legal risk management is useful and what are the limitations of legal risk management. This involves examining risk management methodology and assessing how it can be applied in the context of legal risk. The outcome of this process should result in the development of a framework for legal risk management.

This thesis is an unconventional form of legal research in that it does not seek to identify legal impediments in relation to the conduct of a particular activity, in this case in relation to the conduct of Internet commerce, and then recommend proposals for law reform to remove the legal impediments. Neither does it seek to examine and discuss the policy issues concerning the regulation of a given activity.

Instead, this thesis seeks to establish the extent to which risk management, an important management tool, can be used by businesses to identify and manage legal risk assuming that the regulatory environment remains unchanged.

In this regard it should be noted that risk management is designed as a mechanism for identifying and managing the risks from the perspective of a single entity or a class of entities. Risk management therefore does not attempt to provide a multi-perspective analysis of risk. Accordingly, in the second part of this thesis, when legal risk management is applied in the context of Internet commerce, this thesis identifies and puts forward management strategies in relation to the risks faced by businesses conducting Internet commerce. This thesis does not therefore consider the legal risks that face consumers who purchase through the Internet.

In addition, the topic of Internet commerce raises manifold legal issues and it is not feasible to deal with all these issues here. This thesis focuses on the use of risk management by Australian businesses whose Internet commerce activities are conducted from a location physically based in Australia. Whilst the following discussion may be equally applicable to businesses based in other jurisdictions, it is beyond the scope of this thesis to consider, except, perhaps, in passing, the relevant legislative framework and judicial decisions that govern the conduct of Internet commerce by businesses based in other jurisdictions.

Further, it is beyond the scope of this thesis to consider the following legal aspects of Internet commerce:

- the criminal liability of businesses that conduct Internet commerce;
- the off-line legal risks affecting businesses that conduct Internet commerce (such as the legal issues arising in relation to off-line delivery of goods eg. bills of lading etc, customs, export licensing);

- the legal risks that affect businesses that provide third party Internet services (such as Internet service providers, digital cash providers, certification authorities and virtual mall providers) as distinct from the legal risks arising from business-to-business or business-to-consumer Internet commerce;
- the industry specific legal risks affecting businesses that conduct Internet commerce eg. legal risks affecting the conduct of Internet gambling; legal risks affecting the sale of securities on the Internet; legal risks affecting the sale of x-rated material on the Internet;
- the legal risks affecting businesses that conduct Internet commerce in relation to the application of consumer protection laws to Internet transactions;
- the legal risks affecting businesses that conduct Internet commerce in relation to privacy and confidentiality obligations that arise in relation to the conduct of Internet commerce;
- the legal risks affecting businesses that conduct Internet commerce in relation to the application of taxation law to Internet transactions.

1.4 Outline of thesis structure

This thesis has 6 chapters. This introductory chapter sets the background for and introduces the research issue and methodology used to analyse the research issue. In addition, the choice of research issue and methodology is justified. The discussion in this chapter also sets out the research parameters of this thesis.

Chapter 2 entitled *Using risk management in the context of legal risk* sets the theoretical focus of the thesis. In this chapter the use of risk management in the

context of legal risk is examined. First, the extent to which risk management can be used to identify and manage legal risk is considered. Then, the usefulness or applicability of legal risk management is investigated. By undertaking this research a framework for legal risk management is developed. A series of checklists for undertaking the various stages of the legal risk management process is developed along with sample documentation to record the outcome of these steps. (In order to distinguish the checklists and sample documentation from other material presented in table form, the formatting of the checklists and sample documentation differs in style from other material presented in table form in this chapter.) Also, the role of legal risk management is compared to preventive law and legal compliance.

Chapter 3 entitled *Internet commerce and legal risk management* introduces the second part of this thesis in which the legal risk management approach developed in the first part of the thesis is applied. This chapter considers what constitutes Internet commerce, how Internet commerce can benefit Australian businesses, how Internet commerce is conducted and provides a justification for applying legal risk management to this topic.

Chapter 4 entitled *Cyber - dealing I: Identifying the business's legal risk management objectives and* the legal risks applies the first and second steps in the legal risk management process. That is, the legal risk management objectives of a business in relation to the conduct of Internet commerce and the legal risks associated with Internet commerce are identified. As risk management methodology involves using several techniques to identify risk the discussion will involve some overlap in

relation to the legal risks identified. This overlap is eliminated and an overall list of legal risks identified is presented in table form at the end of the chapter. The format of this table is different in order to distinguish this table from the other tables of legal risks listed in this chapter.

Chapter 5 entitled *Cyber - dealing II: Risk analysis and risk* management strategies applies the third and fourth step of legal risk management. In this chapter a detailed examination of the legal risks associated with Internet commerce is undertaken, including a qualitative analysis of the legal risks. Then various strategies for managing the legal risks are put forward and evaluated.

Chapter 6 sets out the research outcomes and conclusions of the thesis including an assessment of the implications of the research for practice.

1.5 Definition of terms and vocabulary

Throughout this thesis, technical terms and other specialist vocabulary will be used whose definitions will be given only when they first appear. For ease of reference these terms and their definitions are reproduced at the Appendix at page 475.

1.6 Conclusion

This chapter has outlined the foundations for this thesis including the research issue and the methodology used to analyse it, their justification, and the structure and parameters of the thesis. In addition, the structure of the thesis was outlined, and the parameters of the thesis were set out. I now move to a detailed examination of the risk management methodology applied in this thesis.

CHAPTER 2 USING RISK MANAGEMENT IN THE CONTEXT OF LEGAL RISK

2.1 Introduction

This chapter sets out the theoretical focus of this thesis. It investigates the application of risk management and the scope of its application in the context of legal risk. Several risk management models are examined and the *AS/NZS* 4360 *Risk Management* model is selected for investigation as to whether it could be used in the context of legal risk. The research points to the conclusion that risk management methodology can equally be used in the context of legal risk and a framework for applying risk management in the context of legal risk based on Australian Standard 4360 *Risk Management* is developed. More specifically, the research in this chapter finds that legal risk management can be used by business as a tool for achieving legal compliance, avoiding exposure to liability and protecting legal rights and interests. This may not sound controversial but this finding expands upon present understanding of how risk management can be used in the context of legal risk. Risk management, when used in this way, is highly useful as a technique for identifying and managing legal risks that constitute "hazards" according to risk management terminology. In addition, risk management when used in this way may be useful for policy makers as a tool for identifying areas requiring law reform. Importantly, the use of risk management in the context of legal risk results in legal risks being evaluated consistently. This provides an authoritative basis for prioritising legal risks. In contrast, no such mechanisms exist in relation to conventional legal advice to ensure that legal risks are analysed consistently and can therefore be legitimately prioritised (as opposed

to being prioritised according to gut feel and intuition). In addition, the role of legal risk management is considered in relation to legal compliance and preventive law. The research findings of this chapter point to the conclusion that risk management much to offer when applied in the context of legal risk.

2.2 What is risk management?

Risk management is a systematic process that involves the development, implementation and ongoing review of a system for identifying and measuring risks that affect a business's activities which, if they eventuated, would result in exposure to significant loss[12], and devising and implementing strategies to minimise, transfer, share or, if possible, avoid those risks. Risk management, sometimes described as a branch of applied economics[13], is one of several management tools used by businesses to determine whether returns anticipated by a business as a consequence of undertaking certain activities outweigh the associated risks. Risk management is not intended to stand alone- rather it is simply one component of a business's management and decision-making processes.

Historically, risk management emerged in the early 1950s when principles previously used by insurance managers in the context of identifying and assessing risks for insurance purposes were adapted for broader application in relation to

---

[12] Although risk management is most commonly used to identify and manage risks that, if they eventuated, would cause a business to incur a loss it is interesting to note that the risk management process can also be used to determine the level of opportunity a particular risk may pose to a business. This is discussed in more detail by the Standards Australia/Standards New Zealand Joint Technical Committee on Risk Management, "A Basic Introduction to Managing Risk using the Australian and New Zealand Risk Management Standard - AS/NZS 4360: 1999", Master Draft as at 4/1/99 pp 26-27.

[13] Emmett J Vaughan, *Risk Management*, John Wiley & Sons, Inc, New York, 1997, Ch 1, p 21. The author also points out the strong influence of risk management techniques developed by

risk management[14]. Whilst risk management is derived from insurance management principles, the philosophy of risk management is fundamentally different from insurance management:

> Although risk management has its roots in corporate insurance buying, it is a distortion to say that risk management naturally evolved from corporate insurance buying. Actually the emergence of risk management signalled a dramatic, revolutionary shift in philosophy, occurring when attitudes toward insurance changed. For the insurance manger, insurance had always been the standard approach to dealing with risks. Although insurance management included techniques other than insurance (such as noninsurance or retention and loss prevention and control), these techniques had always been considered primarily as alternatives to insurance. The insurance manager viewed insurance as the accepted norm or standard approach to dealing with risk, and retention was viewed as exception to this standard.
>
> ...
>
> The change in attitude toward insurance and the shift to the risk management philosophy had to await management science, with its emphasis on cost-benefit analysis, expected value, and a scientific approach to decision making under uncertainty.[15]

The objectives of risk management are manifold and vary in each circumstance, according to the emphasis placed by the business applying risk management. Such objectives can include: ensuring that a business can, at a minimal cost continue, in the event of adverse loss-inducing circumstances, to increase a business's profit (or for a non-profit organisation to reduce the budget it requires for a particular activity) by reducing the cost to a business of a risk associated with a business's activities without unduly interfering with the activities undertaken by the business[16], to reduce anxiety[17] and to comply with

---

engineers at NASA.

14 Vaughan, p 27.

15 Vaughan, pp 27-28.

16 George L Head and Stephen Horn, *Essentials of Risk Management*, Insurance Institute of America, 1991, http://www.bus.orst.edu/faculty/nielson/rm/chapter1.htm.

17 Vaughan, p 95.

externally imposed objectives such as contractual, tortious or regulatory obligations and to exhibit social responsibility[18].

The theory of risk management is now well established and comprehensively documented[19]. It is unnecessary here to examine theory in detail. It is necessary, however, to include some discussion of risk management techniques in order to examine the extent to which these techniques can be used in relation to the identification, analysis and management of legal risk.

In the Australian context, Standards Australia has developed a guideline for the application of risk management *AS/NZS 4360* - 1999 *Risk Management* (revised). In addition, the application of risk management in the public service is now well established as evidenced by Guidelines for Managing Risk in the Australian Public Service, which is now a public service standard[20], and various other public service publications setting out the application of risk management to particular departments and agencies[21].

---

18 Head and Horn, *Essentials of Risk Management*, http://www.bus.orst.edu/faculty/nielson/rm/chapter1.htm.

19 See for example the following texts that set out the theory of risk management: Emmett J Vaughan, *Risk Management*, John Wiley & Sons, Inc, New York, 1997; George L Head and Stephen Horn, *Essentials of Risk Management*, Insurance Institute of America, 1991 http://www.bus.orst.edu/faculty/nielson/rm/; Robert I Mehr and Bob A Hedges, *Risk Management in the Business Enterprise*, Richard D Irwin Inc, Homewood Illinois, 1963; Neil Crockford, *An Introduction to Risk Management*, 2nd Edition, Woodhead-Faulkner, Cambridge, 1986. There is also an Australian Standard for Risk Management, *AS/NZS 4360-1999, Risk Management*, Standards Australia, Strathfield NSW, 1999.

20 *Guidelines for Managing Risk in the Australian Public Service*, Joint publication of the Management Advisory Board and its Management Improvement Advisory Committee, Report No 22, AGPS, Canberra, October 1996.

21 For example, The Auditor-General, *Risk Management Australian Taxation Office*, Commonwealth of Australia, Audit Report No. 37, 1996-1997; The Auditor-General, *Risk Management in ATO- Small Business Income – Australian Taxation Office*, Commonwealth of Australia, The Auditor-General Audit Report No. 19, 1997- 98; The Auditor-General, *Risk Management by Commonwealth Consumer Product Safety Regulators* Australian Government Publishing Service, Audit Report No. 12 1995-96; *Understanding Risk Management in the APS-an ongoing challenge*, an address to SES Officers in the Australian Customs Service by

The application of risk management has also become quite specialised in relation to some sectors such as project management, disaster planning, environmental risk management and investment, derivatives risk management and portfolio risk management where much has been written on how risk management should be employed in relation to those disciplines.

It is useful to examine, albeit at an elementary level, how risk management is used in these sectors. First, portfolio risk management will be examined. Portfolio risk management derives from a theory on portfolio selection propounded by Harry Markowitz in 1952[22]. The theory is based on that of share diversification, that is, investing in a portfolio of shares to spread the risk associated with share volatility. Portfolio risk management uses quantitative methods to measure variance in returns on shares to assist an investor in selecting a portfolio that reduces the overall volatility of the returns on the investor's portfolio:

> The mathematics of diversification helps to explain its attraction. While the return on a diversified portfolio will be equal to the average of the rates of return on its individual holdings, its volatility will be less than the average volatility of its individual holdings. This means that diversification is a kind of free lunch at which you can combine a group of risky securities with high expected returns into a relatively low-risk portfolio, so long as you minimize the covariances, or correlations, among the returns of the individual securities[23].

The techniques used to undertake portfolio risk management have and continue to be developed. For example, instead of measuring the covariance among individual securities, a technique termed the Capital Asset Pricing Model was

---

Pat Barrett AM, Commonwealth Auditor General, Tuesday, 26 March 1996, Canberra, Public Sector Accounting Centre of Excellence, Working Paper Series No. 1996.

[22] Peter L Bernstein, *Against the Gods- The remarkable story of risk*, John Wiley & Sons, Inc, New York, 1996, p 248.

[23] Bernstein, p 253.

introduced by William Sharpe whereby the variation of a security is calculated in relation to the market as a whole[24]:

> Markowitz' early work on portfolio theory has been extended into the Capital Asset Pricing Model (Sharpe 1964; Lintner 1965) where total risk is divided into two parts- unsystematic (unique, residual or specified) risk, and systematic (market) risk. Unsystematic risk derives from factors unique to each firm which influence firm variability of returns, and it can be diversified away by inclusion of a sufficient number of securities in a portfolio. Systematic risk is the portion of return variability which arises from forces which impinge on the economy as a whole, affect all companies and cannot be eliminated by diversification[25].

Put in layman's terms, the Capital Asset Pricing Model: "analyses how financial assets would be valued if all investors religiously followed Markowitz's recommendations for building portfolios. CAPM, as it is known, uses the term "beta" to describe the average volatility of individual stocks or other assets relative to the market as a whole over some specific period of time."[26] As can be seen portfolio risk management relies heavily on quantitative techniques for analysing risk and selecting appropriate risk management strategies.

Another example of the use of risk management in a specialised context is its use in environmental health risk assessment. In the US in particular, the use of risk management to identify, assess and manage environmental hazards such as toxic and carcinogenic materials has evolved into a separate discipline with a defined methodology[27]. Risk management when used for environmental risk assessment involves: identifying contaminants that are suspected of posing hazards to human health; evaluating the circumstances in which the contaminants

---

24 Bernstein, p 258.

25 Inga S Baird and Howard Thomas, "What is Risk Anyway?", in *Risk, Strategy, and Management*, edited by Richard A Bettis, Howard Thomas, JAI Press Inc, Greenwich, Connecticut, 1990.

26 Bernstein, p 249.

pose health risks to humans and assessing those members of the community who might be exposed to the contaminant; and estimating the magnitude, duration of exposure to the contaminant to which they are exposed[28]. Once this information is obtained a qualitative or quantitative estimate is undertaken of the likelihood that the hazards identified will eventuate[29]. Identification of these contaminants can involve both qualitative and quantitative techniques and usually involves a review of scientific studies and other environmental monitoring projects[30]. There are several US Environmental Protection Agency guidelines that lay down basic principles for using risk management in the context of environmental health risk assessment.

Finally, risk management is used regularly in the public sector. In fact, risk management is considered by the Commonwealth government as an integral part of both good business practice and the Australian public service reform program[31] and a guideline written specifically for the use of risk management in the Australian public sector exists[32]. One specific area where risk management is employed in the public service is the area of procurement[33]. Risk management is used in this context to identify and manage a wide range of risks associated with

---

27 See for example, the methodology described in National Research Council, *Science and Judgment in Risk Assessment*, National Academy Press, Washington DC 1994.

28 National Research Council, p2-2.

29 National Research Council, p2-2.

30 National Research Council, p2-2.

31 MAB/MAIC Report No. 23, *Before you sign the dotted line…ensuring contracts can be managed*, May 1997, p 8.

32 *Guidelines for Managing Risk in the Australian Public Service*, Joint Publication of the Management Advisory Board and its Management Improvement Advisory Committee, Report No 22, AGPS, Canberra, October 1996.

33 See for example, Purchasing Australia, Commonwealth of Australia, *Managing risk in procurement- A handbook*, Australian Government Publishing Service, Canberra, 1996; MAB/MAIC Report No. 23, *Before you sign the dotted line…ensuring contracts can be managed*, May 1997.

procurement by government departments and agencies including quality of goods and services purchased, the ethical behaviour of employees of the outsourcing company, the specification and tendering process, industrial relations, confidentiality and privacy, fraud and negligence and contractual risks associated with outsourcing.

2.3 Outline of the risk management process

The risk management process is variously described as a four-step, five-step or six-step process[34]. In this thesis, a six-step model based on Australian *Standard AS/NZS 4360 -1999 Risk Management* is adopted, the reasons for which will be discussed shortly. It is important, however, to be aware that the differences between the alternative risk management models are for the most part superficial. For example, one model may characterise as one step, what another model may

---

[34] The four-step process is described as follows: (1) defining the problem, (2) evaluating the possible solutions, (3) selecting and implementing the optimal solution, (4) monitoring the performance of the solution (Neil Crockford, *An Introduction to Risk Management*, 2nd Edition, Woodhead-Faulkner, Cambridge, 1986, Ch 1, p 4.) Some writers prefer to describe risk management as a five step process, separating the third step, as earlier described, into two steps: (i) implementing risk management strategies and (ii) putting in place strategies to ensure ongoing compliance with the implemented strategies and modifying them to reflect changed circumstances (see for example, George L Head and Stephen Horn, *Essentials of Risk Management*, Insurance Institute of America, 1991, http://www.bus.orst.edu/faculty/nielson/rm/chapter1.htm). Others refer to risk management as a six step process which includes, in addition to the steps described in the five step process, involves an additional initial step which involves determining the risk management objectives of the business (see for example, Emmett J Vaughan, *Risk Management*, John Wiley & Sons, Inc, New York, 1997, Ch 2, p 34). *AS/NZS 4360- 1999, Risk Management*, Standards Australia, Strathfield NSW, 1999, describes risk management as a seven stage process, which comprises the following: (i) establishing the strategic, organizational and risk management context (this is similar to determining the risk management objectives as described by Vaughan), (ii) identifying risks, (iii) analysing risks; (iv) evaluating and prioritising risks, (v) treating risks; (vi) monitoring and review of the risk management system implemented and (vii) communicating and consulting with internal and external stakeholders. The Australian Public Service has adopted the six step process advocated by the Australian Standard 1995 version which omitted step (vii), as described earlier. See for example, *Guidelines for Managing Risk in the Australian Public* Service, Joint Publication of the Management Advisory Board and its Management Improvement Advisory Committee, Report No 22, AGPS, Canberra, October 1996.

characterise as two steps. Furthermore, as one risk management writer has pertinently noted, in practice, a distinction between each of the steps is not strictly observed. That is, when applying risk management there is a tendency to merge one step with another[35].

For comparison purposes, a brief description of the alternative risk management models follows.

2.3.1 FOUR-STEP RISK MANAGEMENT MODELS

Two four-step risk management models are described here. The first four-step model **("Crockford four-step risk management model")** comprises: (1) defining the problem, (2) evaluating the possible solutions, (3) selecting and implementing the optimal solution, (4) monitoring the performance of the solution[36].

Table 1 CROCKFORD FOUR-STEP RISK MANAGEMENT MODEL

1.	Defining the problem.
2.	Evaluating the possible solutions.
3.	Selecting and implementing the optimal solution.
4.	Monitoring the performance of the solution.

The alternative four-step risk management model **("Sadgrove risk four-step risk management model")** involves: (1) assessing the risks, (2) setting priorities

---

35 Vaughan, p 34.

36 Neil Crockford, *An Introduction to Risk Management*, 2nd Edition, Woodhead-Faulkner, Cambridge, 1986, Ch 1, p 4.

(prioritising the risks), (3) preventing the risks from happening and (4) planning (putting in place a plan for handling risks that eventuate)[37]:

Table 2 SADGROVE FOUR-STEP RISK MANAGEMENT MODEL	
1.	Assessing the risks.
2.	Setting priorities (prioritising the risks).
3.	Preventing the risks from happening.
4.	Planning (putting in place a plan for handling risks that eventuate).

2.3.2 FIVE-STEP RISK MANAGEMENT MODELS

There are several five-step models. One of these models **("Head and Horn five-step risk management model")** is practically the same as the first described four-step model, except that the third step, as described in the four-step process above, is separated into two steps so that risk management comprises: (1) identifying exposures to accidental loss that may interfere with an organization's basic objectives, (2) examining feasible alternative risk management techniques for dealing with these exposures, (3) selecting the apparently best risk management techniques, (4) implementing the selected risk management strategies, and (5) monitoring the results of the selected risk management techniques to ensure that the risk management program remains effective[38].

---

[37] Kit Sadgrove, *The Complete Guide to Business Risk Management*, Gower Publishing Limited, Hampshire,k England, 1996, p 20.

[38] Head and Horn, *Essentials of Risk Management*, http://www.bus.orst.edu/faculty/nielson/rm/chapter1.htm.

Table 3 HEAD AND HORN FIVE-STEP RISK MANAGEMENT MODEL	
1.	Identifying exposures to accidental loss that may interfere with an organization's basic objectives.
2.	Examining feasible alternative risk management techniques for dealing with these exposures.
3.	Selecting the apparently best risk management techniques.
4.	Implementing the selected risk management strategies.
5.	Monitoring the results of the selected risk management techniques to ensure that the risk management program remains effective.

The five-step model has also been characterised as: (1) risk identification, (2) risk quantification, (3) risk evaluation, whereby policy options are formulated and evaluated in terms of their cost, benefits and risks, (4) risk acceptance and avoidance which involves comparing the costs and benefits associated with each risk in order to determine the level of acceptability and (5) risk management, that is implementing the risk management strategies selected **("Haimes five-step risk management model")**[39]:

Table 4 HAIMES FIVE-STEP RISK MANAGEMENT MODEL	
1.	Risk identification.
2.	Risk quantification.
3.	Risk evaluation.
4.	Risk acceptance and avoidance.
5.	Risk management.

[39] Yacov Haimes, *Risk Modeling, Assessment, and Management*, John Wiley & Sons, Inc, New York, 1998, pp 55-56.

A notably different risk management model **("Sadgrove five-step risk management model")** involves the following five steps: (1) Risk awareness- recognise that risks exist in business and that they must be managed, (2) Assessing the risks, (3) Set priorities- decide which risks should have the highest priority, (4) Prevent the risks from happening (Minimise risk, Transfer risk, Spread risk) and (5) Plan for the worst (Disaster plan, Alternative options)[40].

Table 5 SADGROVE FIVE-STEP RISK MANAGEMENT MODEL	
1.	Risk awareness.
2.	Assess (audit, measure).
3.	Set priorities.
4.	Prevent (minimise risk, transfer risk, spread risk).
5.	Plan for the worst (disaster plan, alternative options).

2.3.3 SIX-STEP RISK MANAGEMENT MODELS

There are three six-step risk management models that warrant description. The first six-step model **("Vaughan six-step risk management model")** comprises the following: (1) determining objectives of the business, (2) identifying risks, (3) evaluating the identified risks, (4) considering and selecting risk management strategies, (5) implementing selected risk management strategies and (6) monitoring and review of the risk management system implemented[41]:

---

[40] Sadgrove, pp 19-20.
[41] Vaughan, p 34.

Table 6 VAUGHAN SIX-STEP RISK MANAGEMENT MODEL	
1.	Determining objectives of the business.
2.	Identifying risks.
3.	Evaluating the identified risks.
4.	Considering and selecting risk management strategies.
5.	Implementing selected risk management strategies.
6.	Monitoring and review of the risk management system implemented.

Another six-step model that merits description is the model used in the Canadian Standard CAN/CSA-Q850-97 *Risk Management: Guideline for Decision-Makers*[42] **("Canadian Standard six-step risk management model")**. This model involves: (1) initiation (defining the problem and risk issues, identifying the risk management team, assigning responsibility, authority and resources, identifying potential stakeholders and beginning to develop a consultation process), (2) preliminary analysis (define scope of decision-making, identify hazards, begin stakeholder analysis, start a risk information library), (3) risk estimation (define methodology for estimating frequency and consequences, estimate frequency and consequence, refine stakeholder analysis through dialogue), (4) risk evaluation (estimate and integrate benefits and costs, assess stakeholder assessment of risk), (5) risk control (identify feasible risk control options, evaluate risk control options, assess stakeholder acceptance of proposed

[42] Canadian Standards Association, *Risk Management: Guideline for Decision-Makers CAN/CSA-Q850-97*, Canadian Standards Association, Ontario, Canada, October 1997.

action, evaluate options for dealing with residual risk, assess stakeholder acceptance of residual risk), (6) action/monitoring[43].

Table 7 CANADIAN STANDARD SIX-STEP RISK MANAGEMENT MODEL AS USED IN *RISK MANAGEMENT: GUIDELINE FOR DECISION-MAKERS CAN/CSA-Q850-97*

1.	Initiation.
2.	Preliminary analysis.
3.	Risk estimation.
4.	Risk evaluation.
5.	Risk control.
6.	Action/monitoring.

Finally, the alternative six-step model, set out in *AS/NZS 4360 - 1995, Risk Management*, comprises: (1) establishing the context, (2) identifying risks, (3) analysing the identified risks, (4) evaluating and prioritising the identified risks and accepting those risks evaluated as "acceptable", (5) treating the remaining risks, (6) monitoring and reviewing the risk management system implemented **("Australian Standard six-step risk management model")**[44]:

---

[43] Canadian Standards Association, p 7.

[44] *AS/NZS 4360- 1995, Risk Management*, Standards Australia, Homebush NSW, 1995, para 3.2. The Australian Public Service has adopted the six step process advocated by the Australian Standard. See for example, *Guidelines for Managing Risk in the Australian Public* Service, Joint Publication of the Management Advisory Board and its Management Improvement Advisory Committee, Report No 22, AGPS, Canberra, October 1996.

Table 8 AUSTRALIAN STANDARD SIX-STEP RISK MANAGEMENT MODEL AS USED IN *AS/NZS 4360 - 1995, RISK MANAGEMENT*

1.	Establishing the context.
2.	Identifying risks.
3.	Analysing the identified risks.
4.	Evaluating and prioritising the identified risks and accepting those risks evaluated as "acceptable".
5.	Treating the remaining risks.
6.	Monitoring and reviewing the risk management system implemented[45].

AS/NZS 4360 - 1995, Risk Management has now been revised and reissued as *AS/NZS 4360 - 1999, Risk Management*. The latest version of the Standard incorporates an additional *element*, that of communicating and consulting with relevant stakeholders throughout the risk management process. Strictly speaking this element does not constitute a "step" in the risk management process, as it applies throughout the entire risk management process[46]. The revised Australian Standard model will still be referred to as the six-step model notwithstanding the additional element of communicating and consulting throughout the risk management process with relevant stakeholders. Although the Australian Standard depicts the additional element in its model of the risk management process, it is more convenient here, where the various risk management models have been described as a series of steps, to treat this element in the same way as

[45] According to *AS/NZS 4360- 1995, Risk Management* and its more recent revised version, Step 6 is strictly not a "step" in the risk management process as monitoring and review should take place at every stage of the risk management process . However, even *AS/NZS 4360- 1995, Risk Management* and its more recent revised version, when describing the steps involved in developing and implementing a risk management system refer to the process of monitoring and review as a "step" in the risk management process and it is convenient here to describe the process of monitoring and review as the sixth step, given that the other risk management models employ the term "step".

"documentation", another element of the risk management process that is not a "step", is treated by *AS/NZS 4360 - 1999, Risk Management*. That is, it is not depicted in the risk management model although it is an integral element. Thus, the risk management model put forward in between *AS/NZS 4360 - 1999, Risk Management* has the same steps as the earlier version.

There appears to be one fundamental difference between *AS/NZS 4360 - 1999, Risk Management* (and its earlier version) and the other models. *AS/NZS 4360 - 1999, Risk Management* and other Australian risk management literature that follow it (and its earlier version) advocate that, after analysing each risk in terms of likelihood of risk and magnitude of consequence, each identified risk should be prioritised. Once ranked, the next step in the risk management process is to decide which risks fall into the "acceptable" category in which case treatment may not be required[47]. This involves referring to the business's risk criteria and comparing each categorised risk with the level of risk the business is prepared to accept. In effect, what is therefore being decided is which risks the business will retain. Some commentators maintain that there is a distinction between what constitutes "acceptance" and "retention", the former term referring to the instance where a business decides to set aside funding in the event that a risk eventuates and the latter term referring to the instance where costs incurred as a result of a risk eventuating are kept as part of the business's operational expenses (operating costs)[48]. However, it is argued here that "acceptance" is simply a form of

---

46 *AS/NZS 4360- 1999, Risk Management*, para 4.7.
47 *AS/NZS 4360- 1999, Risk Management*, para 4.4.
48 Information given by Mr Kevin Knight, a member of the Joint Technical Committee OB/7- Risk Management that prepared *AS/NZS 4360- 1999, Risk Management* and its earlier version.

"retention" and therefore it is unhelpful to draw a distinction between "acceptance" and "retention" and use such distinction to divide up the treatment of risks in the way *AS/NZS 4360 - 1999, Risk Management* advocates. According to *AS/NZS 4360 - 1999, Risk Management*, low priority risks are "accepted" and monitored periodically to ensure they remain acceptable[49]. Only those risks that warrant "treatment" go onto the next step which is called "risk treatment" and which involves choosing appropriate risk management strategies for the remaining risks which are assessed as requiring risk treatment. At this point the range of risk management strategies (which is discussed later in this chapter) are considered, including the risk management strategy of risk retention. The approach advocated by *AS/NZS 4360 - 1999 Risk Management* requires consideration of whether to retain a risk at two levels (or adopting a two-step process); first, when ascertaining broadly which identified risks require risk management and, secondly, when determining appropriate risk management strategies for those identified risks that require risk management[50]. Other risk management texts, such as those emanating from the UK and the US, advocate a different approach. Once the risks have been identified and evaluated in terms of probability and frequency the next step is to consider all the risks and what is the appropriate risk management strategy in relation to each risk, which may include risk retention.

From a theoretical perspective, it seems to be unnecessary to consider risk retention in both the "risk evaluation" and "risk treatment" steps of the risk

---

49 *AS/NZS 4360- 1999, Risk Management*, para 4.4.
50 *AS/NZS 4360- 1999, Risk Management*, para 4.4.

management process. Moreover, to consider risk retention at both steps could result in a given risk being managed differently depending on whether it was assessed for retention at the "risk evaluation" step or the "risk treatment" step of the risk management process. As noted earlier at 2.3.3, according to the model advocated by *AS/NZS 4360 - 1999, Risk Management*, if a risk is evaluated as being "low" or "acceptable" at the "risk evaluation" step then that risk "may be accepted with minimal further treatment [51]. No specific techniques are advocated in the discussion of *"risk evaluation"* in *AS/NZS 4360 - 1999, Risk Management* for determining whether a risk should be accepted or not other than to retain risks that have been evaluated as "low" or "acceptable" risks. However, the other risk management models in their discussion of the *"risk treatment"* step (which is where these models advocate considering risk retention as a risk management strategy) consider specific techniques which assist in determining which risks to retain. *AS/NZS 4360 - 1999, Risk Management*, also notes that there are several factors to take into account when determining which risk treatment approach (including risk retention) to apply. These techniques are more fully discussed later in this chapter, but by way of illustration, one such technique is to ascertain the business's cash flow and retain those risks that, if they eventuated, would constitute a range of 5 to 10 percent of the preceding year's non-dedicated cash flow[52].

To use one technique for determining whether to retain a risk at one step of the risk management process, and to use other techniques at another step of the risk

---

51 *AS/NZS 4360- 1999, Risk Management*, para 4.4.

52 Vaughan, p 319.

management process to determine whether to retain a risk, as does *AS/NZS 4360 - 1999, Risk Management*, would result in an inconsistent and unsystematic approach, that in turn, arguably undermines the purpose of risk management, which is to provide a system of systematically identifying and managing risk. It is for these reasons that the approach taken by *AS/NZS 4360 - 1999, Risk Management* (more specifically steps 4 and 5) is considered to be unsatisfactory.

There are, however, some practical reasons for using the two-step process advocated by *AS/NZS 4360 - 1999, Risk Management* which arguably override the reasons against using the two-step approach. The justification for the two-step approach taken by *AS/NZS 4360 - 1999, Risk Management* is that it saves management having to review and consider risk management strategies for risks that have already been assessed as being risks that can be retained as part of the business's normal operational activities[53]. The reasoning is that it is a waste of time and resources if management has to make decisions about retaining a risk that so obviously can be retained by a business. Instead it is preferable to separate those risks that require a management decision as to how they will be treated and to only put to senior management those risks which require input as to what risk treatment (risk management) strategies should be employed by a business[54].

2.3.4 RISK MANAGEMENT MODEL EMPLOYED IN THIS THESIS

Which model will be followed in this thesis? A comparison of each of the models is provided in the following figure:

---

[53] Telephone communication with Mr Kevin Knight on 23 December 1998, Risk Management Coordinator, Education Queensland and a collaborator on *AS/NZS 4360- 1999, Risk Management.*

[54] Telephone communication with Mr Kevin Knight on 23 December 1998.

Table 9 COMPARISON OF RISK MANAGEMENT MODELS AGAINST SIX-STEP RISK MANAGEMENT MODEL USED IN THIS THESIS

6–step risk management model used in this thesis	**Crockford 4–step risk management model.**	**Sadgrove 4–step risk management model**	**Head and Horn 5–step risk management model**	**Sadgrove 5–step risk management model**	**Haimes 5–step risk management model**	**Vaughan 6–step risk management model**	**Canadian Standard 6- step risk management model**	**Australian Standard 6-step risk management model**
1. Determining the objectives of the business, or establishing the context.	1. Defining the problem.	1.Assessing the risks.	1. Identifying exposures to accidental loss that may interfere with an organization's basic objectives.	1. Risk awareness.	1. Risk identification.	1. Determining objectives of the business.	1. Initiation.	1. Establishing the context.
2. Identifying the risks to which the business is exposed by reference to the risk management objectives of the business.	2. Evaluating the possible solutions.	2. Setting priorities (prioritising the risks).	2. Examining feasible alternative risk management techniques for dealing with these exposures.	2. Assess (audit, measure).	2. Risk quantification.	2. Identifying risks.	2. Preliminary analysis.	2. Identifying risks.
3. Analysing the identified risks.	3. Selecting and implementing the optimal solution.	3. Preventing the risks from happening.	3. Selecting the apparently best risk management techniques.	3. Set priorities.	3. Risk evaluation.	3. Evaluating the identified risks.	3. Risk estimation.	3. Analysing the identified risks.
4. Evaluating and selecting risk management strategies	4. Monitoring the performance of the solution.	4. Planning (putting in place a plan for handling risks that eventuate).	4. Implementing the selected risk management strategies.	4. Prevent (minimise risk, transfer risk, spread risk).	4. Risk acceptance and avoidance.	4. Considering and selecting risk management strategies.	4. Risk evaluation.	4. Evaluating and prioritising the identified risks and accepting those risks evaluated as "acceptable".
5. Implementing the selected risk management strategies.			5. Monitoring the results of the selected risk management techniques to ensure that the risk management program remains effective.	5. Plan for the worst (disaster plan, alternative options).	5. Risk management.	5. Implementing selected risk management strategies.	5. Risk control.	5. Treating the remaining risks.
6. Monitoring and conducting an ongoing review of the risk management system implemented.						6. Monitoring and review of the risk management system implemented.	6. Action /monitoring.	6. Monitoring and reviewing the risk management system implemented. # Communicating and consulting with stakeholders. (Strictly, speaking this is an element, rather than a step of the risk management process)

As can be seen, apart from the model advocated by *AS/NZS 4360 - 1999, Risk Management* the risk management models discussed are basically the same with some steps being manifested as one step in some models and two steps in others. Moreover, as noted earlier at 2.3, whether a four, five or six-step model is followed, in practice the steps tend to be merged. On the basis that it is preferable to follow the model advocated by Standards Australia, this thesis adopts the six-step revised model set out in the Standard, although for the reasons discussed above, the two-step process described in steps 4 and 5 of *AS/NZS 4360 - 1999, Risk Management* will not be followed. The reason for not following the two-step process is that, although in practice this approach may well be preferable, it does not make sense when discussing risk management in theory to follow such an approach.

Accordingly, the six-step model that will be followed in this thesis comprises:

Figure 1 SIX-STEP RISK MANAGEMENT MODEL FOLLOWED IN THIS THESIS	
1.	Determining the objectives of the business, or establishing the context.
2.	Identifying the risks to which the business is exposed by reference to the risk management objectives of the business.
3.	Analysing the identified risks.
4.	Evaluating and selecting risk management strategies.
5.	Implementing the selected risk management strategies.
6.	Monitoring and conducting an ongoing review of the risk management system implemented.

2.4 Developing a framework for legal risk management

Very little literature is available in relation to the application of risk management in the context of legal risk. Much of the literature available on the topic of law and risk focuses on the use of law to regulate or apportion risk[55] at a public policy level, or from a law and economics perspective[56], rather than how to apply risk management to identify and manage legal risks affecting a business. Also, there is a tendency by legal practitioners who employ risk management techniques to develop proprietary methodology which they are reluctant to disclose. For example two of the respondents to the survey who were partners in top tier law firms advised that they had developed a proprietary methodology for applying risk management in the context of legal risk, which they were not prepared to disclose.

Further, a distinction has to be made between the literature that examines certain legal risks, such as contractual risks associated with building construction contracts, but does not actually employ or advocate risk management methodology as a means of identifying and managing the legal risks. Such literature is quite common and can be confusing in that it adverts to or employs risk management terminology but does

---

55 See for example the series of papers in *Law and Uncertainty Risks and Legal Processes*, edited by Robert Baldwin with the assistance of Peter Cane, Kluwer Law International, London, 1997, Ch 1, p. 4, which examine the use of law as a means of regulating and apportioning risk at a public policy level.

56 See for example, Jason S Johnston, "Bayesian Fact-Finding and Efficiency: Toward an economic theory of liability under uncertainty", 61 *Southern California Law Review*, 1987, 137; Warren F Schwartz and C Frederick Beckner III, "Article: Toward a theory of the meritorious case": Legal uncertainty as a social choice problem", 6 *George Mason University* Law Review, Summer 1998, 801.

not actually refer to or apply risk management methodology[57]. One area, however, where risk management methodology is discussed as a means for identifying and managing one type of legal risk, contractual risk, has been in relation to government outsourcing and procurement[58].

It has therefore been necessary in this thesis to develop a framework for legal risk management largely by reference to the available literature on risk management methodology. What follows is an analysis of how risk management can be applied in the context of legal risk. This requires an examination of each of the steps involved in the risk management process in relation to how those steps can be undertaken in relation to legal risk. It also involves discussion of some risk management techniques and examining the extent to which these techniques can be used in relation to the identification and management of legal risk.

2.4.1 STEP 1: DETERMINING THE OBJECTIVES OF THE BUSINESS OR ESTABLISHING THE CONTEXT

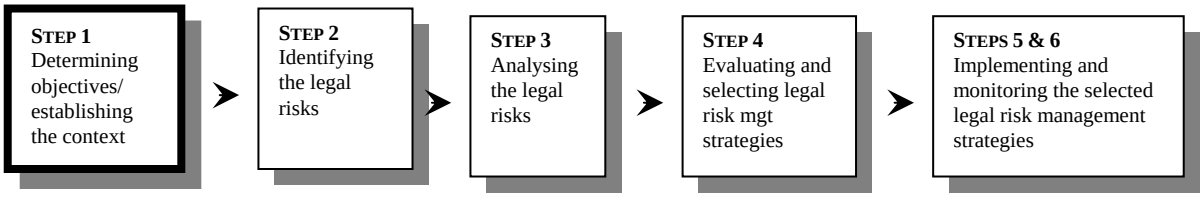
Figure 2 depicts step 1 of the risk management process as it applies in the context of legal risk.

---

[57] For example, in the Australian Law Reform Commission report, *Legal risk in international transactions*, Australian Government Publishing Service, Canberra, 1996, the terms "legal risk" and "risk management" are used yet risk management methodology is not expressly referred to or employed.

[58] See for example, Competitive Tendering and Contracting Group, Department of Finance and Administration, "Limitation of Liability and Risk Management", CTC Toolkits, http://www.ctc.gov.au/toolkits/liability/lia1.htm, last updated 19 April 1999; Competitive Tendering and Contracting Group, Department of Finance and Administration, *Competitive Tendering and Contracting*, Commonwealth of Australia, Parkes, ACT, March 1998.

Figure 2 LEGAL RISK MANAGEMENT: STEP 1



Whilst a risk management system ideally encompasses the entire range of risks which a business may encounter, in practical terms, it is impossible or, at the very least, not cost-effective for a business to undertake risk management in respect of the entire range of risks which it may face. Risk management therefore focuses on identifying those risks that, if they were to eventuate, would curtail or interfere with the business achieving its basic objectives[59]. It is important therefore for a business to specifically set out its risk management objectives as part of the risk management process.

Australian Standard *AS/NZS 4360 -1999 Risk Management* advocates that a business undertake what is described as "establishing the context" a similar, but broader exercise, part of which involves articulating the role and overall objectives of the business as well as the specific objectives of a business in relation to a particular activity[60]. "Establishing the context" encompasses several aspects including defining the "strategic context", the "organisational context", the "risk management context" and the "risk evaluation criteria" for the business. The "strategic context" is the

---

[59] Head and Horn, *Essentials of Risk Management*, http://www.bus.orst.edu/faculty/nielson/rm/chapter1.htm.

[60] See for example, paragraphs 4.1.1-4.1.6 of Australian Standard *AS/NZS 4360- 1999, Risk Management*, Standards Australia, Strathfield NSW, 1999.

relationship between the business and its internal and external environment. This includes: "…financial, operational, competitive, political (public perceptions/image), social, client, cultural and legal aspects of the organisation's functions"[61]. The "organisational context" equates to the business's objectives[62]. The "risk management context" refers to the scope and depth of the risk management process being applied [63].

Establishing the business's objectives or "establishing the context" should ensure that risk management is used effectively in relation to a business and outcomes that are inappropriate in the circumstances are avoided:

> The risk management process should begin at the strategic management level. By completion of the strategic aspect first it is possible to ensure that operational and transactional phases are accurately placed within the strategic context. Similarly transactional activity can be positioned within the operational context, provided this phase is undertaken after completion of the operational analysis. Misalignment can result in risk treatments which are inappropriate; eg., operational risk treatments which fail to address key elements of the organisation's strategic needs or transactional risk treatments which deal excessively with risks identified as acceptable at the operational level[64].

How are a business's objectives determined? Sources include the business's strategic plan, the annual report, the chief executive/ general manager, and the manager responsible for the particular activity for which risk management is being undertaken.

---

61 See paragraph 4.1.2 of Australian Standard *AS/NZS 4360- 1999*.
62 See paragraph 4.1.3 of Australian Standard *AS/NZS 4360- 1999*.
63 See paragraph 4.1.4 of Australian Standard *AS/NZS 4360-1999*.
64 Standards Australia/Standards New Zealand Joint Technical Committee on Risk Management, "A Basic Introduction to Managing Risk using the Australian and New Zealand Risk Management Standard - AS/NZS 4360: 1999", Master Draft as at 4/1/99 p. 15.

In relation to legal risk management, in addition to the broader objectives articulated by a business concerning its role and its overall objectives, the following specific objectives should be included: (a) to comply with any regulatory regime that governs the activities undertaken by the business (in order to avoid criminal prosecution), (b) to avoid exposure to immense civil liability both tortious and contractual as a consequence of the business's activities and (c) to protect a business's legal interests or entitlements in respect of any transactions undertaken by the business.

Whilst these specific objectives appear uncontroversial only a few academic commentators or practitioners (risk management and legal) have advocated *all* of these objectives in relation to legal risk management. Instead, there has been a tendency for writers to identify only one or at most two of the objectives referred to.

Based on a review of the literature on legal risk management there appear to be two views as to what constitutes the objectives of legal risk management. According to one view, the objective of legal risk management is to achieve compliance with the law[65]. An example of this view is reflected in Australian Standard *AS 3806 -1998*

---

[65] A typical example of this interpretation of "risk management" is illustrated by, Alan Ducret, 'Risk Management: the ACCC, the Trade Practices Act and a Practical Compliance Program', *Australian Company Secretary*, vol 49, no 11, December 1997, p 494. The author, a regional director of the ACCC uses the term "risk management" in the title but focuses solely on compliance with the Trade Practices Act 1974 (Cth). Other examples include: Nancy Milne, 'Fiduciary Issues: Compliance Systems- Risk Management in Due Diligence', *Australian Company Secretary*, vol 48 no 8, September 1996. The author, a partner in a law firm, uses the term "risk management" in the title but refers only to issues relating to compliance with the law; Similarly, Greg San Miguel, a partner in a law firm, describes legal risk management as "…a series of management strategies designed to engender, as an essential part of corporate culture, behaviours which comply with the law and protect the company against the risk of legal claims" in

Compliance Programs. Whilst purporting to set "the methods found most satisfactory in securing proper management of legal risks" [66] *AS 3806 -1998* in fact only refers to the objective of identifying and responding to breaches of laws, regulations, codes or organisational standards. This approach reflects only the first objective referred to in this thesis. Whilst it is difficult to generalise, given that there is very little literature on legal risk management, it appears that the focus on compliance only is prevalent amongst legal writers and practitioners and is reflected in the language typically used to describe this approach such as "legal compliance" and "legal compliance audits"[67]. (As will be discussed in more detail at 2.5 at p122 the term "compliance" is sometimes used more broadly to encompass not only the notion of regulatory compliance but also the protection of a business's legal rights and entitlements and avoidance of tortious and contractual liability. Thus, it may well be that legal writers and practitioners when using the term "compliance" use it in its broader meaning.)

The alternative view, a view tended to be promoted by risk management writers and practitioners, is to equate legal risk management with managing exposure to liability such as tortious and contractual liability. These writers therefore tend to

---

an advertorial in *Company Lawyer*, vol 13 no 1, February 1997, p 72. Again, the article focuses on compliance with the law.

66 Australian Standard *AS 3806-1998, Compliance Programs*, Standards Australia, Homebush NSW, 5 February 1998, para 1.1.

67 For example, the law firm Gilbert & Tobin markets its advice on the "legal risks and issues associated with the use of the Internet" as an "Internet Compliance Manual": http://www.gtlaw.com.au.

focus on the objective of avoiding and managing exposure to legal liability although some writers have also included the objective of regulatory compliance[68].

Neither view however commonly refers to the third objective described above, that is, to protect a business's legal rights or entitlements in relation to business transactions. For example, Australian Standard *AS/NZS 4360 -1999 Risk Management*, a standard developed largely by parties with backgrounds in risk management, when setting out suggested applications in which it would be appropriate to use *AS/NZS 4360 -1999* refers to "legislative compliance" and "general liability" but does not expressly refer to the protection of a businesses legal rights and interests in respect of business transactions[69]. Similarly, articles authored by legal practitioners do not commonly refer to the third objective[70] although a promotional brochure of a top tier Australian law firm alludes to this third objective when describing its view of what constitutes legal risk management[71]. Interestingly, however, the risk management literature on the specialised topic of derivative risk management consistently identifies legal risks which fall within the third objective,

---

68 See for example, Neil Crockford, *An Introduction to Risk Management*, 2nd Edition, Woodhead-Faulkner, Cambridge, 1986, Ch 17, pp 92-97 although Crockford also devotes a chapter on environmental pollution law compliance at pp 98-102 and Emmett J Vaughan, *Risk Management*, John Wiley & Sons, Inc, New York, 1997, Ch 23, pp 510-536. See also Jeffrey P Altman, 'Managing Legal Risks', *Association Management*, Jan 1998, v 50 n 1 pp 67-69 which focuses on avoiding the risk of liability when describing legal risk management.

69 See appendix A of Australian Standard *AS/NZS 4360- 1999, Risk Management*, Standards Australia, Strathfield NSW, 1999.

70 For example, none of the articles referred to in footnote 65, which were authored by legal practitioners, identified that an objective of legal risk management is to protect a business's legal rights or entitlements in relation to business transactions.

71 A brochure highlighting the National Legal Risk Management Group of the law firm Freehill Hollingdale & Page notes that: "Freehills Legal Risk Management goes beyond the "compliance square". It is a total approach to managing and protecting an organisation's assets and reputation.", http://www.fhp.com.au/npg/groups/legalleft.htm.

described above[72], such as the risk that a contract cannot be legally enforced due to insufficient documentation or insufficient legal authority of a transacting party, but, presumably due to the nature of the legal risks associated with derivatives trading, the other two objectives referred to in this thesis are not commonly identified.

Perhaps the reason for the failure by many commentators to include all three objectives when describing risk management in the context of legal risk is that historically, risk management evolved from the techniques used by insurance managers for measuring risk and there was a tendency of risk managers to view legal risk in terms of exposure to civil liability and liability arising from regulatory non-compliance. Also, at least in the literature, legal practitioners and writers appear to have equated legal risk management with the concept of compliance, which, in its narrow meaning, focuses on compliance with regulatory frameworks as opposed to managing exposure to civil liability or the protection of a business's rights and interests, although it is difficult to generalise. An alternative explanation is that in the limited instances that legal risk management has been used in the past it has been used in relation to businesses that are subject to considerable government regulation such as businesses that are subject to environmental regulation or trade practices and

---

[72] There is abundant literature available on the use of risk management for derivative risk. It is not possible here to list all such literature. By way of example only, the following literature on derivative risk identifies legal risks that fall within the third objective, such as the risk that a contract cannot be legally enforced due to insufficient documentation or insufficient legal authority of a transacting party: Brandon Becker and Francois-Ihor Mazur, "Symposium: Derivative Securities: Risk Management of Financial Derivative Products: Who's responsible for what?", 21 *Iowa Journal of Corporation Law* 177; Adam R Waldman, "Comment: OTC Derivatives & Systemic Risk: Innovative Finance or the Dance into the Abyss, 43 *American University Law Review* 1023, Spring 1994; International Finance & Commodities Institute, Introduction to Risk Management website: http://risk.ifci.ch/OtherRisks.htm.

consumer protection legislation and this may have caused a perception to arise that legal risk management is simply the same as developing and implementing a compliance program, which is supported by the observation that when legal risk management is applied to a business activity that is largely transactional in nature, such as derivative risk management, the third objective is identified. This explanation gains some support from the fact that in relation to activities where regulation is less of an issue than the potential for tortious or contractual liability or the risk that a business's intellectual property is infringed the objectives of avoiding immense tortious or contractual liability or protecting a business's legal rights and entitlements are more likely to be identified as objectives of the legal risk management process. Whatever the reasons, legal risk management can and should be used to achieve all three objectives referred to.

Determining a business's objectives or "establishing the context" involves not only considering a business's strategic objectives but also setting the business's risk criteria. Setting the business's risk criteria involves setting risk benchmarks, or, as *AS/NZS 4360 -1999 Risk Management* calls it, "risk evaluation criteria", signifying a business's policy on the risk management process, such as the level of risk that is acceptable and unacceptable (this criterion is expressed broadly and it is not essential at this stage to comprehensively set out what is acceptable and what is unacceptable to the business as this step is considered in step 3 of the risk management process when each risk is evaluated) and establishing the resources and costs the business is prepared to expend to undertake risk management. When setting a business's risk

criteria it may be relevant to identify the business's stakeholders (for example, the business's customers, suppliers, community groups, union representatives, individuals affected or perceived to be affected by the business's activities, employees and regulators) and determine stakeholder requirements, which in turn can be incorporated into the business's risk criteria[73]. It is also relevant when setting a business's risk criteria to consider, not only economic factors but also technical (eg is the activity environmentally acceptable, operationally safe?) and socio-political factors (eg. is the activity acceptable to the general public and to employees?)[74].

In relation to legal risk management it is important to consider and decide what are acceptable levels of risk in relation to the three major types of legal risk a business may face. These are the legal risks associated with statutory non-compliance, the legal risks resulting in exposure to tortious and contractual liability, and the legal risks associated with failure to adequately protect a business's legal rights and interests. Thus it is necessary to determine what level of exposure to tortious and contractual liability is acceptable to the business. Does the business seek to avoid any exposure to tortious and contractual liability, or is it acceptable to accept exposure up to a specified dollar value? In relation to the business's legal rights and interests, will all interests be sought to be protected or simply the key rights and interests? Similarly, is absolute compliance with statutory and regulatory frameworks achievable? In relation to this consideration, it should be noted that failure to achieve

---

[73] Standards Australia/Standards New Zealand Joint Technical Committee on Risk Management, p. 18.

[74] John C Chicken, *Risk Handbook*, International Thomson Business Press, London, 1996, p 198.

absolute compliance could expose the business to consequences that may not be acceptable, such as prison sentences for managers, directors and other employees or huge penalties. A business must consider carefully the potential consequences of choosing not to aim for absolute statutory compliance. Also, consideration should be paid to what level of compliance would be sufficient to constitute a defence in the event that a business is charged with statutory non-compliance. Some statutes provide for a defence to a prosecution arising from statutory non-compliance on the basis that the defendant exercised due diligence in seeking to comply with the law. This defence is typically proved by the defendant establishing that an effective system was in place for ensuring statutory compliance. In addition, where a defence of due diligence is not laid down in a statute, the courts have recognised that, where there is an effective system in place for ensuring compliance, this factor will be taken into account when imposing penalties for statutory non-compliance. Clearly it would be prudent for the business to set a level of risk that falls within what either the courts or the statute itself has laid down as a standard comprising effective due diligence. It is beyond the scope of this thesis to consider what standard is acceptable to fall within a due diligence defence for the various statutes that regulate a business that conducts Internet commerce.

Setting risk criteria enables disparate risks to be assessed consistently as risks are assessed and risk management strategies are developed against the same risk criteria. In addition, the use of risk criteria reduces the extent to which assessments of risk and risk management strategies are affected by individual bias or unnecessary subjectivity

by again requiring reference to be made to the risk criteria set by the business when such assessment are being made[75].

Set out below is a checklist for Step 1 of the legal risk management process:

Table 10 CHECKLIST FOR STEP 1 OF THE LEGAL RISK MANAGEMENT PROCESS DETERMINING THE OBJECTIVES OF A BUSINESS OR "ESTABLISHING THE CONTEXT"

1. Determine the business's "strategic context".	What is the relationship between the business and its internal and external environment, such as, the financial, operational, competitive, political, social, clients, cultural and legal aspects of the business's functions? This process can involve communicating and consulting with the business's stakeholders.
2. Determine the "organisational context" of the business.	What are the business's objectives? In relation to legal risk management, in addition to the broader objectives articulated by a business concerning its role and its overall objectives, the following specific objectives should be included: ♦ to comply with any regulatory regime that governs the activities undertaken by the business (in order to avoid criminal prosecution); ♦ to avoid exposure to immense civil liability both tortious and contractual as a consequence of the business's activities and; ♦ to protect a business's legal interests or entitlements in respect of any transactions undertaken by the business. This may involve communicating and consulting with the business's stakeholders.
3. Determine the "risk management context".	What is the scope and depth of legal risks that will be reviewed? Also, determine what level of risk is

[75] The Auditor-General Performance Audit, *Risk Management Australian Taxation Office*, Commonwealth of Australia, Audit Report No. 37, 1996-1997, para 4.4.

	acceptable and unacceptable to the business, that is, set the business's risk criteria. It is not essential at this stage to comprehensively set out the business's risk criteria. When setting a business's risk criteria factors to take into account include: economic factors (what is the level of loss that the business can afford?), technical factors (eg is the activity environmentally acceptable?, operationally safe?) and socio-political factors (eg. is the activity acceptable to the general public and to employees?) In addition, the business should consider and decide what are acceptable levels of risk in relation to: ♦ the legal risks associated with statutory non-compliance; ♦ the legal risks resulting in exposure to tortious and contractual liability; ♦ the legal risks associated with failure to adequately protect a business's legal rights and interests. This step will involve communicating with internal (eg upper management, managers, employees), and perhaps external, stakeholders of the business. External stakeholders that may be consulted include: the business's customers, suppliers, community groups, union representatives and regulators)
4. Document this step.	See sample document set out at Table 11 at p 49.
5. Monitor and review.	The outcome of this step should be periodically reviewed to ensure that the legal risk management system implemented reflects the business's current legal risk management objectives and risk criteria.

The following is a sample Risk Register for documenting step 1 of the legal risk management process:

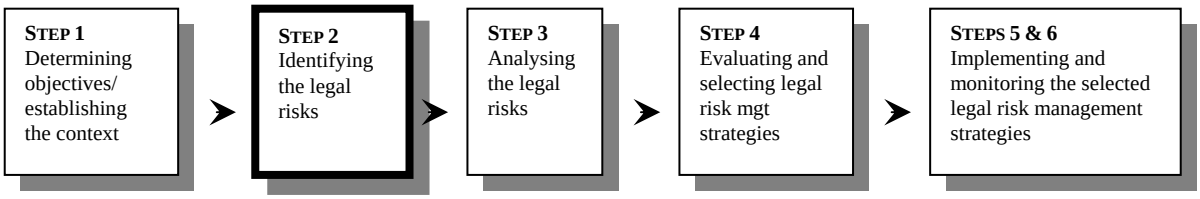
Table 11 SAMPLE RISK REGISTER FOR STEP 1 OF THE LEGAL RISK MANAGEMENT PROCESS

RISK REGISTER (PART 1 OF 4) Date of this Review: Next Review Date: Compiled by: Approved/Reviewed by:	Date:
The strategic context for the business:	
The organisational context for the business: The general objectives for the business are: The legal risk management objectives are:	
	♦ to comply with any regulatory regime that governs the activities undertaken by the business (in order to avoid criminal prosecution); ♦ to avoid exposure to immense civil liability both tortious and contractual as a consequence of the business's activities and; ♦ to protect a business's legal interests or entitlements in respect of any transactions undertaken by the business. [other legal risk management objectives]
The risk management context for the business: What legal risks will the business focus on (trade practices, intellectual property, contractual, product liability, criminal liability, statutory non-compliance)?:	
The risk criteria for the business (list financial, economic, technical and socio-political criteria):	
Internal stakeholders consulted:	
External stakeholders consulted (if relevant):	

2.4.2 STEP 2: IDENTIFYING THE RISKS BY REFERENCE TO THE RISK MANAGEMENT OBJECTIVES OF THE BUSINESS

Figure 3 depicts step 2 of the risk management process as it applies in the context of legal risk.

Figure 3 LEGAL RISK MANAGEMENT: STEP 2



The second step of risk management is to identify the aspects of a business's activities that may result in exposure to significant loss **("risks")**. The types of loss with which risk management is concerned includes property loss (including loss of tangible and intangible property), income loss or loss to earnings, liability and personal injury[76]. Risk management can be used in relation to all types of risks facing a business[77], although some writers prefer to exclude its application in relation to speculative risks[78]. Risks are categorised in a number of ways, some of which overlap. Thus, depending on how risk is classified, risk management can be applied in relation to pure risks (risks, which if they eventuate will result in a loss such as

---

[76] Head and Horn, *Essentials of Risk Management*, http://www.bus.orst.edu/faculty/nielson/rm/chapter1.htm.

[77] See for example Crockford, at p 3 and 6 who argues that risk management can and should be applied to a wide range of risks including pure and speculative risks.

[78] See for example, Vaughan, p 21 who refers to risk management analysis as a tool for managing pure risks.

property damage or loss of income due to death or injury of a key employee[79]), speculative risks (risks, which if they eventuate can result in loss or a gain, such as risks relating to marketing, production and finance decisions[80]), static risks (risks associated with purely random occurrences also classified as pure risks[81]) and dynamic risks (risks resulting from a changing economy. Such risks are also classified as speculative risks[82]), fundamental risks (risks that are economy wide or systematic such as inflation, earthquake, war and floods[83]) or particular risks (risks that are unique to individuals or are unsystematic in nature. These risks can be static or dynamic). Classification of risks is necessary because, in general, it is not possible to obtain insurance for speculative risks and, even in relation to pure risks, insurers may only be willing to insure particular classes of pure risk. Legal risks of the kind that, if they eventuate, result in liability are characterised as pure risks[84] and it is likely that other types of legal risks such as those that involve non-compliance with a regulatory framework and those legal risks that involve the failure to protect a business's legal rights will also be characterised as pure risks.

2.4.2.1 What constitutes a legal risk?

Before considering the techniques used in risk management to identify risk and the extent to which such techniques can be used to identify legal risk it is necessary to

---

79 Robert I Mehr and Bob A Hedges, *Risk Management in the Business Enterprise*, Richard D Irwin Inc, Homewood Illinois, 1963, Ch 1, pp 10-11.
80 Mehr and Hedges, p 5.
81 Mehr and Hedges, pp 8-9.
82 Mehr and Hedges , p 3.
83 Vaughan, p 15.
84 Vaughan, p 16.

consider what is meant by the term "legal risk". There are two possible definitions of legal risk. The first definition of legal risk focuses on what causes a business to incur a "legally related loss", that is what is the origin of a legally related loss. On this view, an example of a legal risk is: the risk that a party takes legal action against the business for tortious or contractual liability. Other examples are: the risk that a regulatory agency prosecutes the business for regulatory non-compliance, or the risk that a party infringes a business's legal rights and interests.

The alternative definition of legal risk focuses on the conditions or circumstances of the law, whether it be statute or common law, that make a "legally related loss" likely or more severe. For example: the risk that a business fails to protect its legal rights and interest, which increases the likelihood that a party can legally "infringe" those legal rights and interests; or the risk that a business fails to ensure that its conduct is not wrongful, which increases the likelihood that the business will have a claim brought against it that is successful[85].

So what type of legal risk should risk management be concerned with? The first definition of legal risk, which focuses on the *cause* of a "legally related loss", is considered in risk management theory to constitute a *"peril"*. Typical "perils" include "fire", "cyclones" or "theft". The second definition of legal risk, which focuses on the *conditions or circumstances that make a loss likely or more severe*, is considered in risk management theory to refer to a *"hazard"*. Hazards are in fact "a

---

[85] George L. Head & Stephen Horn II, *Essentials of the Risk Management Process*, Volume II, Insurance Institute of America, Inc, 1985, Malvern, PA, USA, Chapter 5, p 225.

condition that may create or increase the chance of a loss arising from a given peril"[86]. According to risk management theory, the type of legal risk that risk management is directed at is the legal risk that constitutes a hazard not a peril:

> Regarding liability losses, wrongful conduct that good risk management strives to minimize is really a hazard, not a peril. …[A] hazard is a condition or circumstance that makes a loss more likely or more severe. Wrongful conduct increases the likelihood that an organization will have a claim brought against it and that any suit will be successful. (Similarly, failing to maintain good records documenting legally required conduct or failing to retain good legal counsel are also hazards). Legally proper conduct does not remove the liability peril. It only reduces some liability hazards.[87]

For this reason, the discussion in this thesis uses the second definition of legal risk rather than the first.

2.4.2.2 Techniques for identifying legal risk

Having defined legal risk, it is now convenient to consider the various techniques used for identifying risk and to examine the extent to which they can be used to identify legal risk.

Several methods are used in risk management for identifying risk including:

> …(1) completing a survey/questionnaire for the organization; (2) reviewing loss histories of this and comparable organizations; (3) analyzing its financial statements and accounting records; (4) reviewing the organization's other records and documents; (5) constructing flowcharts of the organization's operations; (6) personally inspecting its facilities; and (7) consulting with experts within and outside the organization.[88]

Australian Standard *AS/NZS 4360 -1999 Risk Management* lists advocates the following approaches to identifying risk:

---

86 Vaughan, p 12.
87 George L. Head & Stephen Horn II, *Essentials of the Risk Management Process*, p 225.
88 George L Head and Stephen Horn, *Essentials of Risk Management*, http://www.bus.orst.edu/faculty/nielson/rm/chapter1.htm.

> Approaches used to identify risks include checklists, judgements based on experience and records, flow charts, brainstorming, systems analysis, scenario analysis and systems engineering techniques. The approach used will depend on the nature of the activities under review and the types of risk[89].

The *Guidelines for Managing Risk in the Australian Public Service* list several techniques for identifying risk:

> [I]nterview/focus group discussion; personal experience or past agency experience; audits or physical inspection; brainstorming; survey, questionnaire, Delphi technique; examination of local or overseas experience; judgmental-consensus, speculative/conjectural, intuitive; history failure analysis; scenario analysis; decision trees; strengths, weaknesses, opportunities and threats (SWOT) analysis; flowcharting, system design review, systems analysis, systems engineering techniques, for example, Hazard and Operability (HAZOP) studies; work breakdown structure analysis; [and] operational modelling.[90]

The Commonwealth Government's *Managing risk in procurement*-A handbook lists the following techniques for identifying risks associated with procurement:

> Consulting previous risk analyses and reference lists, using the knowledge and expertise of your team, brainstorming (imagining everything that could happen during the procurement), generating event tree analyses, referring to existing checklists and reference list and checking that you have identified the stages in the procurement process that are significant for your transaction[91].

The methods described of identifying risk are equally useful for identifying a business's exposure to legal risk. For businesses who have only recently commenced operations or businesses who have not been exposed in the past to legal risks it may be necessary to examine what legal risks other businesses engaged in similar

---

89 *AS/NZS 4360- 1999, Risk Management*, para 4.2.4.

90 *Guidelines for Managing Risk in the Australian Public Service*, p 23.

91 Purchasing Australia, *Managing risk in procurement- A handbook*, Australian Government Publishing, p 18.

activities have faced, a technique that is advocated in the risk management literature in such instances.

Another method of risk identification used in risk management risk in relation to businesses involved in production is to construe a business's activities as an energy chain that involves the redistribution of energy. Risks are identified by categorising the business's operations according to which activities entail the release of energy and identifying how each activity could go wrong and what loss could as a consequence ensue[92]. This technique could also be useful for identifying legal risks where a business is undertaking production type activities.

An additional method of identifying risk used in risk management is to view the organisational structure of a business and from it investigate each division (eg department or section) with a view to identifying those risks that may impede the operations/activities undertaken by that division[93]. This approach could also be used in relation to the identification of legal risk.

Another method used to identify risk is to consider who the "stakeholders" of the business are and then identify how the business can incur loss as a consequence of undertaking activities that affect the "stakeholders". A business's "stakeholders" are those parties who will be affected by or who are potentially affected by risk management decisions made or, more broadly the activities undertaken by a

---

92 Crockford, p 21.
93 Crockford, p 21.

business[94]. A business therefore can have a wide range of "stakeholders" including customers, suppliers, shareholders, investors, community groups, state and federal regulatory agencies, groups representing geographical regions, representatives of different cultural economic or ethnic groups, consumer rights organisations and trade associations[95]. Once the "stakeholders" are ascertained, the risks facing a business are identified by examining how each category of "stakeholder" can be adversely affected by an activity undertaken by the business or what actions the "stakeholder" may take against a business in relation to the activities undertaken by the business. This approach could also be used in relation to the identification of legal risk. For example, some contractual risks faced by a business can be identified by examining the contracts entered into by the business with "stakeholders" with a view to eliciting the expectations of the "stakeholder" and pinpointing areas which may be the basis of dispute between the business and the "stakeholder"[96]. In this way the contractual risks associated with transacting with a particular category of "stakeholder" can be identified. The "stakeholder" approach advocated by the Presidential/Congressional Commission on Risk Assessment and Risk Management in relation the use of risk management principles by regulatory agencies differs in that the Commission

---

94 The Presidential/Congressional Commission on Risk Assessment and Risk Management, *Risk Assessment and Risk Management in Regulatory Decision-Making*, Final Report Volume 2 1997, p 16 and e-mail correspondence dated 22 September 1998, with Mr Rick Davis, Director of Business Development and Security Strategy of Network Risk Management Services Inc (at that time), a company that provides risk management services.

95 The Presidential/Congressional Commission on Risk Assessment and Risk Management, p 16 and e-mail correspondence dated 22 September 1998, with Mr Rick Davis, Director of Business Development and Security Strategy of Network Risk Management Services Inc (at that time), a company that provides risk management services.

96 E-mail correspondence dated 22 September 1998, with Mr Rick Davis.

suggests identifying the business's stakeholders in order to then involve them in the decision-making process[97]. Given the cost associated with such involvement it is unlikely that such approach would be adopted by a private sector business except perhaps large corporations.

In relation to methods aimed at specifically identifying legal risk, Australian Standard *AS 3806 - 1998 Compliance Programs* advocates identification of the legal risks associated with statutory non-compliance (legal risks associated with non-compliance with the law) by seeking advice from legal advisers; being on relevant regulators' mailing lists; membership of professional groups, subscribing to relevant information services; and attending industry forums and seminars[98]. These methods enable a business to identify the legislation that governs the activities it undertakes and in turn identify the legal risks associated with statutory non-compliance. These methods could also be useful for achieving not only the compliance objective of legal risk management but all three objectives earlier expounded, that is legal compliance, avoidance of immense civil liability and avoidance of loss of legal rights or entitlements.

It is suggested that there is a further method for identifying legal risk and that is for a business or its legal advisers, in addition to identifying the relevant legislation that governs the business's activities, to conduct a through review of the case law, if any, that has arisen in respect of the types of activities that the business undertakes.

---

97 The Presidential/Congressional Commission on Risk Assessment and Risk Management, pp 16-19.

98 Australian Standard *AS 3806-1998 Compliance Programs*, para 3.3.1.

Thus, if a business is engaged in Internet commerce a review of the case law relating to the conduct of Internet commerce will reveal some legal risks other businesses conducting Internet commerce have been exposed to.

Finally, another method for identifying legal risk is to review the various international organisation reports (such as the OECD, European Commission), national government reports that have been written in relation to various commercial activities. For example, in the context of Internet commerce there are several OECD reports, European Commission reports and Directives and national reports of the Australian Commonwealth government and other countries that have been written in regard to developing a framework for electronic commerce. Whilst these reports may not be exclusively concerned with Internet commerce or the legal aspects of conducting commerce, most at the very least advert to the regulatory issues associated with the conduct of Internet commerce. Thus, such reports are useful in identifying the legislation that governs a business's commercial activities on the Internet and is useful for anticipating future legislation that regulates a business conducting commerce on the Internet. This in turn enables the identification of the compliance related legal risks associated with Internet commerce.

Set out in Table 12 is a checklist for step 2 of the legal risk management process:

Table 12 Checklist FOR STEP 2 OF THE LEGAL RISK MANAGEMENT PROCESS

IDENTIFYING THE LEGAL RISKS TO WHICH THE BUSINESS IS EXPOSED

1. Select technique/s for identifying legal risk:	♦ Review of relevant legislation and voluntary codes of conduct. Legislation that will typically be relevant includes:

	Trade Practices Act 1975 (Cth), Consumer Credit Code and State Fair Trading Acts. ♦ Review of relevant case law. ♦ Advice from legal advisers. ♦ Review international organisation reports, government and agency reports and other literature. ♦ Undertake a legal compliance survey /questionnaire or using legal checklists or legal audits. ♦ Construct flowcharts of the business's organisational structure. ♦ Review loss histories of the business and comparable businesses. ♦ Analyse the business's financial statements and accounting records. ♦ Review the business's other records and documents. ♦ Inspect the business's facilities. ♦ Consult with experts within and outside the organization. ♦ Being on relevant regulators' mailing list, membership of professional groups, subscribing to relevant information services and attending industry forums and seminars including subscribing to e-mail list groups and subscribing to on-line web sites that provide information concerning the legal risks. ♦ Stakeholder Definition Process (define dependent relationships). ♦ Judgments based on experience, brainstorming or intuition. ♦ Using systems analysis, scenario analysis, strengths, weaknesses, opportunities and threats (SWOT) analysis, systems engineering techniques, energy chain analysis or constructing flowcharts of the business's operations.

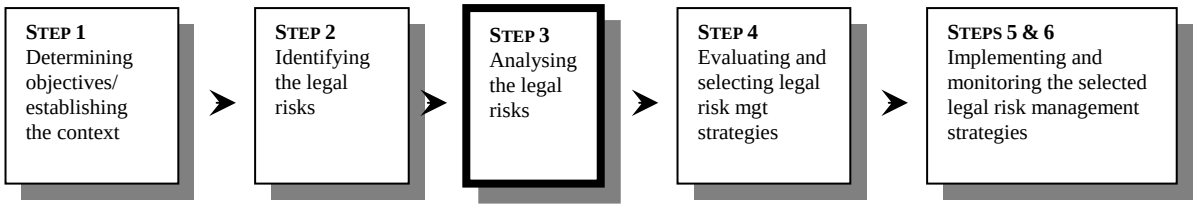
2. Identify legal risks: [The scope and depth of this process should reflect that which was set out in Step 1 of the legal risk management process]	
4. Document this step.	See sample document set out at Table 25 at p 94. This document combines steps 2 and 3 of the legal risk management process.
5. Monitor and review.	The outcome of this step should be periodically reviewed to take into account new legal risks that arise and to eliminate legal risks that no longer affect the business.

A sample Risk Register for documenting step 2 of the legal risk management process is set out in Table 25 at p94.

2.4.3 STEP 3: ANALYSING THE IDENTIFIED RISKS

Figure 4 depicts step 3 of the risk management process as it applies in the context of legal risk.

Figure 4 LEGAL RISK MANAGEMENT: STEP 3



The third step of risk management is to analyse each risk. During this process each identified risk is analysed by reference to a number of factors such as the type of loss that the risk poses (eg loss of property, net income loss, liability loss or personal loss), the circumstances which cause exposure to the loss, the frequency or

probability that such risk will eventuate, the extent of the loss should it eventuate[99] and the extent to which a loss will substantially interfere with a business's ability to achieve its objectives.

2.4.3.1 Techniques for analysing risk

Several methodologies are employed to analyse risk. One author has suggested that they can be categorised as follows: those risk analysis methodologies that take a technical perspective, those risk analysis methodologies that take an economic perspective, and those risk analysis methodologies that take a psychological perspective[100]. The methodologies for analysing risk that fall into the technical perspective category include: the actuarial approach, the toxicological and epidemiological approach and the engineering or 'probabilistic' approach:

> The actuarial approach looks to relative frequencies of events amenable to 'objective' observation (eg, fatalities) and assess probabilities by extrapolating from statistical data on past events. Such an approach demands that there be enough data to allow predictions to be made and it presupposes stability in the relationships between the events at issue and the factors that give rise to these.
>
> The toxicological and epidemiological approaches resemble actuarial analysis but employ different methods of calculating probabilities of undesirable effects. Thus, in epidemiological studies populations exposed to a risk are compared to control populations and attempts are made to quantify relationships between risk agents (eg, ionizing radiation) and physical harms.
>
> The engineering or 'probabilistic' approach attempts to assess the probability of failures in complex systems even in the absence of sufficient data for the system a whole. Fault-tree or event-tree analyses are employed in an attempt to evaluate the failure probabilities for each component in the tree. All such

---

99 Head and Horn, *Essentials of Risk Management,* http://www.bus.orst.edu/faculty/nielson/rm/chapter1.htm.

100 Robert Baldwin, "Risk: The Legal Contribution", in *Law and Uncertainty Risks and Legal Processes,* edited by Robert Baldwin with the assistance of Peter Cane, Kluwer Law International, London, 1997, Ch 1, p. 4.

> probabilities are then synthesized in order to model the failure rate of the whole system.
>
> Such technical approaches anticipate harms, average events over time and space and use relative frequencies in order to specify pro abilities. They are generally associated with the view that decisions about risks can be made on the basis of objective evidence that can be treated mathematically and can produce a numerical result[101].

The economic perspective has been described as follows:

> The economic perspective on risk transforms undesired effects into subjective utilities so that the currency of personal satisfaction allows direct comparisons between risks and benefits across different options. This, in turn, allows such analyses to be integrated into decision processes in which costs and benefits are assessed and compared an in which the ultimate goal is the allocation of resources so as to maximise their utility for society[102].

The economic perspective therefore involves quantifying the costs of minimising each identified risk and determining whether the benefit of implementing strategies to minimise a given risk outweigh the costs of minimising the risk.

Finally, the psychological approach has been described as follows:

> The psychological approach focuses upon individual cognition and such questions as how probabilities are perceived; how personal preferences relating to risk can be accounted for; and how contextual variables shape individual risk estimations and evaluations. … several factors … have been identified as affecting perceived seriousness of risks, including catastrophic potential, degree of personal control over the magnitude or probability of the risk, familiarity with the risk, degree of perceived equity in sharing risk and benefits, visibility of the benefits of risk taking, potential to blame risk creators, delay in the manifestation of any consequences, and voluntariness with which the risk is undertaken. Such an approach holds risk to be a multi-dimensional concept that cannot be reduced to a mere product of probability and consequences[103].

---

[101] Baldwin, p. 4.
[102] Baldwin, p. 4.
[103] Baldwin, p. 8.

Each of these methodologies has been subject to criticism[104] but it is beyond the scope of this thesis to consider them. The advantages and disadvantages of the various methodologies employed to analyse risk is relevant when risk management is being used to determine public and social policy, as it has been argued that each approach reflects various biases[105] and that these factors should be recognised in the formulation of social and public policy and any regulatory approach taken as a consequence. As this thesis is concerned with the use of risk management by individual businesses rather than the use of risk management to formulate social and public policy, it is not necessary to distinguish and comment on the various approaches to analysing risk in any great detail.

As noted earlier, the risk management model used in this thesis is largely the model put forward by the Australian Standard *AS/NZS 4360 -1999 Risk Management.* The method for analysis of risk advocated by Australian Standard *AS/NZS 4360 - 1999 Risk Management*, and many risk management texts, is to analyse a given risk is by reference to the *consequences* and the *likelihood* of a risk eventuating. This methodology arguably falls into the technical perspective category although the method advocated by Australian Standard *AS/NZS 4360 -1999 Risk Management* by which risk management strategies are selected also resembles the economic perspective. So how can *consequences* and *likelihood* of risk be measured? There are numerous techniques that a business can choose from to analyse the consequence and

---

104 See for example, the discussion at pp 4-10 in Baldwin.
105 See for example, the discussion at pp 4-10 in Baldwin.

likelihood of risk. It is not proposed to examine each and every technique used in risk management for measuring these factors, as many techniques are inapplicable or inappropriate to use in the context of legal risk. To illustrate this point it is necessary to consider, albeit at an elementary level, the methods used for analysing risk in risk management. The consequence and the likelihood of a risk eventuating can be analysed quantitatively or qualitatively and, in many circumstances, an assessment may be based on both qualitative and quantitative analyses. It should be emphasised that risk management theory encompasses both quantitative and qualitative risk analysis and the extent to which each technique is used will differ according to the discipline in which risk management is being utilised. For example, in relation to financial portfolio risk management a heavy emphasis is placed on quantitative analysis.

2.4.3.2 Quantitative analysis of risk

There are several techniques used for analysing risks quantitatively including statistical analysis models to calculate the frequency of loss or the distribution of severity; decision analysis models, such as the use of algorithms; the use of a means-end chain; the decision matrix; decision trees; stochastic decision tree analysis; Bayesian theory; stochastic decision tree analysis; multi-attribute value theory; sensitivity analysis; Monte Carlo simulation; portfolio analysis; stochastic

dominance[106] ; multi-variate analysis[107] and fuzzy analysis[108]. One quantitative technique that is particularly considered to be useful is the Poisson distribution, which can be used to estimate the probability of several risks occurring[109]. Other authors, however, have argued that Monte Carlo simulation is the best model to use for analysing risks quantitatively[110]. Quantitative analysis techniques are typically used by the insurance industry in relation to risks about which statistical data has been and continues to be routinely collected, such as asset loss. In addition, quantitative techniques are used extensively in the financial sector especially in relation to derivative risk management, as well as in relation to securities risk management. Quantitative techniques are also used in relation to project risk management.

Several software applications are now available that analyse risk quantitatively. In relation to non-legal risks such software is used extensively by insurance professionals. For example, an E-business Risk Management Professional, states that as part of the risk analysis process he uses a proprietary premium underwriting software "based on relative loss expectancies, experience modifications and other basic insurance industry underwriting mechanisms" to calculate how much insurance

---

106 See for example, Peter G Moore, *Risk in Business Decisions*, Longman, London, 1972, for detailed illustrations of how statistical decision analysis can be used to provide a quantitative assessment of identified risks.

107 John C Chicken, *Risk Handbook*, International Thomson Business Press, London, 1996, pp 240-246.

108 Chicken, pp 240-246.

109 Crockford, p 29.

110 See for example, David Vose, *Quantitative Risk Analysis: A Guide to Monte Carlo Simulation Modelling*, John Wiley & Sons, Chichester, 1996 who argues that Monte Carlo simulation is the better model for analysing risk.

premiums are likely to cost[111]. There are even software applications that purport to be useful for analysing legal risks[112].

As will be discussed later in this chapter, there is little statistical data available in relation to legal risks (at least in Australia) and for this reason, it may not be possible that a purely quantitative analysis of a given legal risk can be undertaken. However, some some types of legal risk can be evaluated quantitatively and one risk manager reports that that he uses quantitative techniques when he evaluates legal risks that are non-compliance related because "qualitative approaches to measurement are very difficult conceptually for clients to relate to"[113]. Another risk manager states that he uses quantitative methods in respect of some aspects of legal risk, "to carry out discrete statistical analysis to isolate particular sub-disciplines and individual instance, case, lawyer, counsel, dollar value etc"[114]. The techniques used to undertake quantiative analysis of legal risk are diverse including:

---

111 Response dated 20 January 2000 to a self-completion questionnaire enquiring how the participant uses management methodology in the context of legal risk. Participants' names have not been disclosed to honour a request of some participants to remain anonymous. All responses are available on file.

112 See, for example, the web site of Litigation Risk Analysis, Inc at http://www.litigationrisk.com which provides software that uses "structured and programmed decision trees" to analyse legal claims quantitatively. The company also provides training and consulting services in relation to the method and software used to analyse legal risks in this way.

113 Response dated 24 November 1999 to a self-completion questionnaire enquiring how the participant uses management methodology in the context of legal risk. Participants' names have not been disclosed to honour a request of some participants to remain anonymous. All responses are available on file.

114 Response dated 8 December 1999 to a self-completion questionnaire enquiring how the participant uses management methodology in the context of legal risk. Participants' names have not been disclosed to honour a request of some participants to remain anonymous. All responses are available on file.

> Different types of standard numerical and logic simulation modelling, fault tree analysis, critical path and PERT analysis. This includes mathematical financial modelling tools[115].

Similarly, the National Legal Risk Management Co-ordinator of a top tier law firm states that in some instances a quantitative analysis of a legal risk can be made:

> The extent of our quantitative analysis is usually limited to surveys and audits and analysis of the results. We have a computer based self assessment survey that is sent to executives in the client organisation and the results are collated by the program and broken down into a wide range of statistics that are presented in a pie chart form to show patterns etc[116].

2.4.3.3 Qualitative evaluation of risk

If a risk cannot be analysed by means of quantitative analysis the risks must be analysed qualitatively. That is, a reasonable and defensible judgment of the frequency and severity of the risk should be undertaken. Australian Standard *AS/NZS 4360 - 1999 Risk Management*[117] suggests a qualitative approach to risk analysis that first involves ascribing to each risk a description of the likelihood of it eventuating. The number of categories and descriptions used will vary according to the needs of the risk management being undertaken[118]. The Australian Standard *AS/NZS 4360 -1999 Risk Management* provides the following model scale for classifying likelihood or frequency of risk:

---

115 Response dated 8 December 1999 to a self-completion questionnaire enquiring how the participant uses management methodology in the context of legal risk. Participants' names have not been disclosed to honour a request of some participants to remain anonymous. All responses are available on file.

116 Response dated 7 December 1999 to a self-completion questionnaire enquiring how the participant uses management methodology in the context of legal risk. Participants' names have not been disclosed to honour a request of some participants to remain anonymous. All responses are available on file.

117 See appendix E, *AS/NZS 4360- 1999, Risk Management*.

118 See appendix E, *AS/NZS 4360- 1999, Risk Management*.

Table 13 *AS/NZS 4360 - 1999, RISK MANAGEMENT*[119] SCALE FOR CLASSIFYING LIKELIHOOD OR FREQUENCY OF RISK	
Descriptor	Example description
Almost certain	The risk is expected to occur in most circumstances.
Likely	The risk will probably occur in most circumstances.
Possible	The risk might occur at some time.
Unlikely	The risk could occur at some time.
Rare	The risk may occur only in exceptional circumstances.

There are several alternative model scales for classifying likelihood or frequency of risk, such as the following alternative scale:

Table 14 B VAN DER SMISSEN[120] SCALE FOR CLASSIFYING LIKELIHOOD OR FREQUENCY OF RISK	
Descriptor	Example description
High or often	What is high or often will depend upon the risk being evaluated; for some risks, often might be yearly, while for certain minor cuts and bruises it might be weekly; thus, in evaluating the frequency, the nature of the risk must be considered.
Medium or infrequent	Occurs occasionally and probably.
Low or seldom	Really a rare occurrence.

119 See appendix E, *AS/NZS 4360- 1999, Risk Management*.

120 Betty van der Smissen, JD, *Legal liability and risk management for public and private entities: sport and physical education, leisure services, recreation and parks, camping and adventure activities,* Anderson Publishing Co, Cincinnati, 1990, Ch 23, p. 8, §23.22.

The second step involves describing each risk according to the consequence or impact of the risk should it eventuate. Again, the number of categories used and the descriptions used will vary according to the needs of the risk analysis being undertaken[121]. Set out below are some model scales for classifying the consequence or impact of a risk eventuating:

Table 15 *AS/NZS 4360 - 1999, RISK MANAGEMENT*[122] ALTERNATIVE SCALE FOR CLASSIFYING CONSEQUENCE OR IMPACT OF A RISK EVENTUATING

Descriptor	Example description
Catastrophic	Huge financial loss
Major	Major financial loss
Moderate	High financial loss
Minor	Medium financial loss
Insignificant	Low financial loss

Table 16 VAUGHAN[123] SCALE FOR CLASSIFYING CONSEQUENCE OR IMPACT OF A RISK EVENTUATING

Descriptor	Example description
Critical	If the risk eventuates, it would expose a business to a loss that would result in the business becoming bankrupt.
Important	If the risk eventuates, the risk would result in the business needing to borrow funds in order to continue its operations.
Unimportant	If the risk eventuates, the risk would result in the business being exposed to losses that could be easily met out of the business's existing assets or current income.

121 See appendix E, *AS/NZS 4360- 1999, Risk Management*.
122 Adapted from Appendix E, *AS/NZS 4360- 1999, Risk Management*.
123 Vaughan, p 36.

Table 17 STANDARDS AUSTRALIA/STANDARDS NEW ZEALAND JOINT TECHNICAL COMMITTEE ON RISK MANAGEMENT [124]: ALTERNATIVE SCALE FOR CLASSIFYING CONSEQUENCE OR IMPACT OF A RISK EVENTUATING

Descriptor	Example description
Extreme	The consequences would threaten the survival of not only the program, but also the organisation, possibly causing major problems for clients, the administration of the program or for a large part of the public sector. Revenue loss greater than x% of total revenue being managed would have extreme consequences for the organisation both financially and politically.
Very high	The consequences would threaten the survival or continued effective function of the program, or require the intervention of top level management or by the Elected Representatives. Revenue loss greater than y% of total revenue being managed would have very high consequences for the organisation both financially and politically.
Medium	The consequences would not threaten the program, but would mean that the administration of the program could be subject to significant review or changed ways of operating. Revenue loss greater than z% of total revenue being managed would have medium consequences for the organisation both financially or politically.
Low	The consequences would threaten the efficiency or effectiveness of some aspects of the program, but would be dealt with internally. A loss of revenue below the tolerance level of 5% (Audit materiality) applied to clients would be of low consequence.
Negligible	The consequences are dealt with by routine operations. A loss of revenue below the program tolerance level of w% (less than Audit materiality) applied to clients would be of negligible consequence.

A useful approach practised by the corporation Fletcher Challenge is to apply descriptors that allow a multi-dimensional analysis of the consequence of a risk. The following figure illustrates how the consequence of a given risk can be analysed by reference to financial, and other factors such as the public image of an organisation:

---

[124] Standards Australia/Standards New Zealand Joint Technical Committee on Risk Management, p. 25.

Table 18 MAYNARD [125]: MULTI-DIMENSIONAL SCALE FOR CLASSIFYING CONSEQUENCE OR IMPACT OF A RISK EVENTUATING

DESCRIPT-ION	SEVERITY WEIGHTING	DEFINITION			
		Health/Safety	Image	Environment	US$ m
Catastrophe	100	Multiple fatalities	International media coverage	Permanent, wide eco-damage	>50
Major	60	Single fatality	National media coverage	Heavy damage, costly restoration	5-50
Serious	25	Major injuries	Regional media cover	Habitats affected, off-site affected	0.5-5
Moderate	10	Minor injuries	Local media cover	No lasting effects	0.05 -0.5
Minor	2	Slight injury	Minor media cover	No long term effect	<0.05

Then each risk, which by now has been described according to the likelihood of it eventuating and the consequence or impact should it eventuate, is plotted on a matrix according to the description accorded to it and, according to its position on the matrix, is categorised according to the level of risk. Again, the categories denoting the level of risk are variable and are determined by reference to factors specific to a business. Set out below are some model scales for denoting the level of risk:

---

125 Ian Maynard, "Development and Implementation of Risk Management Strategy", in David Elms, Editor, *Owning the Future- Integrated Risk Management in Practice*, Centre for Advanced Engineering, University of Canterbury, Christchurch, New Zealand, August 1998, Chapter 10, p135.

Table 19 *AS/NZS 4360 - 1995, RISK MANAGEMENT*[126]: SCALE FOR LEVEL OF RISK	
Descriptor	Example description
High	Detailed research and management planning required at senior levels.
Significant risk	Senior management attention needed.
Moderate risk	Management responsibility must be specified.
Low risk	Manage by routine procedures.

Table 20 *AS/NZS 4360 - 1999, RISK MANAGEMENT*[127]: ALTERNATIVE SCALE FOR LEVEL OF RISK	
Descriptor	Example description
Extreme risk	Immediate action required.
High risk	Senior management attention needed.
Moderate risk	Manage by specific monitoring or response procedures.
Low risk	Manage by routine procedures.

Table 21 CROCKFORD[128]: ALTERNATIVE SCALE FOR LEVEL OF RISK	
Descriptor	Example description
Large risk	A risk whose frequency is low but whose severity is high and whose predictability is minimal. Such losses, when they occur, 'could be catastrophic.
Medium risk	A risk whose frequency is low and severity medium and whose predictability of occurrence is reasonable within 10 years. Such risk, if it eventuates, would require the business to seek

[126] Adapted from Appendix D, *AS/NZS 4360- 1995, Risk Management*.
[127] Adapted from Appendix E, *AS/NZS 4360- 1999, Risk*.
[128] Crockford, pp 11-12.

	external short term funds.
Small risk	Risks whose frequency is high but whose severity is low and whose predictability of occurrence is 'reasonable within 1 year.
Trivial risk	A risk whose frequency is very high, whose severity is very low and whose predictability of occurrence is very high such that if it eventuated it would result in a loss that could be met from normal operating budgets.

It is easier to follow the process of qualitatively analysing risks when viewed in the form of a matrix. The Australian Standard *AS/NZS 4360 -1999 Risk Management* provides the following model matrix for evaluating risk on a qualitative basis:

Table 22 AUSTRALIAN STANDARD *AS4360 : 1999 RISK MANAGEMENT* MODEL MATRIX FOR QUALITATIVELY ANALYSING RISK[129]

The number of categories for "likelihood of risk" and "consequences of risk" used will vary according to the needs of the risk analysis being undertaken.

	CONSEQUENCES OF RISK EVENTUATING				
LIKELIHOOD OF RISK EVENTUATING	**Catastrophic** (huge financial loss)	**Major** (major financial loss)	**Moderate** (high financial loss)	**Minor** (medium financial loss)	**Insignificant** (low financial loss)
Almost certain (the risk will occur in most circumstances)	Extreme risk	Extreme risk	Extreme risk	High risk	High risk
Likely (risk will probably occur in most circumstances)	Extreme risk	Extreme risk	High risk	High risk	Moderate risk
Possible (risk might occur at some time)	Extreme risk	Extreme risk	High risk	Moderate risk	Low risk
Unlikely (risk could occur at some time)	Extreme risk	High risk	Moderate risk	Low risk	Low risk
Rare (risk will occur only in exceptional circumstances)	High risk	High risk	Moderate risk	Low risk	Low risk

Legend:

Extreme Risk = immediate action required
High risk = senior management attention needed

[129] Adapted from Appendix E, *AS/NZS 4360- 1999, Risk Management*.

Moderate risk = management responsibility must be specified
Low risk = manage by routine procedures

Obviously, the format that a matrix will take can vary, depending on the "descriptors" adopted for describing the likelihood of risk, the consequences of risk and level of risk. Thus the model matrix can be quite simple such as the following example:

Table 23 B VAN DER SMISSEN [130] MODEL MATRIX FOR QUALITATIVELY ANALYSING RISK

	FREQUENCY OF OCCURRENCE		
SEVERITY OF INJURY OR FINANCIAL IMPACT	**High or Often**	**Medium or Infrequent**	**Low or Seldom**
High or Vital	Avoid or Transfer	Transfer	Transfer
Medium or Significant	Transfer	Transfer or Retain	Transfer or Retain
Low or Insignificant	Retain	Retain	Retain

So how do you determine which qualitative description best describes a given risk? The Commonwealth government's *Managing Risk in Procurement- A Handbook* provides the following advice in relation to procurement risks that could equally apply in relation to other types of risks:

> You can: draw on the expertise of the members of your … team; use in-house and consultant experts skilled in commercial and technical matters and risk management tools; consult information [like that provided in the handbook Appendixes]; look up historical records; find out about other people's experiences, either with the kind of procurement you are analysing or with similar contractors or suppliers; investigate industry practice and standards; seek advice from potential suppliers; consult relevant literature and research

[130] van der Smissen, p. 13, §23.31.

> reports; look at product brochures, technical manuals and audit reports; check market research, where new information may be helpful….[131]

The level of risk descriptor is not intended to reflect a precise or absolute analysis of a given risk. Rather it enables often disparate risks to be ranked:

> There is no absolute significance to the risk rating. However, it does provide an excellent basis for relatively ranking the significance of different risks to the corporation[132].

2.4.3.4 Semi-quantitative approach

In addition to quantitative and qualitative approaches to risk analysis, Australian Standard *AS/NZS 4360 - 1999 Risk Management* suggests risks can be analysed according to "semi-quantitative analysis" whereby risks are analysed qualitatively in the manner described above but that each risk description should be given a value that "does not have to bear an accurate relationship to the actual magnitude of likelihood or consequence" with a view to obtaining a more easily differentiated assessment of the overall degree of risk for each risk. However, as *AS/NZS 4360 - 1999* warns there are dangers in using this approach because "the numbers chosen may not properly reflect relativities which can lead to inconsistent outcomes"[133].

2.4.3.5 Prioritising the risks

Once the identified risks are analysed, whether quantitatively or quantitatively, they are ordered according to priority. The outcome of this step should be a list of the

---

131 Purchasing Australia, Commonwealth of Australia, *Managing risk in procurement- A handbook*, Australian Government Publishing Service, Canberra, 1996, p 21.
132 Maynard, p136.
133 *AS/NZS 4360- 1999, Risk Management*, para 4.3.4(b).

identified risks that prioritises or categorises each of those risks in terms of their likelihood of eventuating and consequence.

As noted earlier at 2.3.3 (starting at p 26), the risk management texts diverge as to what constitutes the next step in the risk management process. To reiterate, the Australian literature on risk management, which is strongly influenced by the Australian Standard on *Risk Management AS/NZS 4360 - 1999* states that, having categorised each risk in terms of consequence and probability, the next step in the risk management process is to decide which risk is acceptable and which risk is unacceptable. Other risk management texts, such as those emanating from the UK and the US, advocate a different approach. Once the risks have been identified and analysed in terms of probability and consequence the next step is to consider all the risks and consider what is the appropriate risk management strategy in relation to each risk, which may include risk retention. As stated earlier in this thesis at 2.3.3, whilst it is recognised that the *AS/NZS 4360* - 1999 approach may be more practicable, when discussing the process of risk management at a theoretical level, in order to avoid repetition, it is more appropriate to consider the factors that should be considered in determining whether a business should retain a risk only once, when the third step of the risk management process, "Evaluating and choosing appropriate risk management strategies" is discussed.

2.4.3.6 Analysing legal risk

Very little has been written in the literature as to what techniques should be employed for analysing *legal* risk. For example, Australian Standard *AS 3806 -1998*

Compliance Programs, a Standard that is directed at assisting businesses ensure that they comply with the regulatory frameworks that govern them, makes no reference at all as to whether and how legal risks should be assessed (the initial discussion of scope in *AS 3806* does, however, advert to *AS/NZS 4360* as providing good guidance for conducting overall risk management[134]).

Further, unlike other industries and disciplines, it is unusual for data concerning how legal risks are best managed to be routinely collected:

> The business of law may be the only major industry in which firms have no research and development (R & D) departments or models to test which products work and how they can be improved. No data is maintained that catalogs which language leads to smoothly functioning agreements and which often leads to disputes. No data is maintained on the management of disputes once they arise or on how they are most efficiently resolved. There is no data nor basic concepts on the cost-benefit analysis of different methodologies of seeking results. A manufacturer seeks tools to cut the cycle time of production and reduce unit costs. There is no equivalent in the legal business.[135]

There is little or no data publicly available, at least in Australia, that assists analysing the *likelihood* that a legal risk will eventuate although individual law firms or insurance companies may hold statistical data recording the likelihood that specific legal risks will eventuate.

Moreover, little is known (or at least publicly available) about the likelihood that a *loss will be incurred* as a result of a legal risk eventuating. That is, little is known, at least in the Australian context, about whether a business will be prosecuted, and subsequently penalised, if it fails to comply with a statute, or that the business will be

---

[134] *AS 3806 – 1998 Compliance programs*, para 1.1

sued by a party for breach of contract if the business breaches a contract, or that a business's legal rights and interests will be eroded, or lost, if the business fails to protect its legal rights and interests. This is partly because legal risks that eventuate do not automatically result in loss to a business. For example, a business conducting Internet commerce faces the legal risk that it enters into an Internet transaction that is subject to a requirement that it be evidenced in writing. The business does not incur loss simply because this risk eventuates. Rather, the business will incur loss only if the party with whom it transacts breaches the contract or denies that a contract is in existence, because in such instances the business cannot enforce the contract it entered into.

It might therefore be concluded that risk management cannot be used in the context of legal risk. Risk management commentators however do not draw such a conclusion. Rather, as noted at 2.4.2.1 at p51, they distinguish between legal risks that are "hazards" and legal risks that are "perils". As noted earlier in this chapter at 2.4.2.1 at p51, a legal risk constitutes a "hazard" when it is a condition or circumstance that makes a loss more likely or more severe, such as a business engaging in wrongful conduct that increases the likelihood that a claim will be brought against it and that such claim will be successful[136]. A legal risk constitutes a "peril" when it is a condition or circumstance that *causes* a loss, such as the filing of

---

[135] Howard B Miller, "The Randolph W Thrower Symposium: The role of the general counsel: Perspective: Law Risk Management and the General Counsel, 46 *Emory Law Journal* 1223, Summer 1997, at p 1232.

[136] Head and Horn, *Essentials of Risk Management*, http://www.bus.orst.edu/faculty/nielson/rm/chapter6.htm.

a legal claim[137] or a prosecution of the business for statutory non-compliance. Risk management can be used in relation to those legal risks that are "hazards" but not in relation to those legal risks that constitute "perils" [138].

Thus, to return to the question of how a legal risk can be analysed, it is only those legal risks that constitute "hazards" that can presently be analysed. Those legal risks that constitute "perils", such as the risk that a party will commence legal action against a business, cannot be analysed because typically no data (whether quantitative or qualitative) is available that provides a basis for estimating the likelihood of such legal risks eventuating. It is interesting to note, however, that this aspect of law is starting to be the subject of academic research. One author has put forward a model for assessing the likelihood that a defendant will lose a negligence case brought against the defendant using Bayes' Theorem to ascertain how a decision maker (juror) will assess the evidence and determine whether a defendant has met the standard of care[139]. Whilst the discussion by this author focuses on how this model can be used to assess incentives to comply with legal rules and is presented at an abstract level, this model could be equally useful in the context of analysing the likelihood that a legal action brought against a business will succeed. Other authors too, have examined how probability theory can be used to determine the factors affecting the likelihood of a defendant being found liable in the context of incentives

---

[137] Head and Horn, *Essentials of Risk Management*, http://www.bus.orst.edu/faculty/nielson/rm/chapter6.htm.

[138] Head and Horn, *Essentials of Risk Management*, http://www.bus.orst.edu/faculty/nielson/rm/chapter6.htm.

to comply[140]. It will be interesting to see if these authors and others undertake further research in the context of analysing the likelihood that a legal action brought against a business will succeed and how this will affect the current belief that risk management cannot be used to analyse legal risk that constitute "perils".

So how can legal risks that constitute "hazards" be analysed? More specifically, can legal risks that are "hazards" be analysed quantitatively? It will only be possible to carry out a quantitative analysis of the *likelihood* of a legal risk eventuating if statistical data is available or, at the very least, expert advice is available concerning the likelihood that a given legal risk will eventuate. It is understood that in the US there are companies that publish texts predicting the likelihood of winning a case in certain factual circumstances[141]. Whilst such information may be available in the US it is not so readily available in Australia thus making it difficult if not impossible to undertake a quantitative analysis of the *likelihood* of a legal risk eventuating. Undertaking a quantitative analysis of the *consequence* of a legal risk may be much easier to analyse. If the legal risk is the kind of risk that attracts civil liability it will be possible to refer to the relevant legal principles for calculating damages and also to precedents to determine the consequence of such a legal risk eventuating. In some

---

139 Jason S Johnston, "Bayesian Fact-Finding and Efficiency: Toward an economic theory of liability under uncertainty", 61 *Southern California Law Review*, 1987, 137 .

140 See for example, John E Calfee and Richard Craswell, "Article: Some effects of uncertainty on compliance with legal standards", 70 *Virginia Law Review*, 965, June 1984.

141 Stuart S Nagel in "applying Decision Science to the Practice of Law", *The Practical Lawyer*, Vol 30, No 3, April 15 1984, p 13 at p 15 states: "Victory probabilities can be predicted more accurately by consulting the loose-leaf service of the Jury Verdict Research Corporation. …case samples indicate victory probabilities for various types of cases. A lawyer can combines those probabilities to obtain conditional or joint probabilities, or he can simply use them in their raw form by finding the particular type of case that best fits his case."

fields, such as the field of personal injury, texts can be referred to that provide estimates of damages payable in the event the court awards damages[142]. If the legal risk involves liability for statutory non-compliance, it will be possible to refer to the relevant statute to determine the penalty that applies. If the legal risk involves failure to protect a business's legal interests and rights, it may be more difficult to evaluate the consequences but such task is not impossible given this process is undertaken each time a plaintiff claims, for example, a breach of copyright.

So how have legal risks been analysed quantitatively in practice? Documented instances where quantitative techniques have been used to analyse legal risk are rare. A literature review has revealed only a handful of legal practitioners and academics who use and advocate such an approach[143]. It is necessary here to distinguish between instances where quantitative techniques have been employed in relation to legal matters as an evidential tool and where they have been employed to *analyse* the *likelihood* and *consequence* of legal risk. It is quite common, for example, to use quantitative techniques in litigation as evidence, for example, to establish the

---

142 Again, these texts are more prevalent in the US.

143 See Marc B Victor, "Ch 17 Litigation Risk Analysis™ and ADR" in John H Wilkinson, editor, *Donovan Leisure Newton & Irvine ADR practice book*, Wiley Law Publications- John Wiley & Sons, Inc, New York, 1990, pp-307-332: Samuel E Bodily, "When should you go to Court?", *Harvard Business Review*, Boston, May/Jun 1981, Vol 59, No 3, pp 103-113. See also, Margot Costanzo, *Problem Solving- (Essential Legal Skills Serie*s), Cavendish Publishing Limited, London, 1995 pp 169-177 who also gives examples of legal problem analysis involving allocating numeric values to the likelihood of a given legal risk eventuating. Ronald Greenberg in "The Lawyer's Use of Quantitative Analysis in Settlement Negotiations", *The Business Lawyer*, Vol 38, August 1983 1557 advocates using quantitative techniques for analysing liability risk and cites a number of studies that have investigated the use of quantitative techniques for analysing legal liability risk. In addition, Stuart Nagel, in "Literature on Computer Software and Legal Decision Making", *Law Library Journal*, 1990, vol. 82, p 749 describes the use of computer software in relation to legal reasoning including, deciding when to go to trial or to settle a matter and deciding what legal phrasing to use in a contract.

probability of recovering from a disease or to predict a plaintiff's life expectancy after a personal injury[144]. This use of quantitative techniques, which is prevalent and about which much has been written[145], should not be confused with the use of quantitative techniques to analyse the *likelihood* and *consequence* of a legal risk eventuating.

The form of quantitative analysis commonly employed in relation to legal risks is decision tree analysis although other decision-making approaches such as rule based modelling (or expert systems), open claim analysis and closed claim analysis can be used to analyse legal risks[146]. The use of decision tree analysis has primarily been

---

144 DH Kaye, "IV Practice and Procedure: Statistics for Lawyers and Law for Statistics", a review of *Statistics for Lawyers* by Michael O Finkelstein and Bruce Levin, Springer Verlag, New York, 1990 *Michigan Law Review*, Vol 89, May 1991 p 152.

145 The literature on the use of quantitative techniques in litigation matters is voluminous and includes: Michael O Finkelstein and Bruce Levin, *Statistics for Lawyers*, Springer-Verlag, New York 1990; Richard D Friedman, "Symposium: Probability and Inference in the law of evidence: I. Theories of Inference and Adjudication: a diagrammatic approach to evidence", *Boston University Law Review*, Vol 66, July 1996, p 571; Jonathan J Koehler and Daniel N Shaviro, "Veridical Verdicts: Increasing Verdict Accuracy through the use of Overtly Probabilistic Evidence and Methods", *Cornell Law Review*, Vol 75, January 1990, p 247. For a view disputing the scope of the usefulness of one probabilistic technique, Bayesian probability in legal decision making see: Lea Brilmayer, "Symposium: Probability and Inference in the Law of Evidence: II. Bayesian Theory and its Critics: Second-order evidence and Bayesian Logic", *Boston University Law Review*, Vol 66, July 1986, p 673.

146 Stuart Nagel, in "Literature on Computer Software and Legal Decision Making", *Law Library Journal*, 1990, vol. 82, p 749 at pp 750-752 lists several types of software that can assist in legal decision making, which in turn can be used to analyse legal risk. For example, linear programming software is useful in allocating money, time, people or other scarce resources. In addition, statistical software can help to predict how a future case is likely to be decided, the damages payable in light of past cases or expert opinions. Rule-based software too can be used to apply a set of rules to the facts to determine which alternative is likely to be chosen. Mark A Peterson in *New Tools for Reducing Civil Litigation Expenses*, R-3013-ICJ, The Institute for Civil Justice, Rand Publications Series, 1983 suggests there are four computer based methods that can be used to analyse legal risks that give rise to lawsuits: (i) open claim analysis, which involves estimating the costs associated with an active lawsuit; (ii) closed claim analysis, which involves using historical data to estimate the cost of a lawsuit and its likely outcome; (iii) decision analysis, where numerical values are assigned the potential outcomes of a lawsuit and then combined to estimate the cost and likelihood of a given outcome and (iv) rule based modelling (expert systems).

limited to litigation cases although one author suggests its use could be extended to other legal uses such as deciding which phrasing to use for a contract or other legal document[147]. The methodology advocated involves breaking down the potential outcome of a litigious matter that is, to "win" or to "lose" into "decision trees" that trace the various legal uncertainties affecting either a "win" or a "lose" outcome. Then each legal uncertainty is allocated a numerical figure reflecting the probability that the legal uncertainty will eventuate. The use of the technique is demonstrated in the following description:

> Let's imagine a case in which you feel your result will depend on whether you can convince the court to admit certain evidence and on whether you can make the jury understand your technical expert.
>
> First capture each of the important uncertainties in a decision tree. Decision trees consist of *nodes* and *branches*. Each area of uncertainty (eg legal issue) is represented by a node and the possible outcomes of the uncertainty by branches. (While there are usually two possible outcomes to any uncertainty, there can be three or more. In such instances, multiple branches would flow from the node, one for each of the possible outcomes.) Because the ultimate outcome of the case depends on the resolution of several uncertainties, these must be linked together to form all the possible scenarios according to which the case might unfold. …
>
> Second, marshal the pluses and minuses on each of the influencing factors. Imagine the judge allows the evidence. Why? List all the reasons you can think of. Now imagine thee judge excludes the evidence. Why? Again, list all the possible reasons. Then, *before* you formulate your opinion of the likelihood of the evidence being admissible, have a colleague review your list of reasons. What have you overlooked?
>
> Third, when the list is complete, study the reasons supporting each possible outcome and decide on the probability of the alternative outcomes. Because the branches coming from each node represent all the possible outcomes, the probabilities assigned at each node must add up to 1.00. Remember, the

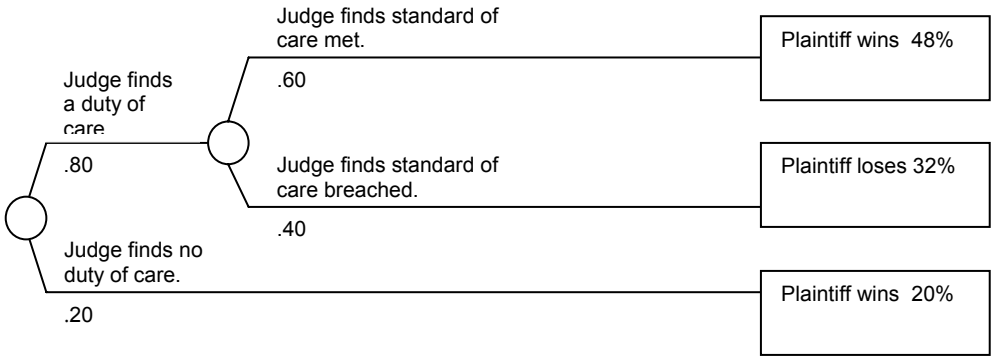
---

147 Stuart Nagel, "Literature on Computer Software and Legal Decision Making", *Law Library Journal*, 1990, vol. 82, p 749 .

> probabilities are only best guesses, because unfortunately, uncertainty exists. No guarantees are possible. …
>
> Fourth, multiply and then add the products to average or weight your individual judgments[148].

The following figure is a simple example illustrating the use of decision tree analysis to calculate probability of a given outcome:

Figure 5 SAMPLE USE OF DECISION TREES TO QUANTITATIVELY ANALYSE LEGAL OUTCOME OF LITIGATION[149]



In this way the probability that a judge or jury will come to a particular decision can be calculated. Having quantified the probability that a particular decision will be reached, a similar process can be used to quantify the costs that a defendant is likely to incur (the consequence) to defend a case in relation to each potential scenario that

---

148 Marc B Victor, "How Much is a Case Worth? Putting Your Intuition To Work To Evaluate the Unique Lawsuit", *TRIAL*, July 1984, Vol 59, No 3, p 103-113.

149 For other examples illustrating a larger number of legal uncertainties (variables) see: Marc B Victor, "Ch 17 Litigation Risk Analysis™ and ADR" in John H Wilkinson, editor, *Donovan Leisure Newton & Irvine ADR practice book*, Wiley Law Publications- John Wiley & Sons, Inc, New York, 1990, Figures 17-3- 17-7 at pp 314-320; Samuel E Bodily, "When should you go to Court?", Harvard Business Review, Boston, May/Jun 1981, Vol 59, No 3, pp 103-113.

could arise[150]. Further, the probabilities allocated for each outcome can be varied using sensitivity analyses to ascertain which legal uncertainties have a greater impact on potential exposure to costs[151]. Thus, decision tree analysis, which requires breaking down a legal risk into the "legal uncertainties" that affect its outcome and allocating quantitative assessments to each of these "legal uncertainties", arguably results in a more "accurate" quantitative estimate than a simple estimate of the likelihood and consequence of the "overall" legal risk eventuating[152].

The use of decision analysis techniques to analyse legal risk is subject to a number of criticisms including that estimates provided by lawyers of probability are questionable, due to their complexity it will not always be possible to estimate the likelihood of all possible potential outcomes of a legal matter and the fact that potential outcomes are often not independent, as is assumed in decision analysis:

> Unfortunately, although decision analysis enables systematic consideration of all issues in complex cases, the calculation of a claim's value may have little meaning. First, the probability estimates provided by litigators are questionable. Neither lawyers nor claims adjusters are trained in or used to providing probability estimates. They may do so if prodded, but their numbers may raise more questions than they answer. For example, if a lawyer says there is a 50/50 chance that a jury will find a product defective, is it his judgment that 50 percent of juries would find a defect and 50 percent would not? Or does the 50/50 estimate also include uncertainty: The lawyer thinks that anywhere from 40 to 60 percent of juries would find the product defective? Or does 50/50 mean that he has not idea how often a jury would find defect? Of course, even if we know what the lawyer means by this estimate, the actual likelihood of a jury finding the product defective might not even be close to 50/50. Since the results of decision analysis rest on these estimates, their unreliability raises questions about the value of the analysis.

---

151 Marc B Victor, "Ch 17 Litigation Risk Analysis™ and ADR", p 326.

152 Marc B Victor "The Proper Use of Decision Analysis to Assist Litigation Strategy", *The Business* Lawyer, Vol 40, February 1985, p 619.

> Second, when a case entails numerous issues, there is no single right way to combine the probabilities. A pure application of this approach requires estimating the likelihood of all possible alternatives for the case. This is simple where there are only four alternatives…. But a complex case may involve many alternatives and issues: what witnesses appear, what type of jury will be selected, whether third party defendants should be named, and so on. To try to estimate the likelihood of all combinations of these alternatives is like trying to plan a chess game by estimating the chance of each possible succession of moves.
>
> The difficulty is even greater if each probability estimates is an estimate of a range of uncertainty about the likelihood that an alternative will occur (eg, if 50 percent does not mean exactly 50 percent but a figure anywhere between 40 percent and 60 percent)…. The estimate of a case's value depends on what specific probabilities are used. A range of values can be fairly well estimated within which the true value is likely to be, but there is no single right value.
>
> Third, methods for calculating the outcome of a case generally assume that the outcomes for the various issues are independent. For example, the analysis assumes-perhaps erroneously- that the likelihood of finding a plaintiff to be contributorily negligent is not affected by whether or not a particular deep-pocketed defendant will be included or dismissed from the case. But this assumption is often false: The resolutions of many issues in litigation may be interrelated.
>
> Because of these problems, the estimate of present value provided by decision analysis cannot be regarded as "right," precise or rational.
>
> The analysis can help organize the issues of a complex claim, but neither defendant nor plaintiff should seize upon it as dogma or belabor the other side into accepting it as the "right" value.
>
> Decision analysis even has its limitation in helping to organize a case. It can aid the identification of important elements of a large claim, but few lawyers or claims persons have the training to follow closely how decision analysis arrives at its outcomes[153].

Another technique used for quantitatively analysing legal risks worth briefly discussing is the use of rule-based expert systems. Rule-based expert systems use software that:

> …contains a set of rules for dealing with a field of law. The user gives the computer a set of facts, and the computer applies the rules to the fact to determine which alternative is likely to be chosen. Such software is sometimes referred to as artificial intelligence (AI) or expert systems, but the other forms of decision-aiding software also have characteristics associate with AI and expert systems[154].

Clearly rule-based expert systems could be useful to quantitatively analyse the consequence of a given legal risk. Again, the rule-based expert system software that exists, such as Judith, DataLex, Rubric, Hypo, Lex, Default, Oblog-2, Esplex and LexVision[155] tends to be US focussed, that is it applies rules that reflect the legal system in the US. It should be also noted that rule-based expert systems is by no means "perfect", one criticism made in relation to one of the earlier rule-based expert systems developed being that they did not give enough "prominence to the adversarial nature of legal reasoning, where the opposing sides seek to establish different, and often contradictory, conclusions"[156] and another criticism being that "the rule-based approach assumes that the set of rules has no inherent difficulties like ambiguities, gaps and conflicts. To make a rule-based system work, the programmer must usually eliminate these problems and make the rules appear more consistent and complete than they are"[157].

---

153 Mark A Peterson in *New Tools for Reducing Civil Litigation Expenses*, R-3013-ICJ, The Institute for Civil Justice, Rand Publications Series, 1983, pp26-28.

154 Stuart Nagel, in "Literature on Computer Software and Legal Decision Making", *Law Library Journal*, 1990, vol. 82, p 749 at p 751 .

155 Nagel, p 751.

156 Edwina Rissland, in commenting on a rule-based legal expert system called "LDS" developed by Donald Waterman and Mark Peterson of the RAND Corporation's Center for Civil Justice in the 1980s in "Comment: Artificial Intelligence and Law: Stepping Stones to a Model of Legal Reasoning", *Yale Law Journal*, Vol 99, June 1990, p 1957 at 1967 .

157 Edwina Rissland in commenting on a rule-based legal expert system called "LDS" developed by Donald Waterman and Mark Peterson of the RAND Corporation's Center for Civil Justice in the

Whilst the above description of the use of decision tree analysis and rule-based expert systems illustrates that it is possible to quantitatively analyse legal risks the fundamental problem remains that, with the exception of specific legal risks that arise in the US, there is little statistical data that is publicly available in relation to the likelihood and consequence of a given legal risk or the "legal uncertainties" affecting its outcome. Where such information is not available, the legal practitioner or risk manager must rely on his or her own judgment and intuition to estimate the probability or consequence of a given outcome eventuating, a fact acknowledged by several of the writers who have examined the use of quantitative methods to analyse legal risk[158]. This raises doubts as to the reliability of any quantitative analysis undertaken, an issue that is discussed further below.

Also, *quantitative analyses* of *legal risks that expose a business to liability* are, difficult to undertake, as the extent of exposure to liability can, in some circumstances, be very difficult to calculate:

> Problems associated with liability losses are not limited to those of foreseeing how liability will arise. It is far more difficult to assess the probable severity of a liability loss than one of material damage, or even of loss of earnings. No one can forecast in advance exactly who will be affected by an action of the company, or to what extent they will be affected.

1980s in "Comment: Artificial Intelligence and Law: Stepping Stones to a Model of Legal Reasoning".

158 See for example, Costanzo, p 176 who states: "A few words of caution are warranted for this approach. First, it must be remembered that the allocation of risk in the form of probabilities was intuitive, not scientific." Similarly, Marc B Victor in, "How Much is a Case Worth? Putting Your Intuition To Work To Evaluate the Unique Lawsuit", *TRIAL*, July 1984, Vol 59, No 3, p 103-113 acknowledges that "Remember, the probabilities are only best guesses, because unfortunately, uncertainty exists" as quoted in the text above.

> Furthermore, the size of a liability incurred may bear no relationship to the importance to the company of the activity which gave rise to it.[159]

Similar sentiments have been expressed by other writers, such as:

> The risk of liability is, in any event, worse for being capricious. It bears no relation to the size of the company, or the value of what it owns, and once the chain of events that leads to a liability begins, it is largely fortuitous whether the loss that results will be trivial or serious.[160]

And likewise:

> No perfect method has yet been developed for measuring the maximum potential dollar loss a given business can suffer from its liability exposure. Who can say how many injuries can arise at the maximum from the tortious actions of a business or through the violation of warranties? Furthermore, who can say how much at the maximum any one injury will cost? Only one statement about the maximum loss potential from liability can be made with full confidence: the maximum the business can lose is the business itself.[161]

Further, the use of quantitative techniques to analyse risks in general (whether the risks are legal or other types of risk) may not always be appropriate:

> One of the greatest dangers in the current emphasis in business schools on statistics and other forms of quantitative analysis is the failure to provide adequate training with respect to the question of when these tools are appropriate and when they are not. Unfortunately, there is an almost irresistible temptation to use quantitative tools to solve every problem, simply because the tools "are there", even when the situation does not merit their use and when the results may be counterproductive.
>
> ….
>
> But it is important that probability theory and quantitative analysis be placed in their proper perspective and used when they are appropriate aids in risk management decisions. [162]

---

159 Crockford, p 93. Similar sentiments have been expressed by Vaughan, p 148 and Mehr and Hedges p 302.
160 Crockford, p 7.
161 Mehr and Hedges, pp 303-304.
162 Vaughan, p 154.

For example, a quantitative measurement of probability of risk may not be reliable due to reliance on limited records to calculate probability:

> The only evidence on which estimations of the probability of future events can be made is what has happened in the past, therefore the more relevant data of past losses that is available for analysis, the more confident one can be about the probability of future events.[163]

In addition, the cost of obtaining a quantitative measurement of risk may outweigh the value gained by being able to measure a risk quantitatively. The US Presidential/Congressional Commission on Risk Assessment and Risk Management in its report on environmental risk regulation has emphasised that the outcome of the risk evaluation step of the risk management process is to guide decisions about risk management. The Commission noted that there is a danger that too much time and resources can be spent on obtaining quantitative measurements of a risk when such resources could be better spent on risk management (or as the Commission puts it, on risk reduction):

> Risk assessments are decision-making tools, not precise analyses of actual or measurable risk, so their focus should remain on how best to inform the ultimate goal- risk reduction- rather than on generating complex distributions of possible risk estimates[164].

Other problems identified with using a quantitative method to analyse *legal risk* include the possibility that the quantitative analysis made is "overconfident":

> In experiments where people untrained in probability assessment [which in most cases would reflect a lawyer's experience] were asked to give their subjective probability distributions for almanac data, they tended to be overconfident in their ability to predict. Outcomes that they predicted would occur 2% of the time actually occurred 40%-50% of the time. Estimates

---

[163] Crockford, p 28.
[164] The Presidential/Congressional Commission on Risk Assessment and Risk Management, p90.

> improved as the subjects' experience with and training in probability assessment increased but some tendency toward overconfidence remained[165].

Accordingly, notwithstanding that, in theory, a quantitative analysis of a legal risk may be possible, it is suggested that legal risks are more likely to be analysed qualitatively or, analysed using a combination of qualitative and quantitative evaluation rather than using quantitative analysis alone. This is not only because it may not always be possible for a business to obtain the statistical data required in order to make a quantitative analysis but because of the present lack of familiarity (and arguably expertise) of lawyers with using quantitative techniques to analyse legal risk. Until user-friendly software exists that assists in the quantitative analysis of legal risks it is unlikely that lawyers will seek to undertake a quantitative analysis of a legal risk. Whilst it may be the case that such software exists in the US (and even in the US its use is not necessarily widespread but rather is used for specific types of legal risk such as risk of liability in tort) the existence of software that analyses legal risks quantitatively is not commonly available in other jurisdictions, such as Australia[166]. Thus, one partner, of a top tier law firm states that she uses a qualitative approach when analysing legal risk[167].

---

[165] Bodily, p 112.

[166] Interestingly, in a report on the Radio National AM program broadcast on 16 August 1999 an announcement was made by an Australian company based in Brisbane that it would shortly release legal software, available nationally, that could be used to estimate the damages payable in relation to certain types of injuries.

[167] Response dated 22 November 1999 to a self-completion questionnaire enquiring how the participant uses management methodology in the context of legal risk. Participants' names have not been disclosed to honour a request of some participants to remain anonymous. All responses are available on file.

Finally, moving away from the discussion of quantitative analysis of legal risk, an analysis of legal risk, whether it is qualitative or quantitative, ideally is undertaken on a case by case basis, taking into account data that is particular to a business such as the business's cash flow, liquid reserves and ability to increase cash flow in the event of an emergency, and where available, historical costs and records relating to how often in the past a risk has eventuated and the extent of losses sustained by a business when such risks have occurred. In this thesis, however, given that this thesis is not applying legal risk management to a specific business, it will only be possible to provide a general (non-specific) assessment of a given legal risk. Thus, when legal risk management is applied in the context of Internet commerce in the second part of this thesis, this thesis will not take into account factors that are particular to a business, such as the resources of the business affected, and the extent to which that business can bear the losses that such risk could bring about, which would involve drawing conclusions that may not be globally applicable to businesses. As will be discussed in more detail in chapter 5, the fact that only a general analysis of legal risk rather than a specific analysis of legal risk will be undertaken in this thesis is problematic only in relation to analysing the *consequence* of a given legal risk if it eventuates. There is no difficulty in analysing the *likelihood* of a given legal risk.

Set out below is a checklist for Step 3 of the legal risk management process:

Table 24 CHECKLIST FOR STEP 3 OF THE LEGAL RISK MANAGEMENT PROCESS

ANALYSING THE IDENTIFIED LEGAL RISKS

1. Select technique for analysing the legal risks. The Australian Standard *AS/NZS 4360 – 1999* advocates using a technical/economic approach to analysing risk. There are quantitative and qualitative techniques for applying a technical/economic approach. At present it is more likely that legal risks will be analysed qualitatively.	Several techniques are available for analysing legal risk. Broadly they fall into three categories, those methodologies that employ (a) a technical perspective (including the actuarial, epidemiological, engineering or "probabilistic" approach), (b) economic perspective (the cost-benefit approach), and (c) a psychological perspective (focus on individual judgment and personal perspective on risk).
2. Select a scale for categorising the *consequences* of a legal risk eventuating	The scale can be quantitative or qualitative. For a qualitative scale, see sample scales at 2.4.3.3 starting at p67.
3. Select a scale for categorising the *likelihood* of a legal risk eventuating.	The scale can be quantitative or qualitative. For a qualitative scale, see sample scales at 2.4.3.3 starting at p67.
4. Select a scale to denote the *level of risk* by reference to likelihood and consequence of risk.	The scale can be quantitative or qualitative. For a qualitative scale, see sample scales at 2.4.3.3 starting at p67.
5. Create a matrix comprised of the descriptors used (assuming a qualitative analysis of legal risk is being undertaken) to categorise the *consequence*, *likelihood* and the *level of risk*.	In respect of a qualitative analysis of the legal risks, see sample matrices at Table 22 and Table 23 at pp 73 -74.
6. Categorise each legal risk in terms of the *consequence* and *likelihood* of eventuating.	That is, apply descriptors from scales adopted.
7. Categorise the *level of risk* for each legal risk by referring to the matrix.	That is, for each legal risk plot the *consequence* and *likelihood* of risk on the matrix to determine the *level of risk*.
8. Prioritise each legal risk.	Numerically categorise each legal risk by reference to its level of risk. For example all legal risks that fall into the "extreme" risk level are given the number 1. This enables the legal risks to be ordered in terms of priority.
9. Communicate and consult with stakeholders (internal and, where relevant, external) in relation to the outcome of this step.	
10. Document this step.	See sample document set out at Table 25 at p94. This document combines steps 2 and 3 of the legal risk management process.

11. Monitor and review.	The outcome of this step should be periodically reviewed to take into account changes in circumstances that affect the likelihood and consequence of a given legal risk eventuating.

The following is a sample Risk Register for documenting steps 2 and 3 of the legal risk management process:

Table 25 SAMPLE RISK REGISTER FOR STEPS 2 AND 3 OF THE LEGAL RISK MANAGEMENT PROCESS (ADAPTED FROM SECTION H: RISK MANAGEMENT DOCUMENTATION, *AS/NZS 4360 - 1999 RISK MANAGEMENT* (REVISED))

RISK REGISTER (PART 2 OF 4)

Date of this Review:

Next Review Date:

Compiled by:

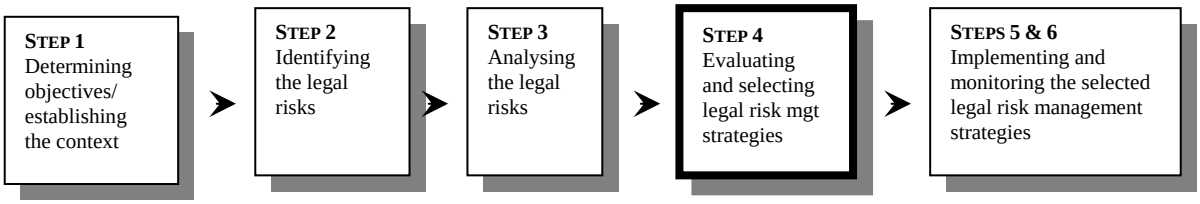
Approved/Reviewed by:

Legal risks identified	Consequences of risk eventuating	Conseq-uence rating	Like-lihood rating	Level of risk	Risk priority
[it may be useful to group identified legal risks into categories]		[use descriptors from scale adopted for consequence of risk]	[use descriptors from scale adopted for likelihood of risk]	[refer to matrix to determine level of risk]	[it is useful to number each risk according to the level accorded to it eg all risks categorised as "extreme" could be given the number 1, all risks categorised as "high" could be given the number 2 and so forth. The legal risks are listed in terms of priority at the next step of the legal risk management process.]

2.4.4 STEP 4: EVALUATING AND SELECTING RISK MANAGEMENT STRATEGIES

Figure 6 depicts step 4 of the risk management process as it applies in the context of legal risk.

Figure 6 LEGAL RISK MANAGEMENT: STEP 4



The fourth step of risk management is to develop a strategy or strategies for managing the identified risks. This step involves developing, evaluating and ultimately choosing risk management strategies in order to bring the business's exposure to risk within the levels of acceptable risk set when setting the risk criteria in Step 1 of the risk management process. In broad terms the strategies available for managing risk can be divided into two categories: those strategies that employ *risk control* techniques and those strategies that employ *risk financing* techniques.

2.4.4.1 Risk control techniques

Risk management strategies that employ *risk control* techniques use:

> ...those risk management techniques designed to minimize the frequency or severity of accidental losses or to make losses more predictable. Risk control techniques include exposure avoidance, loss prevention, loss reduction,

> segregation of loss exposures, and contractual transfers to shift losses to others, both legally and financially[168]

Many of these risk control techniques are self-explanatory. A few risk control techniques, however, require further explanation.

Loss prevention techniques are techniques that reduce the 'probability or frequency of a particular loss'[169]. For example, fire detection devices, education and safety regulations are all examples of loss prevention techniques.

Loss reduction techniques are those techniques that reduce the severity of loss that arises as a consequence of a risk eventuating[170]. For example, sprinkler systems and rehabilitation of employees injured at work constitute loss reduction techniques. In the context of managing legal risk, an important loss reduction technique is the use of contractual clauses to manage legal risk. The use of contractual clauses to manage legal and other risks can be a highly effective loss reduction technique. For example, a business's exposure to liability for negligence can be a reduced through the use of a contractual clause requiring a party transacting with a business to accept full responsibility for its actions and to indemnify the business against any loss or damage. It is not possible here to specify standard clauses that a business should employ in order to manage the legal risks it faces. This is because the contractual clauses that will be applicable will depend on the circumstances of each case and will

---

168 Head and Horn, *Essentials of Risk Management*, Insurance Institute of America, 1991, http://www.bus.orst.edu/faculty/nielson/rm/chapter1.htm.

169 Head and Horn, *Essentials of Risk Management*, http://www.bus.orst.edu/faculty/nielson/rm/chapter8.htm.

170 Head and Horn, *Essentials of Risk Management*, http://www.bus.orst.edu/faculty/nielson/rm/chapter8.htm.

depend on the particular objectives of the business and the party with whom it transacts and the value of the transaction.

Segregation of loss exposures refers to two risk management techniques: *separation of assets or operations* of a business and *duplication of assets or operations* of a business[171].

Separation of assets or operations involves:

> ...dividing an organization's own existing single asset or operation into two or more separate units. (Three examples are dividing an existing inventory between two warehouses, erecting fire walls to create separate fire divisions within a single building, and manufacturing in two plants a component part formerly produced in only one plant.) Separation is appropriate where an organization can meet its goals with only a portion of these separate units left intact. If total loss is suffered by any one unit, the portion of the assets or operations at the other locations) is sufficient. With separation, all separated units are normally kept in daily use in the organization's operations.[172]

Duplication of assets or operations, on the other hand, involves:

> ...complete reproduction of an organization's own "standby" asset or facility to be kept in reserve. This duplicate is not used unless the primary asset or activity is damaged or destroyed. Duplication is appropriate when an entire asset or activity is so important that the consequence of its loss justifies the expense and time of maintaining a duplicate. Two sets of accounting records or key items of equipment and back-up employees are examples of duplication of exposure units[173].

Contractual transfers refer to the use of exclusion or indemnity clauses in contracts or other mechanisms such as leasing and sub-contracting so that, in the event that a risk eventuates, the resulting losses will not be borne by the business.

---

171 Head and Horn, *Essentials of Risk Management*, http://www.bus.orst.edu/faculty/nielson/rm/chapter8.htm.

172 Head and Horn, *Essentials of Risk Management*, http://www.bus.orst.edu/faculty/nielson/rm/chapter8.htm.

173 Head and Horn, *Essentials of Risk Management*, http://www.bus.orst.edu/faculty/nielson/rm/chapter8.htm.

Care has to be taken when using exclusion clauses as a means of managing risk as the transfer of risk is prohibited in relation to particular transactions. For example, the exclusion of warranties implied under consumer protection legislation is prohibited in relation to the sales of goods to consumers. Many risk control techniques such as exposure avoidance, loss reduction and contractual transfer are familiar to legal practitioners and corporate counsel as strategies for managing legal risk and it is reasonable to conclude that the risk control strategies used in risk management can equally be used in the context of legal risk.

2.4.4.2 Risk financing techniques

Risk management strategies that employ *risk financing* techniques use techniques that make available funds to pay for losses that arising in the event that a risk eventuates. Risk financing techniques are further categorised into two subcategories, *risk retention* and *risk transfer*:

> For both private and public organizations, risk financing techniques can be classified into two groups: retention and transfer. Retention includes all means of generating funds from within to pay for losses. Transfer includes all means of generating funds from outside the organization to pay for losses. While this distinction between retention and transfer is useful in analyzing and planning to meet an organization's risk financing needs, some hybrid form of risk financing is often used. [174]

In relation to *risk retention*, a business may choose to retain a risk by paying for losses, as and when they arise. Alternatively, a business may retain a risk and set aside funds on an annual or regular basis to cover any losses arising from a risk that

---

[174] Head and Horn, *Essentials of Risk Management*, http://www.bus.orst.edu/faculty/nielson/rm/chapter1.htm.

eventuates. Such an approach, although saving a business from having to spend funds on other risk management strategies, does have its attendant risks:

> There can be administrative problems, however, with such a fund. Criteria for the acceptance of claims against the fund must be laid down, and internal standards of proof of loss should not be less stringent than those an insurer would apply. Unless this is done the fund may be exploited by the wilier parts of the organisation as a useful additional budget or contingency fund.
>
> There is also the danger that if there is a healthy balance in the fund for several years, and claims upon it are low, it may be "borrowed" to finance other activities within the organisation, so that when the more serious claims come along, the funds is insufficient to meet them.
>
> The fund, too, must be adequately financed when it is set up. If it has to rely on the gradual accumulation of funds from contributions, the organisation may find itself insufficiently protected against an unexpected run of claims early in the fund's life.[175]

Risk retention also encompasses "self-insurance" a term used to describe where a business retains the risks it faces and deals with them by employing insurance techniques[176]. Thus self-insurance involves a business separating the costs associated with funding for risks, that is (administrative costs, average predictable losses and unpredictable losses and funding these costs although it is normal to transfer (obtain external insurance) for those losses that fall into the third category of unpredictable losses[177].

In relation to *risk transfer* strategies, a common form of risk transfer is the use of insurance. Whilst in the past, insurance was used often as a blanket risk management strategy, most risk management writers today consider that the use of insurance should be used more judiciously, as its use in relation to some risks is simply not

---

[175] Crockford, p 40.

cost-effective. Insurance, however, is advocated where the risks are catastrophic in nature or have an adverse effect on operating results[178]. The use of self-insurance can result in cost savings for a business due to the elimination of brokerage fees and high premiums. For example, the corporation Fletcher Challenge has recently adopted a philosophy of self-insuring where possible. This has resulted in savings of at least $20 million per year in premiums[179]. Fletcher Challenge uses self insurance for all losses other than those losses that are considered catastrophic or are required by government legislation[180].

Another form of risk transfer is for the business to borrow funds to meet losses if and when they arise. This strategy too can have its attendant risks:

> The alternative method of non-insurance financing of risk is to borrow the funds necessary to meet losses as they arise. This is a method which is not often chosen, because the fluctuations of the credit market may mean a lower degree of certainty that funds will be available to meet a loss than may be required. This is particularly true if recourse is made to normal credit facilities to meet a loss. Not only may the loss occur at a time when the amount of credit available is restricted, but the loss itself, if it happens to be of a major asset, may diminish the organisation's bargaining power in seeking further credit. [181]

Again, many if not all risk transfer techniques are already familiar to legal practitioners and there is little doubt that these strategies can be used in relation to the management of legal risk.

---

176 Vaughan, pp 212-213.
177 Vaughan, p 324.
178 Standards Australia/Standards New Zealand Joint Technical Committee on Risk Management, p 35.
179 John McDonald, "Risk Management in a Large Corporate Organisation", in David Elms, Editor, *Owning the Future- Integrated Risk Management in Practice*, Centre for Advanced Engineering, University of Canterbury, Christchurch, New Zealand, August 1998, Chapter 9, p130.
180 Maynard, p138.

2.4.4.3 Determining which risk management strategy to implement- the overriding factors

There are two overriding considerations for a business when deciding which risk control or risk financing strategy to implement:

2.4.4.3.1 The effect that each possible strategy may have on the business's ability to fulfil its objectives (as identified in Step 1 of the risk management process).

Thus, each possible risk management strategy is assessed in terms of the extent to which its implementation achieves the risk criteria/ objectives of the business (which set out the levels of risk that are acceptable to the business). In other words, the business needs to establish that the implementation of a given risk management strategy will bring the level of risk within a level acceptable to the business.

2.4.4.3.2 The effectiveness and cost effectiveness of each possible risk management strategy

Cost-effectiveness is an important factor when determining which risk management strategy to implement but other factors concerning effectiveness such as whether the risk management strategy achieves legal compliance or the humanitarian objectives may be relevant[182].

The cost-effectiveness of adopting a particular risk management strategy is calculated by reference to the maximum amount of loss a business can retain. As part of the risk management process, a business must determine the maximum annual loss that it can afford to retain. Such level is determined by reference to various financial indicators, some of which will be considered below in more detail, including the

---

[181] Crockford, p 40.
[182] Head and Horn, http://www.bus.orst.edu/faculty/nielson/rm/chapter1.htm.

business's cash flow, liquid reserves and external funds available to it in the event that a risk eventuates[183]. Such an amount may be expressed as a variable amount:

> For example, a given organization might establish a maximum retention level for all retained losses during any fiscal year as the larger of, say, $50 000 or 10% of the firm's annual working capital.[184]

2.4.4.4 Some further considerations when determining which risk management strategy to adopt

Risk management methodology lays down a number of guiding principles which aid in determining which risk management strategy to adopt:

2.4.4.4.1 The *degree* of *likelihood* and *consequence* is an indicator for determining which risk management strategy to adopt

The *degree* of *likelihood* and *consequence* is influential when determining which risk management strategy to adopt. It is generally accepted that a risk whose consequence is low but has a high likelihood of occurring should be retained and managed by a business[185] largely because the transfer of such risk through insurance is unlikely to be economical as premiums are likely to be high[186]. In relation to risks that have a medium consequence, but whose likelihood of occurring is low it may also be more economical for a business to retain such risks provided that the business has sufficient reserves[187]. In relation to risks that have a high consequence but low likelihood of occurring, such risks should not be retained but should be transferred by

---

183 Vaughan, p 100.
184 Vaughan, p 101.
185 TA Salter, "The indivisibility of risk- the need for its systematic analysis and treatment", *Benefits and Compensation International*, May 1997, volume 26 no 9, pp 7-18; Vaughan, p 66.
186 Vaughan, p 64.
187 Salter, pp 7-18.

way of insurance[188]. In relation to those risks whose consequence is low, and whose frequency is low, such risks should be retained by the business[189]. Whilst the extent to which a risk is predictable can assist in determining which risk management strategy to employ it should be noted that it is not appropriate to take into account this factor where the potential loss is so great that it may render a business insolvent or bankrupt[190]. In such instances, it is more appropriate to use minimax cost (ascertaining the costs associated with each strategy and choosing the strategy whose cost 'corresponds to the minimum of the maximum costs'[191]) or minimax regret strategies (measuring the difference in cost to the business ("regret") that the adoption of each strategy may cause and choosing the strategy that minimises the regret[192]) to determine which risk management strategy to employ.

Table 26 *DEGREE* OF *CONSEQUENCE* AND *LIKELIHOOD* OF RISK CAN ASSIST DETERMINING WHICH RISK MANAGEMENT STRATEGY TO ADOPT

LIKELIHOOD	CONSEQUENCE	RISK MANAGEMENT STRATEGY
High	Low	Retain risk.
Low	High	Transfer risk by way of insurance.
Low	Medium	Retain risk provided business has sufficient resources.
Low	Low	Retain risk.

188 Salter, pp 7-18; Vaughan, p 66.
189 Vaughan, p 66; Ron S Dembo, Andrew Freeman, *Seeing Tomorrow: Rewriting the Rules of Risk*, John Wiley & Sons, Inc, New York, 1998 pp 82-84.
190 Vaughan, p 65.
191 Vaughan, p 61.
192 Vaughan, p 62.

2.4.4.4.2 The business's loss bearing capacity is a key consideration when determining whether to implement a risk management strategy that involves risk retention

Clearly, when determining whether to retain a risk, a key consideration is whether the business could afford to bear the maximum potential loss that could result in the event that the risk eventuates. If the maximum potential loss associated with a given risk would result in the business becoming insolvent or bankrupt, or would seriously impair the business's operations, such risk should not be retained unless the consequence of the risk can be minimised to a loss that can be managed. Furthermore, where the consequence of risk predicted cannot be minimised nor transferred the risk should be avoided[193].

A legal adviser providing legal risk management advice to a business will need to seek instructions from the business as to what the business's assessment is of its loss bearing capacity. For risk managers or in-house counsel employed by a business, who may have to calculate the loss bearing capacity of the firm themselves, the loss bearing capacity of a business can be calculated by reference to one of several financial indicators:

Ascertaining the *resources* of the business that are available to pay for losses incurred as a result of a risk eventuating.

Alternatively, the *working capital* of a business is a good, if not the best, measure of a business's ability to withstand unexpected loss when discussing how to calculate a business's loss bearing capacity in order to determine whether to retain a particular

---

[193] Vaughan, p 63.

risk[194]. A standard risk management text notes that there is no specified percentage of working capital which should be taken as an indicator of a business's capacity to bear loss, and that anything between 19 percent up to 25 percent of a business's working capital is considered to indicate a business's loss bearing capacity[195].

> Ten percent might be used when the firm is inventory intensive and cannot liquidate current assets without financial loss. The high range might be used when the firm has a very liquid working capital position[196].

A business's *total assets* may also be useful as an indicator of a business's loss bearing capacity. A range of between 1-5% of a business's total assets is suggested to constitute a business's loss bearing capacity[197]. However, this financial indicator is not so useful as the working capital of a business as it does not provide an indication of a business's short- term availability of funds[198].

Other financial indicators may be also useful for ascertaining a business's loss bearing capacity.

For example, "[a] range of 5 to 10 percent of the *preceding year's nondedicated cash flow* [emphasis added] is an appropriate measure of the funds available for allocation to the retention program" [199]. This therefore is an indicator of the unexpected losses a business is capable of bearing.

It has been cautiously suggested that a business's capacity to bear unexpected loss can be gauged by measuring a business's *ability to fund losses through earnings*. This

---

194 Vaughan, p 319.
195 Vaughan, p 319.
196 Vaughan, p 319.
197 Vaughan, p 319.
198 Vaughan, p 319.

requires examining a business's retained earnings over an extended period and taking a percentage of these earnings to represent the business's capacity to bear loss[200].

Similarly, a business's capacity to bear loss may be ascertained by reference to its *annual sales*. It has been suggested that a range of 0.5 to 2 percent of annual sales or revenues is an indicator of the loss bearing capacity of a business[201].

In relation to listed public companies, a business's *earnings per share* can be used to gauge its loss bearing capacity, a figure of 10 percent of the earnings per share being suggested as an indication of the business's loss bearing capacity[202].

Finally, a business's *cash flow* may also provide a useful indicator of a business' capacity to bear loss: "A range of 5 to 10 percent of the preceding year's nondedicated cash flow is an appropriate measure of the funds available for allocation to the retention program."[203]

2.4.4.4.3 Account should be taken of associated costs when calculating the cost effectiveness of a particular risk management strategy

In calculating the cost effectiveness of each possible risk management strategy it is important to consider all associated costs. For example, when calculating the cost associated with transferring a risk it is important to include: '...whatever the transferee entity charges for its acceptance of the risk, plus the cost of supplying the entity with necessary information, and the costs of monitoring or reducing the risk as

---

199 Vaughan, p 319.
200 Vaughan, p 319.
201 Vaughan, p 319.
202 Vaughan, p 319.
203 Vaughan, p 319.

required by the transferee entity'[204]. Similarly, in calculating the cost of retaining a risk the business should take into account the cost of monitoring the activity for any increase in likelihood of the risk eventuating[205].

2.4.4.4.4 A business should only accept or retain a risk that it cannot control.

A business should not accept or retain a risk over which it has no control[206]. The underlying principle here is that a business should not assume responsibility for a risk for which it lacks the capacity to manage effectively. Thus, a business should consider implementing risk transfer strategies in relation to risks outside its control. In practice, however, it may be unrealistic and not cost-effective to achieve this.

2.4.4.4.5 It is important that the risk management strategies implemented reflect the business's/ management's attitude to risk taking

Factors such as individual attitude to risk taking, the culture of the organisation, the type and nature of work and the culture of the business can influence the risk management strategy selected for implementation[207]. The person undertaking the risk evaluation process should therefore take care to reflect the business's (management's) policy on taking risk rather than reflecting his or her personal attitude to risk taking when determining which risk management strategy to implement. It is interesting to note that a partner of a top tier law firm who provided a response to the self-completion questionnaire on how risk management is used in the

---

204 Katherine Taylor Eubank, "Paying the Costs of Hazardous Waste Pollution: Why is the Insurance Industry raising such a stink?", *University of Illinois Law Review*, 1991, 173, 189.

205 Taylor Eubank, p. 189.

206 Purchasing Australia, Commonwealth of Australia, *Managing risk in procurement- A handbook*, Australian Government Publishing Service, Canberra, 1996, Chapter 1 at p 4, and Chapter 2 at p 26.

207 Purchasing Australia, p 30.

context of legal risk, identified that client attitude to risk (as well as budgetary considerations) is relevant when evaluating which risk management strategy to implement.

2.4.4.5 The risk evaluation process involves quantitative and qualitative approaches

As can be seen, the risk evaluation process can involve both quantitative and qualitative approaches. These approaches, in particular the quantitative approaches, require reference to information that is particular to a business. Whether legal risk management can be used, at a generic level, to evaluate risk management strategies that may generally be useful for managing legal risk will be investigated in the second part of this thesis when risk management is applied in the context of Internet commerce.

Set out below is a checklist for Step 4 of the legal risk management process:

Table 27 CHECKLIST FOR STEP 4 OF THE LEGAL RISK MANAGEMENT PROCESS

EVALUATING AND SELECTING RISK MANAGEMENT STRATEGIES

1. For each legal risk identify the range of risk management strategies are available	RISK CONTROL TECHNIQUES: ♦ Exposure avoidance ♦ Loss prevention ♦ Loss reduction ♦ Segregation of loss exposures (separation and duplication) ♦ Contractual transfers of financial or legal risk RISK FINANCING TECHNIQUES: ♦ Risk retention- putting aside funds from

	within the business such as choosing to pay for losses as and when they arise, setting aside funds on annual or regular basis to cover any losses arising from a risk that eventuates. ♦ Risk transfer – obtaining funds from outside the business including insurance, borrowing funds to meet losses when and if they arise.
2. For each legal risk select appropriate risk management strategy to implement	TECHNIQUES FOR EVALUATING AND SELECTING RISK MANAGEMENT STRATEGIES: The overriding considerations are: ♦ the effect that each possible strategy may have on the business's ability to fulfil its objectives and; ♦ the effectiveness and cost-effectiveness of each possible risk management strategy. Other considerations include: ♦ *Degree* of *consequence* and *likelihood* of risk. ♦ A business's loss bearing capacity. A business's loss bearing capacity can be ascertained from the following financial indicators: ♦ The resources of a business that are available to pay for losses incurred as a result of a risk eventuating. ♦ The business's working capital. ♦ The business's total assets. ♦ The preceding year's non dedicated cash flow. ♦ The business's ability to fund losses through earnings. ♦ The business's annual sales. ♦ The business's cash flow. ♦ Associated costs. ♦ Retaining or accepting only those risks

	within the control of the business. ♦ Ensuring that risk management strategy selected reflects the business's/management's attitude to risk taking.
3. It may be relevant to communicate with the business's stakeholders when determining which risk management strategies to implement.	
4. Document this step.	See sample document set out at Table 28 at p 111.
5. Monitor and review.	The outcome of this step should be periodically reviewed to take into account changes in circumstances that affect the effectiveness of the legal risk management strategies implemented.

The following is a sample Risk Register for documenting step 4 of the legal risk management process:

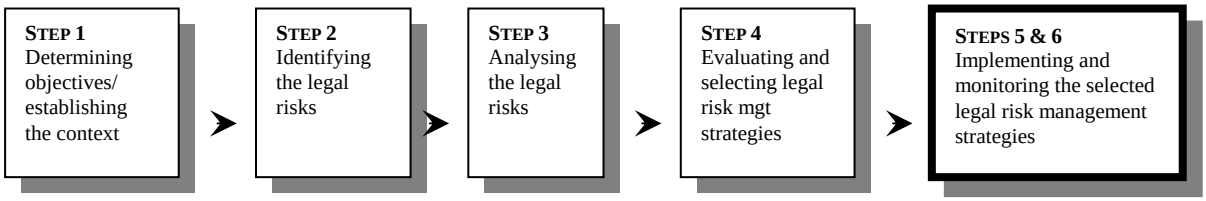
Table 28 SAMPLE RISK REGISTER FOR STEP 4 OF THE LEGAL RISK MANAGEMENT PROCESS (ADAPTED FROM SECTION H: RISK MANAGEMENT DOCUMENTATION, *AS/NZS 4360 -1999 RISK MANAGEMENT* (REVISED))

RISK REGISTER (PART 3 OF 4)					
Date of this Review:					
Next Review Date:					
Compiled by:					
Approved/Reviewed by:			**Date:**		
Legal risks listed in order of priority according to the level of risk [refer to Part 2 of 3 to ascertain the level of each risk]	**Risk management strategy/strategies available**	**Risk management strategy/ strategies selected and reasons for selection**	**Employee responsible for implementing risk management strategy/ strategies**	**Timetable for implementation**	**Review date** [include name of employee responsible for undertaking review of implementation and effectiveness]

2.4.5 STEPS 5 AND 6: IMPLEMENTING THE SELECTED RISK MANAGEMENT SYSTEM AND MONITORING AND REVIEWING IT ON AN ONGOING BASIS.

Figure 7 depicts steps 5 & 6 of the risk management process as it applies in the context of legal risk.

Figure 7 LEGAL RISK MANAGEMENT: STEPS 5 & 6



The fifth and sixth step in the risk management process is to implement a risk management system and to monitor such system on an ongoing basis. A risk management system comprises three aspects: (i) implementation of the strategies selected to manage the identified risks; (ii) monitoring and conducting training and awareness programs to ensure ongoing compliance with the implemented strategies; and (iii) undertaking periodical reviews of the risk management strategies that were implemented and modifying them to reflect new situations that, over the passage of time, have arisen. This aspect includes reviewing the techniques used for identifying risk, reviewing the techniques used to assess each risk and evaluating and reviewing the risk management strategies that a business has implemented (including enquiring why a particular strategy was chosen over another). In addition, a review of a business's objectives in relation to risk management should be periodically reviewed.

Principal responsibility for implementing and ensuring that the risk management system implemented works must lie at the business unit level. That is, each manager must bear the responsibility within his or her area of control of implementing and overseeing the risk management system adopted by the business. The corporation Fletcher Challenge, for example, in its Risk Management Policy Statement, clearly allocates principal responsibility to its managers:

> Every manager has a prime responsibility for eliminating, within the area of his or her control, all conditions and practices which increase hazard or the likelihood of fortuitous loss.
>
> Each manager is accountable for both the frequency and the cost of any:
>
> - property loss or damage;
>
> - injury;
>
> - consequent reduction in earning capacity; and
>
> - any consequent increased cost of operating which may occur from any cause within the area under his or her control.
>
> Each business unit must develop and implement suitable loss prevention programme and business continuation plan for its size, the nature of its operations and the risks to which it is exposed[208].

Other aspects of the risk management system adopted by the business such as monitoring and review can be undertaken by parties outside the individual business unit or even outside the business.

In order to be effective, the process of monitoring and review should: (i) encompass all of the risks faced by a business, (ii) be available very quickly after the review and monitoring has taken place and (iii) result in prompt action in the event that the risk management system implemented requires modification[209].

Clearly, a business must be committed to each aspect of these steps if it is to achieve the risk management objectives it sets. Some writers have suggested that, as part of this commitment, a business should make known the importance it places on risk management through the form of a risk management policy statement that sets

---

[208] Maynard, p135.
[209] Chicken, p 204.

out the risk management objectives the business seeks to achieve.[210] Such policy should also specify that all employees are responsible for the implementation of the business's risk management system and also identify those employees who are responsible for ensuring compliance and for ongoing review of the risk management strategies affecting the areas of the business that they manage[211]. This could be reinforced by introducing accountability should losses result as a consequence of risks eventuating:

> The policy must be enforced by writing accountability for risk management performance into job descriptions. In most companies it will be necessary for this accountability to be expressed in the same terms as others, such as a financial budget, or a target to be met. This in turn will mean that there must be a mechanism for the direct and indirect costs of loss to be included as a factor in reviewing management performance, since they represent risk not managed.[212]

The formulation of a risk management policy is additionally useful in that by setting out the objectives of a business's risk management system, a standard against which risk management strategies can be evaluated and chosen, is provided:

> Just as the organization needs a formal policy with respect to its other activities, a risk management policy can help provide guidance for the risk manager and the risk management department.[213]

Interestingly, some researchers have discovered that "codes of conduct", which presumably can be equated to risk management policy statements, are ineffective in

---

[210] Crockford, p 104. See also *AS/NZS 4360- 1999, Risk Management*, Appendix B in which it is advocated that a business develop and document its policy on risk management. See also *Guidelines for Managing Risk in the Australian Public Service*, Joint publication of the Management Advisory Board and its Management Improvement Advisory Committee, Report No 22, AGPS, Canberra, October 1996.

[211] Crockford, p 104.

[212] Crockford, p 104.

[213] Vaughan, p 98.

terms of achieving employee compliance[214]. Instead it has been suggested that hotlines, provided that they were not staffed by the business's in-house counsel or outside lawyers or an outside answering service were more effective[215]. The most effective hotline approach was if the hotline was staffed by a named representative who was an employee of the business, which also involved a policy of non-retribution policy for those that used the hotline[216].

Finally, in order to be effective, risk management should form part of a business's general management and planning processes and, because the implementation of a risk management strategy may involve significant organisational change, responsibility for its implementation should be given to a person in the business who has sufficient authority to make such decisions[217].

Whilst the fifth and sixth steps in the risk management process are, in practice, an integral part of the risk management process, in relation to the research issue examined in this thesis, it is not necessary to examine these aspects in detail. This is because, unlike the other aspects of risk management, it is clear that the procedures

---

214 Findings of Dr Mark Pastin, President of the Council of Ethical Organizations in relation to research carried out on employee perceptions of company ethics policies and practices: http://www.www.cyberinstitute.com/preventivelaw/polices.htm.

215 Findings of Dr Mark Pastin, http://www.www.cyberinstitute.com/preventivelaw/polices.htm.

216 Findings of Dr Mark Pastin, President of the Council of Ethical Organizations in relation to research carried out on employee perceptions of company ethics policies and practices entitled "A study of organizational factors and their effect on compliance" in *Proceedings of the Second Symposium on Crime and Punishment in the United States, DC Corporate Crime in America-Strengthening the "Good Citizen" Corporation*, United States Sentencing Commission, September 8 1995, Washington, page 142.

217 Katharine Reid, Eugene Clark and George Cho, "Legal Risk Management for Geographic Information Systems", *Journal of Law and Information Science* , Volume 7 No 2, 1996, p 170. See also paras 3.2.1 and 3.2.4 of Australian *Standard AS 3806-1998, Compliance Programs*, Standards Australia, Homebush NSW, 5 February 1998.

for implementing this step of risk management and undertaking monitoring and ongoing review can be applied equally in relation to legal risk management. The Australian Standard *AS 3806 -1998 Compliance Programs*, for example, demonstrates this when it specifies in considerable detail how this aspect of the risk management process should be implemented in relation to legal compliance risk, its specifications closely mirroring standard risk management practice. Although the Australian Standard *AS 3806 -1988 Compliance Programs* restricts its discussion of legal risk to compliance risk it is suggested that the approach specified in this standard and advocated generally in the risk management texts applies more broadly to also include the other legal risks with which legal risk management is concerned, that is the legal risks of exposure to immense liability and loss of legal rights and interests. Also, considerable guidance for implementing a risk management strategy is set out in Australian Standard *AS/NZS 4360 -1999 Risk Management.*

Set out below is a checklist for Steps 5 & 6 of the legal risk management process:

Table 29 CHECKLIST FOR STEPS 5 AND 6 OF THE LEGAL RISK MANAGEMENT PROCESS

IMPLEMENTING THE SELECTED RISK MANAGEMENT STRATEGIES AND MONITORING AND CONDUCTING AN ONGOING REVIEW OF THE LEGAL RISK MANAGEMENT SYSTEM IMPLEMENTED

1. Obtain approval from senior management to implement selected legal risk management strategies.	Approval should include budget approval
2. Inform employees of legal risk management strategies affecting the areas of the business in which they work.	It may be useful to distribute a legal risk management policy statement.
3. Identify those employees who will be given responsibility for implementing the risk management strategies affecting the areas of	Clearly, employees selected should hold sufficient authority to implement the legal risk management strategies and ideally should be the managers responsible for the activity for

the business that they manage.	which the legal risk management strategy is being implemented. Provision is made for this in sample Risk Register Part 3 of 4 set out at Table 28 at p 111.
4. Conduct individual briefing sessions for those employees or training sessions to inform those employees of their particular responsibilities.	
5. Set down a review date by which the legal risk management strategies must be implemented.	Provision is made for this in sample Risk Register Part 3 of 4 set out at Table 28 at p 111.
6. Check periodically that those employees who are responsible for ensuring compliance and for ongoing review of the legal risk management strategies affecting the areas of the business that they manage continue to work in that position. Appoint and train replacements where required.	Update documentation [For example, sample Risk Register Part 3 of 4 set out at Table 28 at p 111 needs updating after this process is completed].
7. Ensure that these employees are made aware of their obligations through training in legal risk awareness.	Provide periodic ongoing training.
8. Introduce a monitoring system, such as a hotline, that all employees are encouraged to use to report instances of non-compliance or problems with the legal risk management system implemented.	Those hotlines that have been proven effective are those that involve appointing a named employee as the relevant hotline contact where there is a policy of non-retribution for those that used the hotline. In addition, it may be relevant to make the hotline open to external stakeholders of the business.
9. Review the business's risk criteria and ensure that the legal risk management system implemented reflects those criteria. Also, ensure that the legal risk management objectives of the business continue to align with the business's overall objectives. It may be necessary again to communicate and consult with the business's stakeholders.	Update documentation [For example, sample Risk Register Part 1 of 4 set out at Table 11 at p 49 needs updating after this process is completed].
10. Review the identified legal risks. Determine whether new legal risks arise. Discount legal risks that may no longer exist, such as where the business has ceased an activity that gave rise to a legal risk, or where legislation eliminates a legal risk.	Update documentation [For example, sample Risk Register Part 2 of 4 Table 25 at p 94 needs updating after this process is completed].
11. Review the effectiveness, legality and cost of implementing and maintaining implemented legal risk management	Update documentation [For example, sample Risk Register 3 of 4 set out at Table 25 at p 111 needs updating after this process is

strategies.	completed].
12. Review the budget allocated for legal risk management and obtain approval from senior management for ongoing financial expenditure on legal risk management.	
13. Document this step.	See references to sample Risk Register (Part 2 of 4 set out at Table 25 at p 94 and Part 3 of 4 set out at Table 28 at p 111) above and the sample Risk Register Part 4 of 4 set out at Table 30 at p 118.

The following is a sample Risk Register for documenting steps 5 and 6 of the legal risk management process:

Table 30 SAMPLE RISK REGISTER FOR STEPS 5 AND 6 OF THE LEGAL RISK MANAGEMENT PROCESS

RISK REGISTER (PART 4 OF 4)	
Date of this Review:	
Next Review Date:	
Compiled by:	
Approved/Reviewed by:	**Date:**
Frequency of review of legal risk management system (circle relevant frequency):	Review 1 due at: [insert date]
	Review 2 due at: [insert date]
Every six months	Review 3 due at: [insert date]
Annually	Review 4 due at: [insert date]
Every two years	Review 5 due at: [insert date]
Every three years	
REVIEW 1	
Date review commenced:	[date]
Legal risk criteria and objectives reviewed and Risk Register updated (See sample Risk Register Part 1 of 4 set out at Table 11 at p 49):	[date]
Legal risks reviewed and Risk Register updated (See sample Risk Register Part 2 of 4 set out at	[date]

Table 25 at p 94):	
Legal risk management strategies reviewed and Risk Register updated (See sample Risk Register Part 3 of 4 set out at Table 28 at p 111):	[date]
Additional resource requirements specified and approval received. Risk register updated (See sample Risk Register Part 3 of 4 set out at Table 28 at p 111) to reflect this:	[specify name of person giving approval and date]
Risk management policy statement (if such statement exists] reviewed and updated:	[date]
Employees who are responsible for ensuring compliance and for ongoing review of the legal risk management strategies contacted to confirm that they continue to work in the business and their legal risk management responsibility is still appropriate:	[date]
Replacement employees responsible for ensuring compliance and for ongoing review of the legal risk management system appointed and trained and Risk Register updated (See sample Risk Register Part 3 of 4 set out at Table 28 at p 111):	[date on which this task is completed]
Update Risk Register (Sample Risk Register Parts 1-4 will need to be updated) with next review date:	
REVIEW 2	
Date review commenced:	[date]
Legal risk criteria and objectives reviewed and Risk Register updated (See sample Risk Register Part 1 of 4 set out at Table 11 at p 49):	[date]
Legal risks reviewed and Risk Register updated (See sample Risk Register Part 2 of 4 set out at Table 25 at p 94):	[date]
Legal risk management strategies reviewed and Risk Register updated (See sample Risk Register Part 3 of 4 set out at Table 28 at p 111):	[date]
Additional resource requirements specified and approval received. Risk register updated (See sample Risk Register Part 3 of 4 set out at Table 28 at p 111) to reflect this:	[specify name of person giving approval and date]
Risk management policy statement (if such statement exists] reviewed and updated:	[date]

Employees who are responsible for ensuring compliance and for ongoing review of the legal risk management strategies contacted to confirm that they continue to work in the business and their legal risk management responsibility is still appropriate:	[date]
Replacement employees responsible for ensuring compliance and for ongoing review of the legal risk management system appointed and trained and Risk Register updated (See sample Risk Register Part 3 of 4 set out at Table 28 at p 111):	[date]
Update Risk Register (Sample Risk Register Parts 1-4 will need to be updated) with next review date:	[date on which this task is completed]

2.4.6 CONSULTING AND COMMUNICATING WITH STAKEHOLDERS

An additional element of the risk management process involves communicating and consulting with both internal and external stakeholders (those who have a vested interested in or are affected by the activities of the business) in relation to the risk management system at all stages of its development and on a continuing basis[218]. The Australian Standard *AS/NZS 4360 -1999 Risk Management* states that the term "stakeholders" extends to persons within the business (such as employees, management and senior management) and to parties outside the business (such as trading partners, union groups, financial institutions, regulators, politicians, non-government organisations, customers, suppliers, the media and community groups[219]. The reason for consulting stakeholders is:

> Effective internal and external communication is important to ensure that those responsible for implementing risk management, and those with a vested

[218] See *AS/NZS 4360- 1999, Risk Management*, at para 4.7.
[219] *AS/NZS 4360- 1999, Risk Management*, Appendix C.

interest understand the basis on which decisions are made and why particular actions are required[220].

2.4.7 DOCUMENTING EVERY STEP IS INTEGRAL

Each step undertaken of the risk management process needs to be documented. Documentation of the risk management process is important for several reasons. First, it may be useful in litigation proceedings commenced against the business to establish, for example, that the business met the reasonable standard of care or that due diligence had been undertaken in relation to achieving statutory compliance. In addition, documentation facilitates transparency, that is, the reasons for particular decisions assessments that are made during the risk management or, for example, justification for adopting a particular management strategy or assessing a particular risk to be low are clearly expressed. The Auditor- General, in a review of the Australian Taxation Office approach to risk management, listed several other benefits that flow if the risk management process is documented including: that documentation provides senior management with a plan for approval and implementation; it also provides continuity and corporate memory when/if changes in personnel occur, and it enables review of the risk management process to be undertaken[221].

Clearly, cost-benefit considerations will determine the level of documentation that is undertaken[222]. A sample four part Risk Register for documenting the legal risk

---

220 *AS/NZS 4360- 1999, Risk Management*, at para 4.7.

221 The Auditor-General, *Risk Managemen in thet Australian Taxation Office*, Commonwealth of Australia, Audit Report No. 37, 1996-1997, para 3.44

222 The Auditor-General, *Risk Management in theAustralian Taxation Office*, para 3.44

management system implemented is provided in this thesis at Table 11 at p 49 (Part 1), Table 25 at p 94 (Part 2), Table 28 at p 111 (Part 3) and Table 30 at p 118 (Part 4).

Having emphasised the importance of keeping records it should, however, be noted that the information recorded may well incriminate the business or its management and employees in relation to breaches of the law or liability under contract or tort. The documentation recording a business's legal risk management system must therefore be carefully planned in order to avoid such documentation being used by regulators or claimants against the business to support a case against the business. One technique that may protect against a business's legal risk management records being used in this way is the use of legal professional privilege. It may however not always be possible to establish legal professional privilege given the limits of its application to confidential communications between clients and their lawyer for the sole purpose of obtaining legal advice or in relation to litigation. It is beyond the scope of this thesis to consider this issue in detail and it is noted in the conclusion that this is an area for further research.

2.5 Legal risk management vs preventive law vs legal compliance

It is relevant at this point to examine the differences between legal risk management, preventive law and legal compliance and to consider why legal risk management is preferred over the other methods for identifying and managing legal risk.

Legal risk management is similar to what is commonly referred to, at least in the United States, as *preventive law*. Preventive law seeks to achieve many, if not all of

the objectives of legal risk management and the methods employed in each approach do overlap. In the words of its founding proponent, Louis M Brown, preventive law "help[s] people stay within the bounds of law (ie. minimise the risk of legal trouble); and take advantage of legal opportunities (ie. maximise the legal benefits)"[223]. Louis M Brown with co-author Edward A Dauer further described preventive law as follows:

> As contrasted with dispute-resolving law, preventive law (more accurately but less elegantly: preventive lawyering) deals with the avoidance of dispute, and with the structuring of relations and transactions apart from any extant dispute. It connotes negatively in its avoidance thrust, but positively in its planning and structuring. At the heart of the practice of preventive law is the relationship between lawyer and client. Here the components of that dyad change in their emphases: the client's goals are more creative and less curative; the lawyer is more counsellor than champion; and the balance of knowledge and authority between the lawyer and his client may be far different from its more familiar dispute-context form[224].

As with legal risk management, a preventive law approach requires the law regulating a business's activities to be viewed in terms of what legal risks they pose to businesses. Preventive law has as its objectives the aim of decreasing the likelihood that a business will be sued and increasing the likelihood that a business preserves its legal rights[225]. It is interesting to note that the objective of "decreasing the likelihood that a business does not comply with statute law" was not identified by the author quoted, given that the preventive law literature clearly contemplates that this objective be included as part of preventive law. Thus, it would appear that the

---

[223] Louis Brown, *The Other Side of the Law* , 1 June 1995, as quoted in Preventive Law, an on-line course, http://www.cyberinstitute.com/preventivelaw/week1.htm.

[224] Louis M Brown and Edward A Dauer, *Planning by Lawyers: Materials on a Nonadversarial Legal Process*, The Foundation Press, Mineola, New York, 1978, p xix.

objectives of preventive law are much the same as the objectives of legal risk management.

Some commentators claim that preventive law is a far broader concept than legal risk management. One academic commentator has argued that preventive law encompasses the following features, only the first of which is featured in legal risk management: (a) systematic risk assessment and corresponding risk avoidance activities, (b) systematic monitoring to detect the development of adverse legal circumstances at the earliest possible points, and (c) affirmative reactive effort to respond to identified problems and to minimize the adverse impacts of those problems[226]. It is submitted here that legal risk management can encompass the second and third described features. As discussed earlier in this chapter, the six-step legal risk management model contemplates that any legal risk management system implemented must be monitored and reviewed on an ongoing basis, in part, to identify and manage new legal risks that may arise. Similarly, the six-step model incorporates mechanisms for responding to identified problems and minimising the adverse impacts of those problems.

Although it is beyond the scope of this thesis to conduct a detailed comparison of the methodologies used in both disciplines, on a preliminary comparison, preventive law does not appear to involve as systematic and consistent approach to identifying and managing legal risk as legal risk management.

---

[225] Louis M Brown assisted by Edward Rubin, *Manual of Preventive Law*, Prentice-Hall, Inc, 1950, p 7.

The methodology advocated in preventive law texts is not as clearly defined as risk management methodology. Whilst preventive law literature describes a number of techniques for the practise of preventive law, how these techniques should be combined in order to achieve a systematic outcome is unclear. Some of the principal techniques used in practising preventive law include: "film rewinding"[227], "legal autopsy"[228], "periodic legal checkups", "pre-trying potential disputes"[229], "creating and preserving evidence", "preventive analysis", using legal drafting as a preventive law tool (for example to insert a contractual clause to limit damages that are payable in the event of a breach of contract by a party) and searching for legal issues other than those for which the client has sought legal advice and bringing this to the attention of the client[230].

Several of these techniques require further explanation. "Film rewinding" is the method by which a legal dispute or transaction is "rewound" back from the conflict or legal dispute stage to a point where preventive action could have been taken to avoid the conflict or legal dispute arising:

> As a pedagogical device - in law school teaching, for example - preventive law proponents also suggest a "rewind" technique. For example, after discussing an appellate decision in contract law, we might "rewind" the

---

226 E-mail from Richard Gruner (in correspondence addressed to the author), Professor of Law, Whittier Law School , dated 16 November 1998.

227 Robert M Hardaway, *Preventive Law - Materials on a Non Adversarial Legal Process*, Anderson Publishing Co., Cincinnati, 1997, pp xlii-xiv.

228 Robert M Hardaway, pp xlv-xlvii.

229 Louis M Brown and Edward A Dauer, *Planning by Lawyers: Materials on a Nonadversarial Legal Process*, p 327.

230 Robert M Hardaway, p xxxviii.

> situation back to the stage of drafting, and ask what might have been done differently to avoid the legal problem presented by the case[231].

A "legal autopsy" involves reviewing a case with a view to identifying how and why a legal issue arose or legal proceedings were commenced[232]. This information in turn can be used to develop internal procedures or handbooks to avoid such legal issue or legal proceedings arising in the future[233]:

> Louis Brown envisioned the use of a legal autopsy as a means of raising and answering a wide array of questions about how and why a case or lawsuit was initiated and conducted. For example: Why was certain evidence and not other evidenced introduced at trial? Why were some witnesses called and others not? Why were some witnesses cross-examined and others not-but most important, why was the case initiated in the first place? This in turn leads to such ultimate questions as what was the initial mistake that led the client into trouble, what led the client to seek the advice of counsel, and what advice was finally given to the client. Was the advice given by the lawyer sound, particularly the advice on whether to proceed to the litigation stage?[234]

The process of undertaking a "legal autopsy" can involve: examining public files such as pleadings, examining where possible the private files of the parties to the dispute, interviewing the lawyers involved n the case, interviewing the parties to the dispute, interviewing the witnesses and experts, and interviewing the judge and jurors[235].

A "periodic legal checkup" is essentially a legal audit designed to identify aspects of a business's activities that may in the future be the subject of legal dispute or

---

231 Marc W. Patry, David B. Wexler, Dennis P. Stolle, Alan J. Tomkins, "Conceiving the Lawyer as Creative Problem Solver: Article: Specific Applications: Better Legal Counseling Through Empirical Research: Identifying Psycholegal Soft Spots and Strategies", 34 *California Western Law Review* 439, Spring, 1998.

232 Robert M Hardaway, p xlv.

233 Robert M Hardaway, p xlvi.

234 Robert M Hardaway, p xlv.

prosecution. There are several types of audits that can be undertaken such as an acquisition audit (due diligence audit), a litigation audit, a compliance audit and a procedural audit:

> Acquisition-Audits. A legal audit of a seller's business is essential to a successful acquisition. In order to avoid assumption of unwanted liabilities and to assure that the combined operations realize the synergies sought by the management of the acquiring company, the acquisitions audit could include a review of the practices and procedures followed by the seller. It also could include an examination of the seller's contracts, pending litigation and status of prior years' tax returns.
>
> Litigation Audits. A legal audit of a particular transaction or corporate function can help the corporation avoid costly litigation and assure the successful outcome of litigation which is unavoidable. A litigation audit might include:
>
> Educating management regarding the likelihood of litigation and outcome of litigation resulting from a particular transaction or course of conduct.
>
> Advising management of practices that increase exposure to litigation (for example, unauthorized representations by marketing staff).
>
> Compliance audits. A compliance audit could be directed at evaluating corporate compliance with the laws governing the company's business. The key element of a compliance audit is to develop procedures to identify exposure resulting from violation of government laws and regulations.
>
> Procedural audits. A procedural audit can help keep the corporation in good legal health by detecting policies or procedures that could result in costly legal mistakes.
>
> For example, poorly worded contract or policies can result in unnecessary litigation between the corporation and its customers, suppliers and employees.
>
> A procedural legal audit could include an examination of purchase-order forms, sales-confirmation forms, corporate minutes, personnel policies and

---

[235] For a more detailed discussion of the process of undertaking a legal autopsy see Robert M Hardaway, pp xlviii- xlix.

> procedures, marketing policies and procedures and purchasing policies and procedures.[236]

"Pre-trying potential disputes" involves treating a transaction undertaken for a client as if it were disputed. From this process, potential issues can be identified:

> One such device is to hypothetically "pre-try" potential disputes during the planning and documentation stages. The lawyer may postulate, "Party A may, under such-and-such circumstances, be tempted to dispute facto or obligation X." He can then identify the issues which such a dispute would entail, the evidence relevant to resolution of the issues, and the effect of various dispositions of those issues. Plans can then be made as to how to make the issues moot, how to meet the evidentiary requirements, and how to render the impact of the dispute minimally disruptive[237].

"Creating and preserving evidence" refers to keeping records of the parties' purpose for entering into a transaction and their expectations, as such information can be decisive, in the event of a dispute, in how a court resolves a dispute as to the meaning or applicability of a contractual term. A technique for "creating and preserving evidence" would be set out the parties' objectives in the form of a recital[238].

"Preventive analysis" involves ascertaining a client's real goal, as opposed to the client's stated purpose, and then analysing the goal in terms of the legal results required to achieve the client's real goal and the non-legal elements. Then the required legal results are analysed to determine which rules of law can achieve the desired legal results:

---

[236] Michael L Goldblatt, "Legal Audits Can Help Companies Act Preventively", as reproduced in Robert M Hardaway, *Preventive Law - Materials on a Non Adversarial Legal Process,* Anderson Publishing Co., Cincinnati, 1997, p 194 at pp 194-195.

[237] Louis M Brown and Edward A Dauer, *Planning by Lawyers: Materials on a Nonadversarial Legal Process*, p 328.

> The preventive lawyer at this stage is reasoning "backward" compared to the brief writing lawyer; he is attempting to determine which presently nonexistent facts will yield the desired results when acted upon by the applicable rules of law. Any given legal result may be attained through the operation of different rule, although, of course, the facts will have to vary. The lawyer may therefore have a rather wide array of possible rules and combinations of rules to choose from. He must select the combination which depends on a set of facts which are the easiest, cheapest or safest to create and, perhaps even more importantly, which are possible within the framework of already existing facts[239].

Finally, the range of facts that will achieve the desired result are ascertained and whether it is possible to create those facts is considered[240]:

> It is at this point that the plan can be "debugged." The lawyer postulates the existence of all the facts which he tentatively plans to create, applies all those rules of law which he thinks may be invoked by a hypothetical adversary, and determines the extent to which the client's goal will be achieved, and whether previously unrecognized problems have been created. In other words, this stage involves running the planned transaction "forward." If the plan fails or creates other problems, the lawyer goes back to the drawing board, to try, in this order: (1) to adjust the nature of the facts, holding their general characteristics constant so that the rules will not change; (2) to adjust the set of rules to give the same results, and check the new facts which the new rules make necessary; and (3) to adjust the set of results necessary to accomplish the goal, to see if some other combination is possible. The lawyer will then work the new theory backward through rules, to facts, and then check it forward again."[241]

The preventive law literature, however, does not specifically state how each of the preventive law techniques should or could be used in order to achieve a consistent approach to preventing and managing legal risk. It would appear that this is a

---

238 Louis M Brown and Edward A Dauer, *Planning by Lawyers: Materials on a Nonadversarial Legal Process*, p 328.

239 L Brown & E Dauer, "Preventive Law- A Synopsis of Practice and Theory", ABA, *The Lawyer's Handbook*, c 3 at A3-7 to A3-10 (Rev.Ed. 1975) as reproduced in Robert M Hardaway, *Preventive Law - Materials on a Non Adversarial Legal Process*, Anderson Publishing Co., Cincinnati, 1997, p 143 at p 145,

240 L Brown & E Dauer, "Preventive Law- A Synopsis of Practice and Theory", p 145,

241 L Brown & E Dauer, "Preventive Law- A Synopsis of Practice and Theory", pp 145- 146,

conscious omission, as one preventive law author has noted in relation to the "preventive analysis" approach set out above that:

> …if taken structurally [the Brown and Dauer approach and another similar approach described by Corneel in relation to tax planning] would appear to be attempts to construct a problem solving routine. They are not. As Wickelgren observed, "non-formal" problems are not amenable to formal solution routines, since the outer limits of goal possibilities and information or givens cannot ever be stated.[242]

Thus, preventive law at least to the extent that it has developed to date does not provide guidance as to how to predict the legal consequences of undertaking a particular activity consistently across the range of legal risks that a business may face. Neither does preventive law provide a technique for evaluating a legal risk in the context of all the legal risks that a business faces, which makes it difficult if not impossible to legitimately compare and prioritise the legal risks that a business faces. In contrast, legal risk management methodology implements an articulated and consistent approach to preventing legal risk. For example, legal risk management methodology requires each legal risk to be evaluated in terms of the likelihood of the risk eventuating and the consequences of the risk eventuating. The legal risk management approach results in a consistent assessment of legal risk and enables disparate legal risks to compared and prioritised. It is for this reason that legal risk management is superior to preventive law. It should be noted, however, that preventive law shares with legal risk management many techniques for assessing and managing legal risk. Moreover, it could be beneficial if some of the techniques advocated by preventive law proponents for practising preventive law were integrated

into legal risk management. By way of example, many of the techniques used in preventive law, described above, could be used as additional techniques for identifying legal risks in respect of legal risk management. Given, that both disciplines aim to achieve essentially the same objectives, it is both desirable and likely and that the two disciplines will converge.

Legal compliance systems, on the other hand, traditionally focus on achieving regulatory compliance. For example, as noted above, Australian Standard *AS 3806 - 1998 Compliance Programs* states that the purpose of a compliance system is to:

> …prevent, and where necessary, identify and respond to, breaches of laws, regulations, codes or organizational standards occurring in the organization; promote a culture of compliance within the organization; and assist the organization in remaining or becoming a good corporate citizen[243].

Another example of this use of the term compliance can be found in the following extract from an Australian textbook on compliance:

> Legal compliance is the management discipline of designing and implementing effective steps to ensure that an organisation actually complies with the laws, regulations and cods of practice relating to its operations. Put another way, it is a system which is designed to ensure that the organisation does, as far as is reasonably practical, what is necessary to "get it right" in relation to its legal obligations.
>
> Legal compliance is also called "due diligence"[244].

This use of the term compliance to connote regulatory compliance is used widely. For example, a typical advertisement seeking a compliance professional will specify

---

[242] Hardaway, p 151,
[243] Australian Standard *AS 3806-1998, Compliance Programs*, para 1.2.
[244] Brian Sharpe, *Making Legal Compliance Work*, CCH Australia Limited, North Ryde, 1996, p1, para 101.

that the position involves ensuring that the company "operates within all relevant legislative and regulatory frameworks"[245].

A review of the literature, although by no means a comprehensive review, indicates that the methodology involved with achieving legal compliance does not appear to be as fixed as the methodology associated with legal risk management, with texts differing as to how a compliance system is planned and implemented. One text states that an effective compliance system comprises three elements: (1) management commitment, (2) education and awareness (creating awareness of the laws and an understanding of their requirements amongst employees who are in a position to breach those laws) and (3) implementation and control[246]. The Australian Standard *AS 3806 -1998 Compliance Programs* and the accompanying guide, *A Guide to AS 3806 -1998 Compliance programs, SAA HB133-1999*[247] sets out what it terms "essential elements" of a compliance system. These elements are described as structural, operational and maintenance elements[248]. Structural elements include: commitment to effective compliance by the business at all levels[249], a compliance policy outlining the business's commitment to compliance and how the commitment is to be carried out[250], responsibility by management for compliance[251], resources

---

245 Advertisement for a Senior Manager Compliance in *The Australian Financial Review*, Friday July 9 1999 p 4.

246 J Sigler & J Murphy, *Interactive Corporate Compliance: An Alternative to Regulatory Compulsion*, Quorum Books, New York, 1988, pp 79-107.

247 Australian Standard *AS 3806-1998, Compliance Programs*, Standards Australia, Homebush NSW, 5 February 1998; Brian Sharpe and Randal Dennings, *A Guide to AS 3806-1998, Compliance Programs SAA HB133-1999*, Published by Standards Australia, Homebush NSW, 1999.

248 Australian Standard *AS 3806-1998, Compliance Programs*, para 2.1.

249 Australian Standard *AS 3806-1998, Compliance Programs*, para 2.2.1.

250 Australian Standard *AS 3806-1998, Compliance Programs*, para 2.2.2.

allocated to achieve compliance[252] and a philosophy of continuous improvement[253]. Operational elements include identifying the compliance issues affecting the business[254], integrating the requirements of laws, regulations, codes etc into the business's day-to-day operating procedures[255], consistently enforcing the compliance program developed[256], implementing a system for handling complaints[257], recording the compliance program implemented[258], investigating, analysing and rectifying compliance failures in particular systemic and recurring compliance failures[259], implementing adequate internal reporting arrangements to ensure compliance failures are rectified and systemic and recurring non-compliance is reported to those who are responsible for and have authority to rectify them[260] and undertaking supervision at all levels to ensure compliance[261]. Maintenance elements include: undertaking practical education and training of employees[262], visible commitment to and communication of the business's compliance system[263], monitoring for compliance and reviewing the effectiveness of the compliance system implemented[264], liaising with regulatory authorities in order to keep up to date with compliance

---

251 Australian Standard *AS 3806-1998, Compliance Programs*, para 2.2.3.
252 Australian Standard *AS 3806-1998, Compliance Programs*, para 2.2.4.
253 Australian Standard *AS 3806-1998, Compliance Programs*, para 2.2.5.
254 Australian Standard *AS 3806-1998, Compliance Programs*, para 2.3.1.
255 Australian Standard *AS 3806-1998, Compliance Programs*, para 2.3.2.
256 Australian Standard *AS 3806-1998, Compliance Programs*, para 2.3.3.
257 Australian Standard *AS 3806-1998, Compliance Programs*, para 2.3.4.
258 Australian Standard *AS 3806-1998, Compliance Programs*, para 2.3.5.
259 Australian Standard *AS 3806-1998, Compliance Programs*, para 2.3.6- 2.3.7.
260 Australian Standard *AS 3806-1998, Compliance Programs*, para 2.3.8.
261 Australian Standard *AS 3806-1998, Compliance Programs*, para 2.3.9.
262 Australian Standard *AS 3806-1998, Compliance Programs*, para 2.4.1.
263 Australian Standard *AS 3806-1998, Compliance Programs*, para 2.4.2.
264 Australian Standard *AS 3806-1998, Compliance Programs*, paras 2.4.3- 2.4.4

requirements[265] and making sure employees at all levels are aware and made accountable for achieving compliance[266]. Whilst useful, the information provided does not itself constitute a compliance system as noted by a prominent compliance writer and the co-author of the accompanying guide to Australian Standard *AS 3806 - 1998, Compliance Programs*:

> [Australian Standard *AS 3806 -1998, Compliance Programs*] is not a management system in itself. It is necessary to take the principles in AS3806 and develop them into an actual management system that will work in the real world[267].

Proponents of compliance commonly advocate the use of legal audits to identify aspects of a business's activities that may contravene legislation or other forms of regulation. As noted earlier in this thesis, the traditional focus of compliance is too narrow an approach. Businesses face other legal risks and depending on the types of activities undertaken by a business these other types of legal risk may expose a business to more liability than the risks associated with regulatory non-compliance. Not only does legal risk management encompass compliance but also its objectives include avoiding excess liability and protecting legal rights and entitlements of a business.

It should be noted, however, that compliance and legal risk management are similar in many respects. A typical compliance system will involve: identifying the law regulating the business for which a compliance system is being undertaken;

---

265 Australian Standard *AS 3806-1998, Compliance Programs*, para 2.4.5.
266 Australian Standard *AS 3806-1998, Compliance Programs*, para 2.4.6.
267 Brian Sharpe, "Problems in AS3806 Implementation", *Compliance News*, Vol 10, July 1999, pp 7- 11 at p 9.

identifying the risk that can arise with failure to comply with the law, planning and implementing a compliance system, setting up a training program to educate employees and management as to statutory imposed legal requirements; a monitoring component to ensure that the business and its employees are complying with the statutory imposed legal requirements; a review component to identify shortcomings in the compliance system and to enable modification of the compliance program as necessary; and implementation of a policy by the business setting out management's endorsement of and commitment to the compliance program and the disciplinary consequences of an employee failing to comply with the business's compliance system[268]. These aspects also form part of legal risk management.

Moreover, it should be noted that some proponents of compliance define compliance much more broadly than the traditional definition. The broader definition of compliance envisages that a compliance program incorporates objectives more akin to legal risk management such as ensuring that a business's contractual rights and intellectual property rights are protected[269]. Thus, the broader definition of compliance encompasses not only the notion of achieving regulatory compliance but also preventively dealing with other legal risks. In fact, one leading practitioner in the

---

[268] See for example, the components of a compliance program set out by Herbert I Zinn Esq in "Putting It All in Motion: Designing and Implementing an Effective Compliance Program" as reproduced in Robert M Hardaway, *Preventive Law - Materials on a Non Adversarial Legal Process*, Anderson Publishing Co., Cincinnati, 1997, p 199 at p 201. See also the planning steps set out by Brian Sharpe in Brian Sharpe, *Making Legal Compliance Work*, CCH Australia Limited, North Ryde, 1996, p40, para 302.

[269] See for example, the discussion of Melvin Simensky and Eric C Osterberg, in "The Insurance and Management of Intellectual Property Risks", 17 *Cardozo Arts & Entertainment Law Journal* 321 , who use the term legal compliance to encompass the objectives of: "(1) to avoid, infringement of

field of compliance has observed that it is no longer the case that compliance is solely concerned with ensuring that a business does not breach the law[270]. Whilst in practice it may be the case that compliance is used to achieve objectives broader than ensuring that a business achieves regulatory compliance, the current literature on compliance often does not refer to this broader use. *AS 3806 -1998 Compliance Programs*, for example, assumes compliance operates in a way that reflects the traditional definition of compliance (that is, the objective is to ensure that laws, regulations and organisational standards are not breached). Similarly, it is typical for compliance to be described in following manner, which again reflects the traditional definition of compliance:

> Compliance programs are frameworks developed and implemented by an enterprise for the purpose of monitoring and modifying employee behaviour to minimize the incidence of criminal conduct.[271]

In conversations with practitioners and academic writers[272] it appears that the broader definition of compliance roughly mirrors the objectives of legal risk management. Assuming that compliance has a broader meaning (as it does for at least for some practitioners and writers) it becomes necessary to examine whether there are any differences between compliance (according to its broader definition) and legal

---

other's intellectual property rights, and to (2) protect one's own [intellectual] property from infringement while maximising its value" at p 321.

270 Discussion with Professor Brent Fisse, partner, Gilbert & Tobin, 17 June 1999. See also Professor's Fisse's comment in "Corporate Compliance Programmes: The Trade Practices Act and Beyond", *Australian Business Law Review*, December 1989, 356 at p 358 that "…the platform on which compliance programmes should be built is not merely provision of legal services but management of risk of exposure to liability and related losses."

271 Michael K Braswell, "Compliance Programs: An Alternative to Punitive Damages for Corporate Defendants", 49 *South Carolina Law Review*, Winter 1998, 247 at p 262 .

risk management. As noted in relation to the traditional narrow definition of compliance, there are already many similarities between compliance and legal risk management. Clearly the broader definition of compliance shares these similarities with legal risk management too. Moreover, the broader definition of compliance appears to overlap with legal risk management in terms of its objectives.

It is therefore tempting to conclude that legal risk management and legal compliance (at least in its broader form) are in fact the same or at least that legal compliance is a subset of legal risk management:

> We all appreciate that compliance programming is part of a broader process of risk management analysis[273].

It should be noted that others, however, have argued forcefully that legal compliance should not be equated with risk management:

> 'Beware the false prophets'-Risk management is not compliance!
>
> One hears advocates of the view that legal compliance is part of risk management, so it should be treated using risk management methods. This is dangerous and must instantly cause a red light to flash!
>
> Compliance is, broadly, part of overall control of risks, but risk management as set out in AS/NZS4360 [*Risk Management*] and associated literature cannot be relied upon to produce legal protection.
>
> The basic reason is that risk management and compliance have different purposes, and use different methods.
>
> This is why clause 1.1 of AS3806 [Compliance] warns against simply using risk management principles where legal protection is needed, and refers to the Courts' high due diligence standards.

---

[272] Conversation held with Dr Christine Parker, Lecturer, UNSW on or about 22 June 1999 and discussion with Professor Brent Fisse, Partner, Gilbert & Tobin, on 17 June 1999.

[273] Peter Toy, "Class Action Exposure and Compliance Programs", *Compliance News*, Vol 10, July 1999, pp 11- 13 at p11.

> If risk management and compliance were interchangeable, a compliance Standard would not have been needed[274].

One factor seen as distinguishing compliance from legal risk management is that the objective of compliance is "legal protection" but the objective of risk management is to "manage exposure to risks". Thus it is argued:

> In risk management, the potential cost of the risk is usually assessed in $ terms and is often reduced by factors representing the assumed likelihood and frequency of the risk.
>
> Such reductions are considered unsound in relation to legal compliance. If the chairman can go to gaol, he will not be impressed to hear that he was not fully covered because it was thought that it may only happen once in 10 years![275]

These assertions fail to recognise that in legal risk management a business must set its risk criteria (step 1 of the legal risk management process) a process whereby decisions, such as whether to achieve absolute legal compliance, are made. Both financial and non-financial factors, such as the risk of a prison sentence, are factored in at this point. As noted in the discussion at 4.2 at p 167, where the potential outcome of statutory non-compliance is a prison sentence it is highly advisable that a business's risk criteria be to achieve absolute compliance. It is therefore possible to achieve "legal protection" with legal risk management in the same way it can be achieved with legal compliance. It is true that legal risk management allows a business to decide not to achieve absolute compliance and therefore "legal protection", through the step of setting the business's risk criteria. It is incorrect,

---

[274] Brian Sharpe, "Problems in AS3806 Implementation", *Compliance News*, Vol 10, July 1999, pp 7- 11 at p7.

[275] Brian Sharpe, "Problems in AS3806 Implementation", p8.

however, to suggest that "legal protection" cannot be achieved through legal risk management or that "legal protection" is not an objective of legal risk management. Rather, it is up to the business, when setting its risk criteria, to decide what its objectives are in respect of compliance and legal protection. It is therefore concluded that this distinction is not material.

There are, however, other distinctions between compliance and legal risk management that are arguably material. For example legal compliance does differ from legal risk management in the approach taken once legal risks are identified. According to one practitioner, in compliance once a legal risk (relating to breaches of the law) is identified, the only option available is full compliance with the law[276]. This is in contrast with the legal risk management options of retaining a legal risk, risk control, risk transfer and risk avoidance. Also, it has been suggested that techniques used in legal risk management to determine which legal risk management strategy to adopt, such as cost-benefit analysis, are not applicable in relation to legal compliance, as it is not an option to "decline to control [a legal risk] effectively on [the] ground of cost."[277] Whilst it may the view of some compliance practitioners that the only option available is absolute compliance, other compliance practitioners and writers are more pragmatic:

> Compliance programs will never eliminate from a business system all risk of non-compliance with the law but they can reduce the magnitude of any

[276] Brian Sharpe, "Problems in AS3806 Implementation", p7 (See table "Comparison of Legal Compliance and Risk Management).

[277] Brian Sharpe, "Problems in AS3806 Implementation p7 (See table "Comparison of Legal Compliance and Risk Management).

> failure and can prevent the attitudes or practices that lead to such failings from becoming endemic in the culture of the business[278].

A further possible material distinction between compliance (both the narrow and broad definition) and legal risk management exists. Although it is not possible to be definitive here, given that the research undertaken in this thesis on compliance does not purport to be comprehensive, it is suggested that compliance differs from legal risk management in that it does not involve a process which results in a consistent approach to analysing and managing legal risk. That is, it appears that compliance does not advocate using techniques, such as those used in legal risk management, that result in the legal risks identified being analysed and managed consistently. This is not to say that compliance is not systematic. But it does mean it is more difficult to compare legal risks using the preventive law and compliance approaches, because under such approaches legal risks have not necessarily been evaluated consistently in the way they would be using risk management methodology. What is argued here is that these approaches have no mechanism in place that results in disparate legal risks being analysed consistently, as is the case with legal risk management. The distinction drawn here may be overstated as one compliance expert Professor Brent Fisse argues that there is no reason why compliance can't simply be treated as one major step in the legal risk management process[279].

To conclude, legal risk management encompasses aspects of preventive law and compliance (at least the narrow definition of compliance). Legal risk management

---

[278] Toy, p11.
[279] Personal communication on about 18 February 2000.

applies to a broader range of legal risks than does compliance in its narrow definition and overlaps with compliance in its broader definition. Preventive law encompasses compliance (in both its narrow and broad definition) and some aspects of legal risk management. What distinguishes legal risk management from both preventive law and compliance (in both its narrow and broad definition) is the use of a process by which disparate legal risks are analysed and evaluated consistently . This allows legal risks and risk management strategies to be prioritised which in turn makes it easier for businesses to appreciate how serious a given legal risk is and to make decisions about which legal risk management strategy to implement or whether to implement a legal risk management strategy at all. Further, legal risk management uses techniques that enable strategies for managing identified legal risks to be evaluated consistently. In addition, risk management methodology requires that risk management strategies are selected according to guiding principles such as that the effect each possible strategy may have on the business's ability to fulfill its objectives. The outcome is that the risk management strategies ultimately selected automatically take into account circumstances particular to the business. Preventive law and compliance do not explicitly embody such techniques and therefore it is necessary for the legal adviser who uses such approaches to consciously take into account factors particular to the business, which may very well be overlooked. It is suggested here that it is these features of legal risk management that make it superior to either preventive law or compliance (both in its narrow and broad definition) as a practical guide.

TABLE 31 COMPARISON OF LEGAL RISK MANAGEMENT, COMPLIANCE AND PREVENTIVE LAW

	Legal Risk Management	Compliance	Preventive Law
Objectives include to reduce or eliminate the legal liability the business may be exposed to; to achieve compliance with the laws that regulate the activities of the business; and to protect a business's legal rights and interests	√	X (According to the traditional definition) √ (According to the broader definition)	√
Specifies techniques for *identifying* range of legal risks	√ (A wide range of techniques are advocated for identifying risks. These techniques can be used equally for identifying legal risks.)	√ (Literature tends to focus on using checklists and audits. This may limit range of legal risks identified.)	√ (Literature focuses on select group of techniques. This may limit range of legal risks identified.)
Specifies techniques for *managing* identified legal risks.	√ (Risk management lays down guiding principles concerning how risks should be managed. Broadly, risks can be managed through employing risk control techniques or risk financing techniques. Risk control techniques involve minimising the frequency or severity of a risk. Risk financing techniques involve making available funds to pay for losses that arise in the event that a risk eventuates. These principles apply equally to legal risk.)	X (The literature focuses on identifying legal risks and little guidance is given on how to manage them once identified. One author suggests that with compliance, only one strategy is available, elimination of the risk by full compliance. Thus, risk retention is not an option and it is considered inappropriate to choose not to comply fully on the basis that it is not cost effective for the business to do so[280].)	X (The literature focuses on identifying legal risks and little guidance is given on how to manage them once identified)
Specifies techniques for *evaluating* and *selecting* appropriate risk management strategies.	√ Risk management specifies a comprehensive range of techniques for evaluating and selecting the most appropriate risk management strategies.	X	X
Process results in consistent *analysis* of legal risks	√	X	X
Process results in consistent *evaluation* of *legal risk management strategies*	√	X	X
Process involves ongoing review and monitoring	√	√	√
Outcome can be easily integrated into business's overall risk management system	√ (Because risk management methodology treats identified legal risks consistently, the results can be prioritised and easily integrated into a business's overall risk management system.)	X Compliance lacks a methodology that results in legal risks being analysed consistently. This makes it difficult to integrate results into a business's overall risk management.	X Preventive Law lacks a methodology that results in legal risks being analysed consistently. This makes it difficult to integrate results into a business's overall risk management.

[280] Brian Sharpe, "Problems in AS3806 Implementation", p7 (see table comparing legal compliance and risk management).

2.6 Conclusion

Based on the investigation in this chapter of risk management and its use in the context of legal risk, a number of conclusions can be drawn in relation to the use and applicability of risk management in the context of legal risk.

First, there appears to be no reason in theory why risk management cannot be applied in the context of legal risk. The discussion in this chapter examined several risk management models and, using one of the models examined, *AS/NZS 4360 -1999 Risk Management*, demonstrated that risk management methodology could be used in the context of legal risk. Further, it is suggested that risk management can achieve much wider risk management objectives than previously considered. That is, risk management can be used to achieve the three objectives earlier set out in this article of: legal compliance, avoidance of exposure to immense liability and protection of legal rights and interests.

Secondly, risk management, through its iterative methodology and the requirement that each risk be analysed (usually in terms of consequence and likelihood of eventuating), enables consistent analysis of often disparate risks. This, in turn allows risks to be prioritised. Applying such methodology in the context of legal risks is clearly desirable. Legal practitioners often fail to analyse legal risks in such a way that enables diverse legal risks to be compared and prioritised. In fact, some authors have suggested that the way in which legal practitioners analyse risks is often

idiosyncratic and highly individualistic[281], largely because the process of legal analysis is not explicitly taught in law schools:

> [Legal analysis] is usually taught indirectly, that is, as a by-product of the case book method. The process of legal analysis is treated as a gestalt with components remaining unexpressed beyond the ultimately tautological observation that one applies the law to the facts. As a result, there is no shared articulated model of legal analysis. Each professional develops his own consciously or unconsciously. The models, therefore…are idiosyncratic…" [282]

Thirdly, the use of risk management methodology in the context of legal risk results in legal advice that is attuned to business needs, more so than is conventional legal advice. For example, legal risk management methodology requires that legal risks be analysed by reference to a business's specific financial position and categorised according to the business's risk criteria. Conventional legal advice does not typically take such factors into account. Also, determining which risk management strategies to implement is achieved by reference to a business's particular financial position and its risk criteria. The usual approach to giving legal advice is to provide more generic advice in the sense that often the same legal advice would be given in respect of a particular legal risk whether the client was a large business or a small business. Legal risk management, in contrast, results in the provision of more "tailored" legal advice. It seems both desirable and logical that legal advisers should provide legal advice that actively accommodates the client's perspective.

---

[281] Costanzo, p 72.

Fourthly, although risk management is regarded primarily as a management tool for businesses to identify risks and strategies for dealing with that risk on a case-by-case basis legal risk management may have a wider scope. In fact it is suggested that legal risk management can be used to identify the extent to which legal uncertainty exists in relation to a given business activity. Because risk management involves the identification of risks and the evaluation and implementation of strategies to manage the identified risks, risk management can be used as a means of identifying those aspects of Internet commerce that are truly legally uncertain. The application of risk management enables the isolation of legal uncertainty on two levels. By identifying the legal risks associated with a business's activities we eliminate those activities or circumstances for which a perception of uncertainty exists that on closer scrutiny is not justified. Of those identified risks a second level of uncertainty is eliminated by examining whether risk management strategies for those identified risks exist, a step in the risk management process. By eliminating those identified legal risks for which a risk management strategy exists (apart from ceasing the activity) we can isolate those legal risks management strategies which are insurmountable and therefore bring about legal uncertainty. This makes legal risk management not only of use to businesses but of use to regulators and policy makers as legal risk management can provide a means for identifying areas of activity for which there is a need for law reform.

---

[282] Gee and Jackson, "Bridging the Gap-Legal Education and Lawyer Competency", 1977 Brigham Law Review 695 quoted from Margot Costanzo, *Problem Solving- (Essential Legal Skills Serie*s), Cavendish Publishing Limited, London, 1995 p 72.

Fifthly, risk management used in the context of legal risk should be distinguished from legal compliance and preventive law. Whilst there are similarities between these various techniques used by lawyers for identifying and managing legal risk, the use of risk management it is argued is superior. Risk management when applied in the context of legal risk results in disparate legal risks being analysed and evaluated consistently. This in turn enables legal risks and management strategies to be prioritised. This feature is significant because it makes it clear to business how serious a given legal risk is in relation to the other legal risks it faces and facilitates a business's decision making process concerning what legal risk management strategy it should implement.

What are the limitations of legal risk management? The usefulness of risk management in relation to law reform is limited to providing a means by which areas requiring law reform can be identified. That is, legal risk management is less useful as a tool for determining what law reform should be implemented in response to an identified area of legal uncertainty. This is partly because proposals for law reform require taking into account competing interests. As noted earlier, risk management (and accordingly legal risk management) is designed for developing strategies for dealing with risk from only one perspective, the perspective of the business implementing risk management and is not designed to take into account competing interests.

Further, for the time being the use of risk management in the context of legal risk is limited to those legal risks which make a "legally related loss" likely or more

severe. Such risks are termed "hazards" in risk management theory. In contrast, risk management cannot be used in respect of those legal risks that cause a business to incur a "legally related loss", that is, a loss incurred as a result of a legal claim being brought against the business, or the business being prosecuted for statutory non-compliance, or a business incurring losses due to a failure to protect the business's legal rights and interests. Such legal risks focus on the cause of a "legally related loss", and are considered in risk management theory to constitute a "peril". According to risk management theory, the type of legal risk that risk management is directed at is the legal risk that constitutes a hazard not a peril[283]. The use of legal risk management in relation to legal risks that constitute perils warrants further research given that the quantitative analysis of such types of legal risks is already the subject of research.

A further limitation is the extent to which legal risk management can be used as a mechanism for assessing the degree of legal risk on a generic basis. Again, as noted earlier, legal risk management is designed to assess legal risks on a case by case basis. Whether legal risk management provides a useful mechanism for producing a single, generic risk management approach requires further investigation and will be examined in the second part of this thesis.

---

283 "The wrongful conduct that good risk management strives to minimize is really a hazard, not a peril, with respect to liability losses. As … explained, a hazard is a condition or circumstance that makes a loss more likely or more severe. Wrongful conduct increases the likelihood that an organization will have a claim brought against it and that any suit will be successful. (Similarly, failing to maintain good records documenting legally-required conduct or failing to retain good legal counsel are also hazards.) Legally proper conduct does not remove the liability peril; it only reduces some liability hazards" in George L Head and Stephen Horn, *Essentials of Risk*

The use of risk management in the context of legal risk gives rise to some policy and practice implications. One important policy issue concerns the extent to which legal risk management should be allowed to be used as a defence, or in mitigation, in legal proceedings. This issue, and another important policy issue, that is the use in legal proceedings of a business's legal risk management records and documentation by regulators and other parties are identified as areas for further research in chapter 6 of this thesis.

The use of risk management in the context of legal risk also has several practical implications. One such practical use of applying risk management in the context of legal risk is that it enables a business to take "calculated" legal risks. In addition, by using risk management in the context of legal risk a business can control the amount of time it spends on managing legal risks, as opposed to the time spent on responding to legal risks that have eventuated such as litigation proceedings. These topics are further explored in chapter 6 of this thesis.

Finally, the research in this chapter provides a framework for applying *legal risk management*. A number of risk management models were examined and a legal risk management framework based on *AS/NZS 4360 Risk Management* developed. In particular, to facilitate the use of this framework, a series of checklists for undertaking the various stages of the legal risk management process were developed and sample documentation to record the outcome of these steps provided.

Management, Insurance Institute of America, 1991, http://www.bus.orst.edu/faculty/nielson/rm/chapter6.htm.

The conclusions drawn establish the setting for the following chapters in which the legal risk management framework developed is determined through its practical application to the legal risks associated with Internet commerce.

CHAPTER 3 INTERNET COMMERCE AND LEGAL RISK MANAGEMENT

3.1 Introduction

This chapter, which is essentially an explanatory chapter, marks the beginning of the second part of this thesis. Internet commerce was chosen for evaluating the legal risk management framework developed in this thesis because it raises several issues that will test the usefulness and effectiveness of the legal risk management framework developed. Internet commerce is widely perceived to operate in a legally uncertain environment. This in turn has given rise to the perception that a business conducting Internet commerce is exposed to more legal risks than it would in relation to the conduct of commerce off-line. In addition, governments and policymakers are often being called upon to implement law reform so as to remove perceived impediments to the conduct of Internet commerce. But are the so-called impediments and legal risks any different to that which are faced by businesses conducting commerce off-line? Is the call for law reform justified? There is clearly a need to identify whether, in fact, there are substantial legal risks associated with Internet commerce, and the extent to which Internet commerce operates in an uncertain legal environment. This situation is ideal for evaluating the usefulness of legal risk management because, if the conclusions drawn in chapter 2 are correct, the application of legal risk management will help to provide answers to these issues.

3.2 What is the Internet?

The Internet in physical terms is a network of computers that use defined protocols for sending packets of information between computers. The use of these protocols enables information to be exchanged between computers regardless of the type used to access the Internet.

In functional terms, the Internet is a versatile communication tool for which various methods of communication have developed. The principal forms of communication available on the Internet are: (i) the World Wide Web which enables documents (containing graphical elements and text) to be accessed and read (browsed) by any computer that is linked to the Internet; (ii) file transfer protocol (ftp), which enables the transfer of files from one computer to another; (iii) Internet Relay Chat (IRC), which enables 'real time' communication between parties; (iv) e-mail, which enables messages to be sent between computers; (v) newsgroups, which enable mass distribution of messages or articles via "news servers" that contain databases of articles/ messages and are operated by Internet service providers, schools, universities, and companies[284].

3.3 What is Internet commerce?

The term Internet commerce, often referred to as "electronic commerce", "on-line commerce" or "e-commerce", in a narrow sense refers to the sale of goods or services on the Internet including both business-to-business and business-to-consumer

---

[284] "news.newusers.questions-What newsgroups are and how they work", http://www.geocities.com/ResearchTriangle/8211/how-it-works.html.

transactions. The broader meaning of Internet commerce which is adopted in this thesis expands the definition of Internet commerce to include the trade and commercial activity (such as marketing and advertising, provision of product information, pre and post sales customer service, electronic payment, supply chain management for inventory, distribution and order and shipment tracking[285]) that is conducted on the Internet.

Internet commerce is often mistakenly referred to in the literature as electronic commerce, a broader term that refers to any commercial activity that is conducted electronically and includes commercial activities that are not necessarily conducted on the Internet (such as electronic funds transfer and electronic data interchange).

The main forum for Internet commerce is the World Wide Web although Internet commerce can also be conducted, or at least partially conducted, through other forms of Internet communication such as e-mail, electronic data interchange, bulletin boards and e-mail lists. The World Wide Web has become the main forum for Internet commerce for two reasons. First, unlike other forms of Internet communication, the World Wide Web enables sound, images, video, animation, colour and text to be incorporated into a document in clever and visually stimulating ways. From an Internet commerce perspective, the World Wide Web allows the incorporation of several interactive elements that make possible the exchange of information between

---

[285] "Electronic Commerce- An Introduction", Information Technology Programme managed by the Directorate General for Industry of the European Commission, last updated 8 May 1996, http://www.cordis.lu/espirit/src/ecomint.htm; Soon-Yong Choi and Dale O'Stahl, "Electronic Payments and the future of Electronic Commerce", The Center for Research in Electronic Commerce, 1997, http://cism.bus.utexas.edu/works/articles/cyberpayments.html.

a business and the party with whom the business transacts. Importantly, payment by customers can be effected on the World Wide Web. In addition, businesses can use metaphors that are familiar to potential customers, such as “virtual shops” where a party can browse a business’s web site, select products by putting them in a virtual shopping cart and proceed to the “cash register” to pay. Secondly, the use of other forms of Internet communication for the conduct of commerce, particularly the e-mailing of unsolicited marketing and advertising material to potential customers (spamming), is widely regarded by Internet users as unacceptable[286].

In practice, a business may use several forms of Internet communication to conduct commerce on the Internet. A business may offer its goods and services through an e-mail list or bulletin board, and invite prospective customers to e-mail an order or visit the business’s web page. If the business has a web page, a prospective customer may be invited to e-mail an order by clicking on a hypertext link to the

---

[286] What happens if a business contravenes the netiquette rule against spamming? The failure to observe netiquette (the unwritten code of Internet conduct) creates a real risk of loss in monetary and in public relations terms. Perhaps the most celebrated case concerning the consequences for businesses that breach netiquette is the Canter and Siegel story. Canter and Siegel are practising US attorneys. In an effort to obtain business, and contrary to netiquette rule against spamming (the practice of indiscriminately sending out unsolicited material on e-mail, newsgroups or bulletin boards usually with the aim of attracting business) they distributed an advertisement for their services in relation to the US greencard lottery to about a hundred newsgroups. The advertisement attracted hundreds of inquiries for further information but also some "flames" (e-mail messages which criticised their conduct for contravening netiquette). Canter and Siegel then posted their advertisement to ultimately another 7000 newsgroups. In response they were deluged with "flames" whose sheer volume overloaded and crashed the computers of their Internet service provider several times. Other Internet users, estimated in to be in their thousands, took retributive action by requesting written information so that Canter and Siegel would incur expenses in replying. Ultimately Canter and Siegel’s Internet service provider closed their account. Whilst it is reported that Canter and Siegel are unrepentant, their conduct was regarded by many Internet users as a serious breach of netiquette. Clearly, the consequences of failure to observe netiquette can result in considerable negative publicity and wasted expense. See for example: EFF "Canter & Siegel Green Card Lottery Net Spam Case" Archive:

business's e-mail address, or to fill in an order form on the business's web page. Payment may be made by entering credit card details in a form provided on the business's web site or by e-mail. Alternatively, payment may be effected using digital cash, electronic cheques, or electronic credit cards, or through a cheque sent in the post. Delivery of the goods or services may be effected by conventional means or, in some instances, by on-line delivery.

Typical examples of Internet commerce include: business-to- business transactions, such as those that involve supply, purchasing, distribution and servicing and financial services; on-line shopping, which can take the form of a business soliciting commerce directly through its own web site, or through taking part in a "virtual mall" in which groups of businesses are located; electronic bill presentment; electronic banking; electronic gambling and electronic share trading[287]. At present the highest area of growth in Internet commerce is in business-to-business Internet commerce and it has been estimated that, on a global basis, the value of business-to-business Internet commerce will exceed US$300 billion by the year 2002[288].

3.4 How can Internet commerce benefit Australian businesses?

Internet commerce offers manifold and substantial opportunities for Australian businesses in terms of increased sales and sizeable cost savings such as: 24 hour access to customers, exposure to global markets, faster response to customer demand

---

http://eff.org/pub/Legal/Cases/Canter_Siegel/; Blacklist of Internet Advertisers: http://math-www.uni-paderborn.de/~axel/BL/blacklist.html.

[287] Jonathan Rosenoer, "Late-Night Thoughts on Electronic Commerce", *Law Technology Product News"*, p 42, col 1, October 1996, http://www.ljx.com/ltpn/october96/late_night_p42.html

and inquiries, shortened or elimination of supply chains[289], reduced cost of transactions[290], reduced procurement costs, reduced inventory, lower cycle times[291], more efficient and effective customer service[292] and reduced marketing costs in comparison to alternative marketing strategies such as mail out catalogues and tele-marketing. And, where a business's product or service can be delivered on-line there are additional benefits of reduced delivery and packaging costs.

As with all Internet statistics, there are differing predictions for the estimated value of Internet commerce to Australian business. According to one Internet research company, the value of Internet transactions in Australia alone amounted to $61 million in 1996 and this amount is expected to grow to more than $1.3 billion in

---

288 *The Emerging Digital Economy*, Report of the Secretariat of Electronic Commerce, http://www.ecommerce.gov/EmergingDig.pdf, p 7.

289 A business's goods or services can be delivered directly to the consumer bypassing the wholesaler and retailer.

290 A report of the Subcommittee on International Transactions in relation to the law of commerce in cyberspace of the American Bar Association , Business Law Section, referred to studies that that show that up to 28% of transaction costs associated with trading durable goods results from paper-based movement of information. The report states that much of this cost can be removed if trading is done electronically: American Bar Association, Section of Business Law, Committee on Law of Commerce in Cyberspace, Subcommittee on International Transactions, "Supporting Report for the Recommendation Committee on Law of Commerce in Cyberspace Subcommittee on International Transactions", January 1997, http://www.abanet.org/buslaw/cyber/finaires.html.

291 See for example the following comments made in *The Emerging Digital Economy*, Report of the Secretariat of Electronic Commerce, http://www.ecommerce.gov/EmergingDig.pdf, p 16: "Cycle time is the total time it takes to build a product. There are certain fixed costs associated with building any product that do not vary with the amount of production, but rather are time dependent. These "fixed" costs include depreciation of equipment, most utility and building costs, and most managerial and supervisory time. If the time to build a product can be reduced to seven days instated of ten, then the fixed costs per product are lower since less time was needed. Electronic commerce allows "cycle times" to be shortened, allowing more to be produced for the same or lower costs."

292 See for example the comments made in *The Emerging Digital Economy* at page 19: "In addition to improved customer satisfaction, companies using the Internet for customer service report savings from putting order tracking, software downloads and technical support information online. For instance, Cisco reports that its customer service productivity has increased by 200 to 300 percent, resulting in savings of $125 million in customer service costs. Dell estimates that it saves several

2001[293]. Interestingly, the same company is reported to have estimated that the Australian share of goods and services traded over the Internet will be US 5.0 billion in 2001[294]. Another Internet research company however has estimated that the value of local goods sold in Australia through the Internet amounted to $16 million in 1996 which increased to $55 million by 1997[295]. The Electronic Commerce Expert Group reported that it was estimated that the value of Internet commerce would grow to $2 billion by 2000[296]. A recent report carried out by the ABS indicated that for the 12 months to May 1999, a total of 650 000 adult Australians used the Internet for purchasing/ordering goods and services for private use comprising an estimated 3 million transactions[297]. Even more recently, a report commissioned by the National Office for the Information Economy entitled E-commerce beyond 2000 forecasts that e-commerce will add 2.7 per cent to Australia's Gross Domestic Product over ten

---

million dollars a year by having basic customer service and technical support functions available on the Internet."

293 This figure was estimated by the research company International Data Corp (IDC) in an article in *The Australian*, Tuesday May 6, 1997, p 36. IDC predicts that on a global perspective Internet commerce is predicted to grow from $2.6 billion in 1996 to $215 billion by the year 2001. The estimate that Internet based commerce in Australia will grow to $1.3 billion by the year 2001 was reiterated in a a report commissioned by the National Office for the Information Economy entitled *E-Commerce-beyond 2000*, 1999, http://www.noie.gov.au/ecom/HOME/Policy/Economic_Impacts_Study.

294 Andersen Consulting, *eCommerce: our Future Today*, A review of eCommerce in Australia, 1998.

295 See, *stats.electronic commerce in australia, april 1998*, a study compiled by www.consult for the Department of Industry, Science and Tourism, 25 May 1998, http://www.dist.gov.au/html/new.html.

296 See for example, *Electronic Commerce: Building the Legal Framework*, Report of the Electronic Commerce Expert Group to the Attorney-General, 31 March 1998, http://law.gov.au/aghome/advisory/eceg/ecegreport.html para 1.5.

297 Australian Bureau of Statistics, "Press Release: Home Internet Use Grows Strongly-ABS Figures", press release dated September 6 1999, 106/99 3 Million Internet Purchases and1.5 Million Households Oline – ABS", http://www.abs.gov.au/websitedbs/d3110125.nsf/4a255eef008309e44a255eef00061e57/0c6b7ec6e6a0e5d3ca2567e400028e5e?OpenDocument. Full Report in *Use of Internet by Householders*, Australia, May 1999 (Cat. No. 8147.0).

years to 2007[298]. Whatever figure proves to be correct, it is clear that Internet commerce presents Australian businesses with considerable opportunities for new and expanding markets.

3.5 How is commerce conducted on the Internet?

Business-to-consumer Internet commerce is substantially conducted on the World Wide Web **("web")** where, typically, a business's goods or services are advertised, ordered and paid for entirely on the web. Internet commerce can also be conducted, or at least partially conducted, by means of e-mail. For example, a business may solicit customers by mass e-mailing marketing and promotional material to news groups or bulletin boards, and a customer may respond by e-mail to make an order for the business's goods or services. Or, a business may distribute marketing and promotional material by e-mail in which customers are directed to a business's web site. Business-to-business Internet commerce is often web based but can also involve Electronic Data Interchange (an automated method of exchanging messages which traditionally occurred on private, limited access networks called Value Added Networks (VANS) but can also take place using the Internet).

There are several ways in which a contract can be transacted on the Internet. First, a contract can be solely transacted on the Internet. That is, formation of the contract **("formation")** takes place on the Internet, and delivery of and payment for the goods or services purchased **("performance")** is wholly effected on the Internet. For

---

[298] Department of Communications, Information Technology and the Arts, "E-commerce Beyond 2000", Commonwealth of Australia, 2000: http://www.noie.gov.au/beyond2000.

example, a customer may order software through a business's web page (or, for that matter, by e-mail) that is paid for either by credit card or some other form of electronic payment such as digital cash or electronic cheque. Delivery of the software is also effected on the web. Alternatively, Internet commerce may be conducted partly through the Internet and partly off-line. For example, a business's goods or services may be advertised on the Internet but a customer may choose to order and pay for the business's goods or services by downloading and printing out the order form provided on the business's web page and faxing or posting the order form and payment details. Finally, it should be noted that a business may choose to conduct its business so that there is no contractual relationship created on the Internet. For example, a business may use the Internet solely to advertise its goods or services with both contract formation and performance taking place off-line.

Analysed from a contractual perspective, the combinations by which a contract may be transacted through the Internet are as follows:

3.5.1 FORMATION AND PERFORMANCE OF THE CONTRACT OCCURS ENTIRELY ON THE INTERNET

A contract may be transacted entirely on the Internet. That is, formation and performance of the contract takes place wholly on the Internet. Formation of a contract on the Internet can occur in several ways: it can occur through the exchange of e-mails between a business and its customer(s). Formation can also occur through a customer completing and transmitting to a business an order form provided on a business's web site.

In relation to the payment aspect of performance, payment can be effected through the Internet in several ways. For example, payment may be effected by way of credit card, electronic cheque, electronic credit card or digital cash. Finally, in relation to the delivery aspect of performance, delivery can, depending on the nature of the goods or services offered by a business, be effected through the Internet (eg software is downloaded by the customer, or data or information is e-mailed to the customer or displayed on the customer's computer screen for the customer to browse and/or download).

3.5.2 FORMATION OF THE CONTRACT TAKES PLACE ON THE INTERNET; PERFORMANCE OF THE CONTRACT TAKES PLACE OFF-LINE

A contract may be transacted partially on the Internet with formation taking place on the Internet and performance taking place off-line. Formation occurs on the Internet in the ways described in (i) above. In relation to the payment aspect of performance, payment off-line can be effected in a number of ways including by way of telephone, by way of facsimile (where for example, credit card details are provided by means of telephone or facsimile), or by way of post (such as when a cheque or credit card details are posted to the business). Delivery is effected off-line by way of post.

3.5.3 FORMATION OF THE CONTRACT TAKES PLACE ON THE INTERNET; PERFORMANCE OF THE CONTRACT TAKES PLACE PARTLY ON THE INTERNET AND PARTLY OFF-LINE

A contract transacted on the Internet may be formed on the Internet, with performance taking place on the Internet and partly off-line. Formation of such contract occurs in the manner described in (i). Performance of the contract can occur

in two ways. Either delivery takes place on the Internet in instances (where such delivery is technically possible, as in, for example, the sale of software) and payment occurs off-line (in the manner discussed in (ii) above). Or, delivery occurs off-line (in the manner discussed in (ii) above) and payment takes place on the Internet (in the manner discussed in (i) above).

3.5.4 FORMATION OF THE CONTRACT TAKES PLACE OFF-LINE AND PERFORMANCE OF THE CONTRACT TAKES PLACE ON THE INTERNET

A contract transacted on the Internet may be formed off-line, with performance taking place on the Internet. A contract could be formed off-line by a customer faxing or posting an order to the business (for example, a customer could print out an order form displayed on a web page, or e-mailed to the customer, and fax or post the completed order form to a business). Performance of the contract takes place on the Internet in the manner discussed in (i) above.

3.5.5 FORMATION OF THE CONTRACT TAKES PLACE OFF-LINE WITH PERFORMANCE OCCURRING PARTLY ON THE INTERNET AND PARTLY OFF-LINE

A contract transacted on the Internet may be formed off-line in the manner described in (iv) above with performance occurring partly on the Internet and partly off-line. Performance of the contract can occur in the manner described in (iii) above.

3.6 Justification for applying legal risk management in relation to Internet commerce

Governments, including the Australian Commonwealth and State governments, are increasingly recognising the importance that Internet commerce will have on the economy of the future, and businesses are continuously being exhorted by

government and by industry commentators, to utilise the Internet as a forum for commerce or risk losing market opportunities to other competitors[299].

Whilst there has been considerable interest by both businesses and consumers in the use of the Internet as a forum for commerce, there is a widely held perception that for a consumer or a business to conduct Internet commerce would expose both parties to substantial legal risks to which they wouldn't be exposed if the same transaction were conducted off the Internet, and that therefore Internet commerce operates in an uncertain legal environment[300].

Thus, Senator Richard Alston, Minister for Communications, Information Technology and the Arts, Deputy Leader of the Government in the Senate has said: "There has been widespread concern within industry that consumer and small business distrust of electronic transactions is inhibiting the development of online

---

299 See, for example, Communiqué from the Canberra Summit on E-Commerce Great Hall, Parliament House 16-17 April 1998, 17 April 1998; Grant Butler and Steve Lewis, "E-commerce future 'grim', *The Australian Financial Review*, April 17 1998, p 15; Steve Lewis and Stan Beer, "'Wait and see' Australians are late starters", *The Australian Financial Review*, April 17 1998, p 17. See also the views of Peter Leonard, Partner, Gilbert & Tobin who in "Response to the Attorney-General's Speech Regarding the Draft Digital Agenda Copyright Bill and the Draft Electronic Transactions Bill", 12 March 1999, http://www.gtlaw.com.au/pubs/index_Internet.html stated "The second reason we need to fix the legislative framework for the information economy is to reduce transaction costs. Lawyers have been major beneficiaries from the current shambolic underpinnings of electronic commerce and content dissemination. The current complexity of dealing in the digital environment increases transaction costs."

300 See for example, *Electronic Commerce: Building the Legal Framework*, para 4.01. See also the United Kingdom Department of Trade and Industry Public Consultation Paper entitled, "Licensing of Trusted Third Parties for the provision of Encryption Services", Public Consultation Paper on Detailed Proposals for Legislation, March 1997, http://www.dti.gov.uk/pubs/ at para 51, in which it was stated: "In the UK research has shown that uncertainty as to the legal effect of using electronic commerce is seen by the business community as a considerable barrier to its development.

commerce. The Government recognises that it has a leadership role to play in building trust".[301]

Illustrative of this perception of legal uncertainty is the following statement made by Internet Law & Policy Forum (ILPF) Executive Director Ruth Day:

> The growth of electronic commerce has raised uncertainties. The Internet offers an efficient medium for global electronic business and can contribute significantly to economic growth. At the same time, the borderless nature of the medium creates new challenges to governments' territorial-based powers. Buyers and sellers want to know whether traditional legal protections apply to reach a party which does not live up to its commercial obligations even if that party is in another country. Governments want to know what impact these cross border transactions will have on fundamental powers, most notably to raise tax and tariff revenue and to guard citizens against harm[302].

The following extract from *The Weekend Australian* reflects a typical view concerning the legal uncertainty associated with conducting commerce on the Internet from a consumer perspective:

> Shopping on the Internet may look attractive to those who hate standing in queues, but if there is a problem with the item you bought, you could be in real trouble; that is if the item you thought you were buying ever arrives.
>
> Consumers International recently ordered and then returned more than 150 items from e-commerce sites from 17 different countries. One in 10 items never arrived; two buyers have waited over five months for refunds; more than half of the products ordered arrived without receipts; 73 per cent of traders failed to give crucial contract terms; more than 25 per cent of traders gave no address or telephone number and 24 per cent were unclear about the total cost of the item that was ordered.
>
> This is disconcerting stuff for virtual shoppers and indicates a real need for cyber rules of conduct[303].

---

301 Press release of Senator Richard Alston, Minister for Communications, Information Technology and the Arts, Deputy Leader of the Government in the Senate dated 23 June 1999 at http://www.dca.gov.au/nsapi-graphics/?MIval=dca_dispdoc&ID=3981&template=Newsroom.

302 Ruth Day, ILPF Executive Director, July 16, 1999, http://www.ilpf.org/press/1999jul16.htm.

303 Bina Brown, "Internet Shopping Basket Case", *The Weekend Australian*, October 30-31, 1999, p 46.

This gives rise to reluctance amongst consumers to use the Internet as a forum for commerce:

> There is evidence suggesting that consumers are reluctant to purchase goods and services over the Internet because of concerns with payment systems and consumer protection issues such as redress and compensation, and the reliability of retailers[304].

The following extract from the NY Times illustrates that there is a perception that conducting Internet commerce is legally uncertain from a business perspective too:

> The law is inherently based on geographic boundaries, historically an effective way to impose a socialized order on human behavior. But the Internet knows no such boundaries and has prospered because of a kind of anarchy. The law can only work when the government or a private plaintiff can identify a wrongdoer as defendant. By contrast, the Internet thrives on anonymity.
>
> …
>
> Not surprisingly, these differences between the law and the Internet, and between the Internet and older technologies, have led to the emergence of some legal issues that the courts have never before confronted.
>
> …
>
> More fundamentally, must a business that puts up a Web site abide by the laws and regulations of every jurisdiction around the world – even those that may be inconsistent – because anyone anywhere with a telephone, a computer and some basic software can theoretically read and respond to the site? [305]

Increasingly, governments are being called upon to enact legislation to remove perceived impediments to the conduct of Internet commerce. But is such legislation actually necessary? Are there aspects of Internet commerce which expose businesses

---

[304] Report of Joint Committee of Public Accounts, Parliament of Australia inquiry into the commercial and revenue implications of the growth in electronic commerce, 27 May 1998: http://www.aph.gov.au/house/committees/jcpa/termscom.htm, para 7.13.

to legal risks that to which they would not be exposed if they were conducting off-line commerce?

Clearly, there is a need to identify whether, in fact, there are substantial legal risks associated with Internet commerce, and the extent to which Internet commerce operates in an uncertain legal environment. This is ideal for evaluating the usefulness of legal risk management because, if the conclusions drawn in chapter 2 of this thesis are correct, the application of legal risk management should be able to determine these issues.

The topic of Internet commerce is investigated from the perspective of Australian businesses whose Internet commerce activities are conducted from a location physically based in Australia, with parties who may be located within the same State/Territory in which the business is located, or with parties located interstate or overseas.

3.7 Conclusion

In this chapter, the scene was set for the second part of this thesis in which the legal risk management framework developed in this thesis is evaluated by applying it to the legal risks associated with Internet commerce. By way of background, the Internet and an explanation of the various ways in which Internet commerce can be conducted were introduced. In addition, a justification for examining legal risk management in relation to Internet commerce was provided. The next chapter, in

---

[305] Stephen Labaton, "Can Defendants Cry 'E-Sanctuary' and Escape the Courts*?*, *The New York Times*, September 22, 1999.

which the first and second steps of the legal risk management process (establishing the context and identifying the legal risks) is applied, marks the beginning of an in-depth examination of the use of legal risk management in the context of Internet commerce.

CHAPTER 4 CYBER - DEALING I: IDENTIFYING THE BUSINESS'S LEGAL RISK MANAGEMENT OBJECTIVES AND THE LEGAL RISKS

4.1 Introduction

In this chapter, the first and second steps of the legal risk management framework developed in chapter 2 are evaluated by applying them to the legal risks associated with conducting Internet commerce.

The research finds that, when used generically, the effectiveness of the first step of the legal risk management framework (determining the objectives of the business or establishing the context) is somewhat limited. This is because it is only possible to set general objectives for businesses that conduct Internet commerce such as: to reduce or eliminate the legal liability the business is exposed to in relation to conducting Internet commerce; to achieve compliance with the laws that regulate the conduct of Internet commerce; and to protect a business's legal rights and interests during the course of any transaction conducted using the Internet.

In relation to the second step of the legal risk management framework (identifying the legal risks) the research indicates that many of the risk management techniques used for identifying risks can equally be applied in relation to identifying legal risk. Several legal risks associated with the conduct of Internet commerce are identified in this chapter. In evaluating the usefulness of various risk identification techniques in the context of Internet commerce, there is some duplication as a given legal risk may be identified by more than one risk identification technique. This duplication is eliminated in the discussion towards the end of this chapter when the legal risks that are particular to businesses conducting Internet commerce are isolated.

The isolation of those legal risks that are particular to the conduct of Internet commerce leads to the selection of the following legal risks to which the remaining steps of the legal risk management framework will be applied: 1. The risk that an Internet transaction is unenforceable for failure to satisfy the Statute of Frauds Statute of Frauds writing requirement; 2.The risk that a business becomes contractually bound to terms unintentionally; 3. The risk that an acceptance communicated by a business does not give rise to a binding contract; 4. The risk that a customer is not contractually bound to standard terms purportedly incorporated by a business; 5. The risk that a business enters into a contract that is invalid because it was unauthorised; and 6. The risk of incurring liability in relation to the acceptance of on-line payments.

4.2 Identifying a business's legal risk management objectives in relation to the conduct of Internet commerce ("Establishing the context")

As noted in chapter 2, the first step in the legal risk management process is to "establish the context", that is, ascertain the role and overall objectives of the business as well as ascertain the specific objectives of a business, in relation to the activities it undertakes. Part of this process includes the business establishing risk benchmarks. It is not possible, however, in this thesis to set definitive risk benchmarks signifying the level of risk that is acceptable or unacceptable to a business in relation to the conduct of Internet commerce. This is because, to a large extent, such benchmarks rely on factors particular to a business, such as the financial resources of the business. This illustrates the difficulty of using legal risk management without specific reference to a particular business. It is however possible to discuss the factors a risk manager or legal adviser should take into

account when setting the risk benchmarks in relation to the level of risk that is unacceptable to a business. Such factors to take into account include the goals, objectives and values of the business. Does the business want to operate its Internet commerce activities on a high legal risk basis, a low legal risk basis or somewhere in between? In other words, what level of legal risk is the business prepared to accept in relation to its Internet commerce activities? Does the business require absolute regulatory compliance in relation to its Internet commerce activities or will the business accept liability for regulatory non-compliance up to a certain dollar level (in terms of fines imposed). It should be noted that, given the use of prison sentences for regulatory non-compliance in some instances, the business may be reluctant to accept a standard of regulatory non-compliance that is below absolute compliance.

Whilst it may not be possible in this thesis to define specifically the risk benchmarks for a business conducting Internet commerce, some general objectives of a business for the purposes of "establishing the context" can be stated. Thus, the objectives of a business that conducts Internet commerce in the context of identifying and managing legal risk includes: to reduce or eliminate the legal liability the business is exposed to in relation to conducting Internet commerce; to achieve compliance with the laws that regulate the conduct of Internet commerce; and to protect a business's legal rights and interests during the course of any transaction conducted using the Internet.

Table 32 LEGAL RISK MANAGEMENT IN RELATION TO INTERNET COMMERCE- STEP 1

STEP 1 **DETERMINING THE OBJECTIVES OF THE BUSINESS OR "ESTABLISHING THE CONTEXT"**	THE OBJECTIVES OR CONTEXT FOR A BUSINESS CONDUCTING INTERNET COMMERCE Some factors a risk manager or legal adviser should take into account when setting risk benchmarks for business's conducting Internet commerce: ♦ The goals, objectives and values of the business. In general terms, the objectives of a business that conducts Internet commerce should include: to reduce or eliminate the legal liability the business is exposed to in relation to conducting Internet commerce, to achieve compliance with the laws that regulate the conduct of Internet commerce and to protect a business's legal rights and interests in respect of any Internet transaction conducted by the business. ♦ Does the business want to operate its Internet commerce activities on a high legal risk basis, a low legal risk basis or somewhere in between? In other words, what level of legal risk is the business prepared to accept in relation to its Internet commerce activities? ♦ Does the business require absolute regulatory compliance in relation to its Internet commerce activities or will the business accept liability for regulatory non-compliance up to a certain dollar level (in terms of fines imposed and legal costs associated with a prosecution for statutory non-compliance). It should be noted that, given the use of prison sentences for regulatory non-compliance in some instances, the business may be reluctant to accept a standard other than absolute compliance.

4.3 Identifying the legal risks associated with Internet commerce

Several methods for identifying risk and, more specifically, legal risk were discussed in chapter 2. The usefulness of these techniques for identifying the legal risks associated with Internet commerce is assessed here. It is foreshadowed that certain risk identification techniques can not be applied in this thesis simply because such techniques require reference to a specific business. Finally, some duplication will occur in relation to the legal risks identified when applying the various techniques for identifying risk. That is, a legal risk may be identified by more than one risk identification technique. This duplication is left in the following discussion as it demonstrates that it is not necessary to use all of the techniques described in chapter 2 to identify the range of legal risks that affect a particular activity or

business. The "duplicate" identified legal risks, however, are eliminated in the discussion beginning at 4.4 at p214 where the legal risks associated with Internet commerce are isolated from the identified legal risks that equally affect businesses conducting off-line commerce.

4.3.1 COMPLETING A SURVEY/QUESTIONNAIRE FOR THE BUSINESS OR USING CHECKLISTS & AUDITS

Conducting surveys, questionnaires, checklists or audits is likely to be the most commonly used technique for identifying legal risk. However, as noted in chapter 2, because legal audits have tended to emphasise or focus solely on regulatory compliance, it is important that a business instruct its legal advisers or its risk management consultants, or whoever is undertaking the legal audit, that any legal audit undertaken must encompass questions directed at detecting, in addition to regulatory non-compliance, the legal risks facing the business in relation to the protection of a business's legal rights and entitlements and the legal risks facing the business in relation to the protection of a business from exposure to tortious or contractual liability.

There are two limitations associated with using questionnaires, checklists and audits etc to identify legal risk. First, no questionnaire or checklist can identify every single legal risk to which a business is exposed, unless of course the business is willing to incur the considerable cost, in terms of time and money, that such a checklist would involve to prepare and undertake. Secondly, it has been observed that there is a danger that too much emphasis is placed on the questionnaire or checklist itself:

> The function of the risk analysis questionnaire is often misunderstood. Sometimes a risk management consultant or an insurance agent will approach a client with the questionnaire, fully expecting to proceed through an agonising series of questions from start to finish. Other consultants and agents reject the use of lengthy questionnaires because they anticipate an adverse reaction from clients. These practices and attitudes are based on a fundamental misunderstanding of the purpose and function of the questionnaire.
>
> The risk analysis questionnaire is designed to serve as a repository or the information that is gained from documents, interviews, and inspections. The information in the completed questionnaire is gained from an analysis of documents, inspections, records, and interviews. Its purpose is to lead the person attempting to identify exposures through the identification process in a logical and consistent fashion.[306]

So how does a business know which questions to ask? There are various texts that have been published which set out checklists or questionnaires for businesses in order to identify legal risk. Some of these texts provide checklists or questionnaires in relation to specific areas of law, such as information technology law, copyright law or tortious liability. Others touch generally on the areas of law that typically give rise to legal risks in relation to a business. In addition, law firms in their promotional literature often make available sample checklists or questionnaires that a business can employ to identify exposure to legal risk. Regulatory agencies also sometimes provide guidelines or audits for business's to undertake in order to identify areas of regulatory non-compliance. It is understood that, at least in the United States, insurance companies make available insurance policy checklists, which set out various risks a business can face and the type of insurance policies available. By referring to such checklist a business can identify some types of legal risks to which it is exposed as a consequence of conducting Internet commerce. As risks that are non-

insurable are unlikely to appear on an insurance policy checklist, care must be taken not to rely on such checklists exclusively to identify the legal risks associated with Internet commerce. Also, the checklist being essentially a document intended to stimulate use of an insurance company's services, will be limited in the types of legal risks that can be identified in that the checklist will be directed at identifying the legal risks against which the insurance company is offering to insure.

Increasingly, services directed specifically at providing risk management services in relation to the conduct of Internet commerce are now being offered which apply audits or checklists to identify risk. Ernst & Young, in partnership with TRUSTe (a nonprofit organisation that monitors businesses in respect of the steps they take to protect the privacy of information acquired about their customers who make purchases through the Internet), offers audits of a business's security and information management systems. The American Institute of Certified Public Accountants offers a similar service called CPA WebTrust which is supported by the accounting firms Deloitte & Touche, Coopers & Lybrand, and KPMG. Such audits can also reveal the legal risks a business faces in relation to a business's security and information management systems used in relation to Internet commerce. Network Risk Management Services Inc is a US company that offers risk management services in relation to businesses conducting Internet commerce. The range of topics covered in their checklists/questionnaires are wide, many of which are also relevant to cover in order to identify the legal risks associated with Internet commerce:

---

[306] Vaughan, p 112.

Corporate Status / Market Status, Current Insurance Status, Stakeholder Definition Process (define dependent relationships), Executive Management Security Policy Awareness, Security Organization and Responsibilities, Employee Security Policy, Employee Security Training and Staff Education, Business Unit Information, Coverage Information, E-Commerce Qualification, Third-Party Audit Information, Accountability for Users, Password / Access Management, Data and Software Exchange Agreements, User Information Network Computer Activities, Private Publishing Controls, Outsource Provider Assessment, Internet Service Provider Relationships, Security Service / Network Maintenance Provider Relationships, Quantify Digital Assets, General Written Policies, Modem Controls, Software Piracy Controls, Operational Procedures and Responsibilities, Controlling Super Users, System Planing and Acceptance, Malicious Software and Virus Protection, Security Housekeeping, Public Website Content Control Information, Network Security Components, Configuration Management, Lifecycle Maintenance and Update Information, Authentication, Integrity, Availability, Intrusion Detection, Non-Repudiation, Confidentiality, Reaction, Media Handling and Security, Physical Security, Secure Areas, Equipment Security, Insurance Coverage Needs.

Using the above list as a starting point, the following legal risks to Australian businesses associated with the conduct of Internet commerce have been identified. This list does not purport to be exhaustive:

Table 33 SOME LEGAL RISKS ASSOCIATED WITH INTERNET COMMERCE IDENTIFIED THROUGH USING CHECKLISTS AND AUDITS
Risk, if the business is incorporated, of **contravening the Corporations Law** by **failing to display** the business's **Australian Company Number (ACN) or Australian Registered Body Number (ARBN)** on its web page or in its e-mail. It should be noted that whether a corporation is required to display its ACN on its web page or in its e-mail is at present a "grey area". Section 153 of the Corporations Law states that an ACN needs to be displayed on a corporation's "public documents". Section 88A of the Corporations Law defines what is a "public document". It is arguable that a business's e-mail and web page constitute public documents but this has not been tested by the courts nor is it clarified by ASIC policy.
Risk of **contravening the Corporations Law** by **offering securities for sale** on the Internet **without being licensed**.
Risk that the business in its sale or supply of goods or services is liable in contract for **breach of the implied conditions and warranties** under the **Trade Practices Act 1974 (Cth), the State and Territory Fair Trading Acts and Sales of Goods Acts** equivalents.
Risk that the business is liable in contract for **breach of any other conditions or warranties**. To determine whether such liability exists it is necessary to examine a sample contract to see what conditions and warranties are set out in the business's standard contract for the sale or supply of

its goods or services.
Risk that the business in its sale or supply of good or services is liable for **contravention of the consumer protection provisions** of **Trade Practices Act 1974 (Cth), the State and Territory Fair Trading Acts** such as section 52 and section 53 of the Trade Practices Act 1974 (Cth).
Risk of **liability in tort** for **passing off** if the business conducts commerce by means of a web site and web site has links to a competitor's web site without making it clear that the links are not part of the business's web site.
Risk of **liability in tort** for **negligent misstatement** for any statements made by the business in its promotional and advertising material which are untrue whether it is sent by e-mail, on the business's web site or appears in banner advertising on another party's web site.
Risk of **liability in negligence** and under the **product liability** provisions of the Trade Practices Act 1974 (Cth) to purchasers of the business's goods if the goods are defective and consequently cause personal injury or loss.
Risk that the business is subject to a **contractual term** that the business **agreed to inadvertently** as a consequence of a defect or failure in the business's hardware or software. For example, due to an error in the business's hardware or software, an offer of a customer conveyed by e-mail or a form in a business's web page is accepted by the business's computer system on conditions or terms contrary to those which the software or hardware was presumed to have been programmed to accept. Or, the purchase price for products supplied or sold by the business, due to a programming error, has a decimal point put in the wrong place. If a customer fills in a web page order form ordering product on that basis, at law, business would be bound by such offer[307].
Risk that the business transacts with a party who **does not have legal capacity** to contract eg a minor.
Risk of **liability in negligence** to a customer for **failure to adequately protect credit card information** provided by the customer during the course of Internet transaction from external users and as a consequence the customer has incurred loss due to a third party having obtained such details from the business (eg through hacking the business's computer system) and then fraudulently used such details.
Risk of **liability for an employee** fraudulently using credit card information provided by a customer during the course of an Internet transaction.
Risk of **liability in negligence** to a customer if a **customer's credit card information is made available to third party services** used by the business during the course of an Internet transaction eg an Internet service provider, a credit provider, or a trusted third party and such third parties fraudulently misuse customer credit card information.
Risk of legal **liability for regulatory non-compliance** resulting from a failure to adequately ensure that a party contracting with the business is legally permitted to transact with the business eg non-compliance with legislation that prohibits certain contracts being entered into with a minor, or non-compliance with legislation to prohibits a resident from using the business's products or services are illegal (eg gambling or pornography).

[307] Some writers have referred to this in terms of agency, that is, the business is liable for the acts of an electronic agent. If an electronic agent, in error or due to software or hardware error, makes an offer which is then accepted by a client then such offer is contractually binding on the business as principal.

Risk of **liability in defamation** if the business allows chat groups on its web page or allows bulletin boards or accepts other forms of customer input that is displayed on the business's web site or is disseminated in some other way by the business (eg by way of e-mail).
Risk of **liability for trade mark infringement** if the business uses domain names that infringe another business's trade mark and the associated risk of **liability for passing off**.
Risk that **customers infringe the business's copyright** in goods supplied or sold through Internet, eg through pirating software purchased through the Internet.
Risk that an **Internet transaction is repudiated** by a party because the party with whom the business conducted Internet commerce was an imposter who pays using a third party's credit card or identity in order to incur liability on the third party's behalf.
Risk that a **transacting party will fraudulently deny contractual liability** on the basis that communications from the transacting party were not actually communications of the transacting party but were that of an imposter.
Risk of **liability in negligence** for an **inadequate system for computer security** if a business's computer system is hacked and credit card information of customers is stolen and used by imposters.

4.3.2 REVIEWING LOSS HISTORIES OF THE BUSINESS OR COMPARABLE BUSINESSES, ANALYSING FINANCIAL STATEMENTS AND ACCOUNTING RECORDS AND REVIEWING OTHER RECORDS AND DOCUMENTS OF THE BUSINESS

In chapter 2, it was stated that reviewing loss histories of the business, analysing financial statements and accounting records and reviewing other records and documents of the business were techniques for identifying legal risk. Apart from reviewing the loss histories of comparable businesses, these techniques, require legal risk management to be applied to a specific business. Also, in practice, it may not be relevant to review loss histories of a business given that Internet commerce is a relatively new commercial activity and that a business may not as yet have incurred any losses arising from conducting Internet commerce. Similarly, in relation to reviewing loss histories of comparable businesses, in this instance, businesses that conduct Internet commerce, such information is not yet publicly available. As the Internet commerce industry matures, such information is more likely to become

publicly available when losses incurred by such businesses are documented in the media and in the literature. The discussion here therefore is limited to examining how the above mentioned techniques can help identify the legal risks associated with Internet commerce.

Viewing financial statements, accounting records and other records and documents of a business is particularly useful for identifying the legal risks associated with Internet commerce if the legal risk management process is being undertaken by a third party legal adviser, rather than an in-house risk manager or in-house counsel, as such documents usually set out the activities of the business and other general information about the business[308].

All commercial activities referred to in the businesses financial statements and other accounting records of the business that involve the use of the Internet by the business should be noted.

If the business's activities are limited to *advertising* on the Internet the legal risks the business will be exposed to are largely the same legal risks associated with advertising in relation to off-line commerce. Thus, an Australian business faces the following legal risks:

Table 34 LEGAL RISKS ASSOCIATED WITH INTERNET COMMERCE IDENTIFIED THROUGH REVIEWING THE BUSINESS'S ADVERTISING MATERIAL

Risk that the business's **advertising material contravenes** section 52 or 53 of the **Trade Practices Act 1974 (Cth) and the State or Territory Fair Trading equivalents**.

[308] Vaughan, p 114.

Risk that the business's **advertising material** is **actionable as false representations, or "offers"** as opposed to "puffs" or "invitations to treat", or as enforceable terms of a contract by a customer.
Risk of **failure to protect** the **business's legal rights and interests**, where the advertising takes the form of **banner appearing on a third party's web page**, and the business has **failed to ensure** that the third party will not insert the business's banner advertisements with **web content** that the business does not want to be associated with.
Risk of **failure to protect** the business's **legal rights and interests**, where the advertising takes the form of **banner appearing on a third party's web page**, and the business **fails to ensure** that the agreement between the parties sets out the **frequency of the display** of the banner advertisement.
Risk of **failure to protect** the business's **legal rights and interests** where the business uses a **third party to display banner advertisements**, and the business **fails to ensure** that the agreement between the parties sets out a **benchmark for market exposure**, such as a specified number of individuals who visit the web site, or what constitutes a visit to the third party's web site[309]?
If **advertising** is **disseminated** by way of **e-mail**, and such advertising is distributed to recipients in the US, the business faces the risk of **contravening US legislation** prohibiting the use of unsolicited e-mail to sell products.
If **advertising** takes the form of the business's own web page, and the business provides **links to other web sites**, the business faces the risk of **liability for copyright infringement**. Whilst yet to be litigated in Australia, in both the UK and the US legal suits have been instituted against businesses whose web sites contained links to pages of a competitor's web page that linked beyond a competitors "front web page" or "entrance page". These cases, however, have not conclusively determined that such conduct would constitute copyright infringement. Alternatively if the business's web site contains links to illegal sites or sites that infringe copyright the business faces the risk of statutory non-compliance (if legislation prohibits linking to illegal sites) or the risk of liability for infringing copyright.
Risk of **liability for contravention** of another party's **copyright or trademarks** if the content used in the business's web site uses **images or material or trademarks of another** not owned by the business.

If the business is *conducting transactions on the Internet* whether it be by way of business-to-business transactions or business-to-consumer transactions other legal risks, may arise:

---

309 Often a web surfer will click out of a web page before it is fully loaded because of lack of viewer interest- the business needs to decide whether this type of visit will "count" when determining whether a third party has adequately displayed the business's banner advertisement). Similarly, will a hit that occurs every time a file is downloaded from a server to a host computer constitute a visit? If yes, this would mean that web page that contained several images would register multiple

Table 35 LEGAL RISKS ASSOCIATED WITH INTERNET COMMERCE IDENTIFIED THROUGH REVIEWING RECORDS AND DOCUMENTS OF THE BUSINESS
Risk of **contractual liability** for any **statements** made by the business during the course of transacting on the Internet as **false representations, or offers** as opposed to "puffs" or invitations to treat, or as enforceable terms of a contract by a customer.
Risk of **entering into an unenforceable contract** if the transactions the business conducts on the Internet are subject to the **requirement** that they be **evidenced in writing and signed**.

4.3.3 CONSTRUCTING FLOWCHARTS OF THE BUSINESS'S ORGANISATIONAL STRUCTURE

In identifying the legal risks associated with Internet commerce it is also useful to construct a flowchart of that part of the business's organisational structure that undertakes Internet commerce.

Once a flowchart has been constructed, it may reveal gaps in the business's organisational structure which expose a business to legal risk. By ascertaining, for example, whether a person has been appointed to consider and choose appropriate systems for securing customer credit card information or to vet promotional material, or whether a person is responsible for setting the parameters vis a vis the circumstances under which Internet orders are accepted and filled and in what circumstances Internet orders are rejected, we can identify some legal risks that an Australian business is exposed to. If the business does not have a person undertaking such responsibilities the business will expose itself to legal riskssuch as:

---

visits. Or will visits be measured by reference to 'user sessions', which identify individuals visiting

Table 36 LEGAL RISKS ASSOCIATED WITH INTERNET COMMERCE IDENTIFIED THROUGH CONSTRUCTING FLOWCHARTS OF THE BUSINESS'S ORGANISATIONAL STRUCTURE
Risk of **liability in negligence** for having an **inadequate system for computer security** if a business's computer system is hacked and **credit card information of customers is stolen and used by imposters**.
Risk that the business's **advertising material contravenes** section 52 or 53 of the **Trade Practices Act 1974 (Cth) and the State or Territory Fair Trading equivalents**.
Risk that the business's **advertising material** is actionable as **false representations, or "offers"** as opposed to "puffs" or "invitations to treat", or as enforceable terms of a contract by a customer.

4.3.4 INSPECTING THE BUSINESS'S FACILITIES

This risk identification technique is particularly useful for identifying risks faced by businesses that have plant or manufacturing operations. A physical inspection can in these circumstances reveal risks such as safety risks or environmental risks. In relation to identifying the legal risks to Australian businesses associated with Internet commerce businesses should undertake an inspection of the software and hardware used in respect of its Internet commerce activities. For example, an inspection of security logs generated by a business's Internet facilities may reveal that hackers have successfully broken into a business's customer records including credit card information, which in turn could expose the business to legal risks.

Similarly, the operating system, server software and Internet commerce software used by the business to operate its Internet commerce facilities should be reviewed for potential security problems that may in turn give rise to legal liability for a business conducting Internet commerce. For example, the operating system of the

---

the site

business or the businesses virus protection software may have some security flaw that allows the system to be infected by a computer virus. If a virus attacked a business's Internet commerce facilities a scenario could arise whereby the business could unintentionally transmit a computer virus to its customers giving rise to liability in negligence or for trespass.

Inspection of a business's facilities may also reveal whether the business's Internet commerce facilities are physically secure from physical break-in or access by unauthorised employees, which would give rise to liability to customers if customer information were accessed and used fraudulently.

Some legal risks that can be identified through inspecting a businesses facilities include:

Table 37 SOME LEGAL RISKS ASSOCIATED WITH INTERNET COMMERCE IDENTIFIED THROUGH INSPECTING THE BUSINESS'S FACILITIES
In the event that a business unintentionally transmits a computer virus to a customer during the course of conducting Internet commerce, risk of **liability in trespass for wrongfully transmitting a computer virus**[310].
In the event that a business unintentionally transmits a computer virus to a customer during the course of conducting Internet commerce, risk of **liability in negligence for wrongfully transmitting a computer virus**[311].
Risk of **liability in negligence** to customers **for failure to adequately protect personal and financial information about customers** when such information is hacked and used fraudulently by third parties.
Risk of **regulatory non-compliance** in relation to **worker safety**.
Risk of **liability in negligence** to employees arising from **failure to provide a safe system of work**.

[310] Law Commission, para 153.
[311] Law Commission, paras 172-175.

4.3.5 CONSULTING WITH EXPERTS WITHIN AND OUTSIDE THE BUSINESS

It may be useful for a business to engage, for example, a systems security expert to identify the security risks faced by a business in relation to its Internet commerce operations. The identified security risks may give rise to legal risks, some of which are listed in Table 37 at p180[312].

Alternatively, the business's information technology employees can be asked to provide assessments of where the business's exposure to security breaches are, which, as previously stated, can give rise to legal risks.

Also, as noted earlier, increasingly, there are now experts offering risk management services to business. In fact there are now some businesses that offer risk management services specifically in relation to a business's Internet commerce activities. Again use of such services by a business should include an assessment of the legal risks associated with Internet commerce subject to the observation made in chapter 2 that risk managers often focus on statutory non-compliance and exposure to tortious and contractual liability and fail to consider the legal risks associated with failure to protect a business's legal rights and interests.

Finally, a business may rely on legal advisers (whether in-house or external) to identify the legal risks associated with Internet commerce. Again, the business will

---

[312] Some security risks whilst not directly giving rise to legal risks are so serious as to completely disrupt a business's Internet commerce activities such as Denial of Service attacks (DOS) such as those experienced by Yahoo, Amazon.com, eBay and CNN. These DOS attacks involved sending huge volumes of data (ping packets) resulting in access to this sites being blocked. See Stuart Fist,"DoS message goes unheeded", The Australian, February 22, 2000 p60.

need to ensure that the legal adviser is instructed to advise in relation to the legal risks associated with statutory non-compliance, the legal risks associated with failure to protect legal interests and rights and the legal risks arising from tortious and contractual liability.

Many expert consultants and academics make available information on the World Wide Web in relation to the types of issues that a business should consider in relation to conducting Internet commerce. Although in the case of expert consultants such information is presumably primarily intended to make a potential customer draw the conclusion that they need to use the legal services offered by the expert consultant, often the depth of information provided in these web sites is sufficient to enable a business to ascertain the range of legal risks it faces in relation to the conduct of Internet commerce. Based on a select review of web sites purporting to provide businesses guidance in relation to using the Internet, in particular a web site of a US law firm, and a web site of an Australian law firm[313] as well as some academic articles on legal aspects of Internet commerce made available on the Web the following legal risks to Australian businesses associated with Internet commerce were identified:

Table 38 LEGAL RISKS ASSOCIATED WITH INTERNET COMMERCE IDENTIFIED THROUGH CONSULTING WITH EXPERTS WITHIN AND OUTSIDE THE BUSINESS

Risk of **liability for defamation** in **multiple jurisdictions** in relation **to material appearing on the business's web site** whether it be **material produced by** or on behalf of **the business** or

313 Gilbert & Tobin Lawyers, "Internet Compliance Manual", http://www.gtlaw.com.au, 1997.
314 Gilbert & Tobin Lawyers, "Internet Compliance Manual", section 2.1(i).

material posted by third parties onto bulletin boards provided by the business on the web site[314].
Risk that the business's **use of information collected from customers** during the course of transacting commerce **contravenes privacy** laws in overseas **jurisdictions or Australia's privacy laws** (if the business is a government agency, or to the extent that Australia's privacy laws regulate the private sector)[315].
Risk that the **business's promotional material contravenes** section 52 of the **Trade Practices Act 1974 (Cth) and the State and Territory Fair Trading Act or equivalents** due to engaging in **misleading and deceptive conduct**[316].
Risk that **material** provided in the business's web site **contravenes** State **legislation prohibiting the transmission of "objectionable material"** such as child pornography and instructions on how to commit violent crimes[317] **or contravenes the Broadcasting Services Act 1992 (Cth) (Regulation of Online Content-Schedule 5) in relation to prohibited online content.**
Risk of **failure** to adequately **protect the business's intellectual property** in the business's web site[318].
Risk of exposure to **liability for intellectual property infringement** by the business's web site in relation **to images, icons and other content used in the business's web site**[319].
Where a business uses a domain name that has the potential for confusion with a registered trademark, risk of **contravention of s 120(3) of the Trademarks Act 1995** (Cth) or **s52 of the Trade Practices Act 1974** (Cth)[320].
Where a business uses a domain name that has the potential for confusion with a **US registered trademark**, risk of **liability in the US for dilution** of the **trademark**[321].
Where a third party has developed the business's web site, risk of **failure** by the business **to ensure** that the business obtains **copyright in the web site developed** and **failure to ensure** that the **third party developer** promises to **keep information** disclosed by the business **confidential**[322].
Where a third party has developed the business's web site, risk of **failure to obtain warranties and indemnities from the third party developer** in relation to any material prepared by the

315 Gilbert & Tobin Lawyers, "Internet Compliance Manual", section 2.1(i). The Commonwealth government will shortly introduce a Bill to extend the operation of the Privacy Act to the private sector.

316 Gilbert & Tobin Lawyers, "Internet Compliance Manual", section 2.1(i).

317 Gilbert & Tobin Lawyers, "Internet Compliance Manual", section 2.1(i).

318 Gilbert & Tobin Lawyers, "Internet Compliance Manual", section 2.1(i).

319 Gilbert & Tobin Lawyers, "Internet Compliance Manual", section 2.1(i).

320 Brian Fitzgerald, Leif Gamertsfelder, Tonje Gullikson, "Marketing your Website: Legal Issues relating to the Allocation of Internet Domain Names", *UNSW Law Journal*, 1998, Volume 21(2), http://www.law.unsw.edu.au/unswlj/ecommerce/fitzgerald.html at III.

321 Brian Fitzgerald, Leif Gamertsfelder, Tonje Gullikson, "Marketing your Website: Legal Issues relating to the Allocation of Internet Domain Names", *UNSW Law Journal*, 1998, Volume 21(2), http://www.law.unsw.edu.au/unswlj/ecommerce/fitzgerald.html at III.

322 Gilbert & Tobin Lawyers, "Internet Compliance Manual", section 2.1(ii).

323 Gilbert & Tobin Lawyers, "Internet Compliance Manual", section 2.1(ii).

developer that may be **defamatory, or illegal** or in any other way attract exposure to legal liability or involve statutory non-compliance[323].
Risk of **failure to protect** the business's **legal rights and interests** by failing to ensure **clear service levels are set in the developer agreement** between the business and the web developer such as **response time, download rates and bandwidth usage**[324].
Where a third party hosts the business's web site, risk of **failure to protect** a business's **legal rights and interests** by **failing to ensure clear service levels** are set in the web site host agreement between the business and the hosting third party such as **24 hour availability, response time to fix technical errors, help-desk support for access difficulties experienced by customers, maintenance and renewal of the business's domain name** (where such service is purchased by the business) [325].
In jurisdictions where such legislation exists, risk of **statutory non-compliance** in relation to various taxation laws which impose **liability to pay taxes** such as **customs tax, stamp duties, sales tax**[326].
Risk of **statutory non-compliance** in relation to **consumer protection laws in multiple jurisdictions**[327].
If advertisements of other parties are displayed on the business's web site or access to part of the web site is restricted to "members only", risk of **failure to adequately protect** the business's **intellectual property rights** by granting access or location rights by way of licence[328].
If advertisements of other parties are displayed on the business's web site or access to part of the web site is restricted to "members only", risk of **liability for breach of contract for removing content contributed by third parties** because the business failed to include as a term of allowing third party material on its web site the right to remove any such material[329].
If advertisements of other parties are displayed on the business's web site or access to part of the web site is restricted to "members only", risk of **liability for material uploaded** on to the business's web site **by a third party** that may be defamatory, or illegal or in any other way attract exposure to legal liability or involve statutory non-compliance[330].
Risk of exposure to **liability which could have been limited through** the use of **disclaimers**, for example a business's vicarious liability for material posted to the business's web site by third parties or a business's liability to third parties who incur injury as a consequence of following advice or information provided on the business's web site (eg health, diet and fitness

324 Gilbert & Tobin Lawyers, "Internet Compliance Manual", section 2.1(ii).
325 Gilbert & Tobin Lawyers, "Internet Compliance Manual", section 2.2(ii).
326 Gilbert & Tobin Lawyers, "Internet Compliance Manual", section 2.1(iv).
327 Gilbert & Tobin Lawyers, "Internet Compliance Manual", section 2.1(iv).
328 Gilbert & Tobin Lawyers, "Internet Compliance Manual", section 2.1(iv).
329 Gilbert & Tobin Lawyers, "Internet Compliance Manual", section 2.1(iv).
330 Gilbert & Tobin Lawyers, "Internet Compliance Manual", section 2.1(iv).
331 Lance Rose Law Office, "Build a Safer Web Site-Webmasters can lower their legal risks even when the laws are uncertain", http://www.netlaw.com/explaind/sepfunc.htm, 1996-97.

information)[331].
Risk of exposure to **liability which could have been limited through the use of contracting out** particular aspects of the business's web site such as the development of the web site, the provision of information made available on the web site[332].
Risk **of liability for content provided by third parties**, such as when the business's web site allows chat groups or bulletin boards, or reproduces material provided by parties commissioned by the business to provide material, or reproduces material from other web sites[333].

4.3.6 BEING ON RELEVANT REGULATORS' MAILING LIST, MEMBERSHIP OF PROFESSIONAL GROUPS, SUBSCRIBING TO RELEVANT INFORMATION SERVICES AND ATTENDING INDUSTRY FORUMS AND SEMINARS INCLUDING SUBSCRIBING TO E-MAIL LIST GROUPS AND SUBSCRIBING TO ON-LINE WEB SITES THAT PROVIDE INFORMATION CONCERNING THE LEGAL RISKS ASSOCIATED WITH INTERNET COMMERCE

There is presently a wealth of information that is available to businesses on a subscription basis or on the basis of membership of professional groups, or available in the forms of seminars and industry forums.

Many such services are available through the Internet. For example, Cyberlaw journal (http://www.nytimes.com) part of New York Times web site is published weekly and deals with various legal issues affecting the Internet.

Wired Digital Inc's Wired News web site provides another source of information on legal issues affecting the use of the Internet as Wired News often carries stories relating to legal issues on the Internet.

In addition, there are several e-mail lists, US based, and Australian based, that discuss from time to time, or exclusively, specific legal issues affecting the Internet such as copyright, content regulation, public key authentication, domain names and

---

332 Lance Rose Law Office, "Build a Safer Web Site-Webmasters can lower their legal risks even when the laws are uncertain", http://www.netlaw.com/explaind/outsurc.htm, 1996-97.

333 Lance Rose Law Office, "Build a Safer Web Site-Webmasters can lower their legal risks even when the laws are uncertain", http://www.netlaw.com/explaind/datastrm.htm and http://www.netlaw.com/explained/republsh.htm, 1996-97.

Internet governance. To name but a handful of such e-mail lists, ICA is an e-mail list devoted to the use of the Internet for e-commerce in Australia and LINK is concerned with the state of the information industry in Australia. Other lists that discuss the legal risks associated with Internet commerce include E-CARM, which is a list devoted to rights management, secure transactions, digital signatures and certificates, the USENET comp.risks, which also takes the form of a moderated digest, "The RISKS Forum", at http://catless.ncl.ac.uk/Risks, which is a digest of the Association for Computing Machinery devoted to risks to the public in computers and related systems and ACSELSIC which is an e-mail list of the Australian Computer Society that relates to a section of the ACS concerned with the legal, economic and social implications of the information industry.

Also, AusCERT (Australian Computer Emergency Response Team), which centralises reporting of security incidents, system vulnerabilities and facilitates communication of defence strategies and mechanisms and early warning of likely attacks[334] provides extensive information in the form of advisories and information repository, may be useful for identifying legal risks that could arise from security issues relating to Internet commerce.

The following legal risks to Australian businesses were identified from a recent review of posts made to various mailing lists:

---

[334] See: Australian Computer Emergency Response Team, "What is AusCERT?" http://ftp.auscert.org.au/Information/Auscert_info/whatis.html.

Table 39 LEGAL RISKS ASSOCIATED WITH INTERNET COMMERCE IDENTIFIED THROUGH BEING ON RELEVANT REGULATORS' MAILING LISTS, MEMBERSHIP OF PROFESSIONAL GROUPS, SUBSCRIBING TO RELEVANT INFORMATION SERVICES AND ATTENDING INDUSTRY FORUMS AND SEMINARS INCLUDING SUBSCRIBING TO E-MAIL LIST GROUPS AND SUBSCRIBING TO ON-LINE WEB SITES THAT PROVIDE INFORMATION CONCERNING THE LEGAL RISKS ASSOCIATED WITH INTERNET COMMERCE
Risk that a **business will be closed down** by the Australian Securities and Investment Commission for **providing investment advice without a licence** in **contravention of the Corporations Law**[335].
Risk that a **third party imposter** will **hack** the business's e-mail address and **fraudulently** use it to transact with customers on that basis[336].
Risk of **contravention of the Racing Administration Act 1998 (NSW)** where a business, other than a business operating as a service provider that is a member of the Internet Industry Association of Australia and is bound by the Internet Industry Code of Practice, provides a service that (i) enables a person to access the gambling operations carried on by a person who is **not a lawful bookmaker or who is not licensed under the Totaliser Act 1997** (NSW); or (ii) **enables a person to access information relating to those 'unlawful' gambling operations**[337].

4.3.7 CONSIDERING THE BUSINESS'S STAKEHOLDERS

Legal risk can be identified through considering the "stakeholders" of the business, and examining the circumstances in which the business may be exposed to legal liability to these stakeholders as a consequence of risk management decisions made by the business and the activities it undertakes. This technique is perhaps not as useful for identifying legal risks as it is for identifying other types of risks, given that many of the risks associated with "stakeholders" are based on the risk to business of bad publicity or public pressure rather than a legal risk such as a stakeholder enforcing a legal right against the business.

---

335 Several posts in relation to the issue were made on the LINK list on or about 19 February 1999.

336 A post made in relation to this issue was made by Russell Ashdown on the LINK list on 23 February 1999.

337 A post made in relation to this issue was made on LINK by Lachlan Simpkins on 24 Feb 1999.

Whilst not purporting to be comprehensive, the following "stakeholders" and the potential legal risks an Australian business may be exposed to in relation to these stakeholders were identified:

Table 40 LEGAL RISKS ASSOCIATED WITH INTERNET COMMERCE IDENTIFIED THROUGH IDENTIFYING RELEVANT STAKEHOLDERS- CUSTOMERS
Risk of **liability for defective products sold to customers** during the course of transacting with the business on the Internet.
Risk of **liability for breach of the duty of confidence for disclosing confidential information disclosed by customers** during the course of transacting with the business on the Internet.
Risk that the business, whilst conducting Internet commerce, **transacts** with an **imposter** who fraudulently assumes the identity of another party, and that the **party whose identity has been assumed later repudiates the transaction**.
Where there is **legislation that prohibits distribution of advertising material via e-mail**, and such legislation has mechanisms for affected parties to commence legal action to stop such activities or seek compensation where such activity has occurred in contravention of the legislation (For example, some anti-spam legislation in the USA allows parties who have been subjected to spam from a business to seek damages from that businesses), risk of **liability to pay damages to a party for contravention** of such legislation.

Table 41 LEGAL RISKS ASSOCIATED WITH INTERNET COMMERCE IDENTIFIED THROUGH IDENTIFYING RELEVANT STAKEHOLDERS - COMMUNITY GROUPS
Where there is legislation that prohibits the **transmission of particular content or activities**, such as pornography or gambling, and such legislation also has mechanisms for interested **third parties to commence legal action to stop** such, risk of legal action commenced against the business by community groups to stop the business from operating its Internet commerce activities and/or for contravention of such legislation.

Table 42 LEGAL RISKS ASSOCIATED WITH INTERNET COMMERCE IDENTIFIED THROUGH IDENTIFYING RELEVANT STAKEHOLDERS - CONSUMER RIGHTS ORGANISATIONS
Where there is legislation that prohibits **distribution of advertising material via e-mail**, and such legislation has mechanisms for **interested third parties to commence legal action to stop** such activities, risk of legal action against the business by a consumer rights organisation for

contravention of such legislation and/or to stop the business form operating its Internet commerce activities in such a way.

Table 43 LEGAL RISKS ASSOCIATED WITH INTERNET COMMERCE IDENTIFIED THROUGH IDENTIFYING RELEVANT STAKEHOLDERS - INTERNET SERVICE PROVIDERS

Where the business uses an Internet service provider in relation to its Internet commerce activities, risk of **liability for breach of contract** if the business conducts Internet activities such as offering for sale pornography or provides restricted content on its web site or conducts advertising campaigns using spam, **in contravention of the Internet service provider agreement between the business** and its Internet service provider.

Table 44 LEGAL RISKS ASSOCIATED WITH INTERNET COMMERCE IDENTIFIED THROUGH IDENTIFYING RELEVANT STAKEHOLDERS - CREDIT CARD PROCESSORS/BANKS

Risk of **contractual liability** for breach of contract or **risk that the credit card processor is contractually entitled to refuse to honour payment** made by a customer if the business accepts credit payments via the Internet.

4.3.8 REVIEWING INTERNATIONAL ORGANISATION REPORTS, GOVERNMENT AND AGENCY REPORTS AND OTHER LITERATURE

Several Australian government and agency reports and reports of international organisations and other countries consider the impact of electronic commerce and, as a consequence, touch on some of the legal issues associated with undertaking Internet commerce. There are also reports that have focussed exclusively on the legal issues associated with undertaking Internet commerce. Usually written from a regulatory perspective, these reports are, nevertheless, if reviewed and analysed from a business perspective, very useful for identifying the legal risks to businesses associated with the conduct of Internet commerce.

Whilst not purporting to be comprehensive, a literature review of key Australian government and agency reports, international organisation reports and reports of other countries has identified the following legal issues, which, if analysed from a business perspective, reveal some legal risks to businesses associated with the conduct of Internet commerce:

A key Australian government (Commonwealth) report, "Electronic Commerce: Building the Legal Framework- Report of the Electronic Commerce Expert Group to the Attorney General"[338], in considering the extent to which Australian laws required reform to ensure international competitiveness in relation to the use of e-commerce, examined a number of areas of law in respect of potential law reform. These areas of law examined largely corresponded to the areas of law to which the United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Commerce 1996 applies. Viewed from an Australian business perspective, the following legal risks to businesses are identified:

Table 45 LEGAL RISKS ASSOCIATED WITH INTERNET COMMERCE IDENTIFIED THROUGH REVIEWING "ELECTRONIC COMMERCE: BUILDING THE LEGAL FRAMEWORK- REPORT OF THE ELECTRONIC COMMERCE EXPERT GROUP TO THE ATTORNEY GENERAL"
Risk that **information, records and signatures** that are **in an electronic form** are **denied legal effect** solely on the grounds that they are in an electronic form[339].
Risk, if the Internet transaction were subject to the **requirement** that it be in **writing**, that an

[338] *Electronic Commerce: Building the Legal Framework* Report of the Electronic Commerce Expert Group to the Attorney-General, 31 March 1998, http://law.gov.au/aghome/advisory/eceg/ecegreport.html.

[339] *Electronic Commerce: Building the Legal Framework*, para 2.5.8.

Internet communication would not satisfy the requirement if the transaction were evidenced only in electronic form[340].
Risk that a **signature signed electronically (eg by using digital signatures) does not have legal effect**[341].
Risk that an **Internet communication** evidenced only in electronic form **does not satisfy the requirements to constitute an original** for evidential purposes in jurisdictions other than the Commonwealth and NSW, where the common law principles and rules relating to the means of proving the contents of documents have been abolished[342].
Risk that in some Australian jurisdictions (Commonwealth, NSW) an **Internet communication (other than an e-mail)** evidenced only in electronic **form is not admissible for evidential purposes**[343].
Risk that **storage of records in electronic form does not comply with laws** requiring records to be retained[344].
Risk of **legal uncertainty concerning** the **use** and **validity** of **Internet communications in contract formation**[345].
Risk of **legal uncertainty concerning** the **time** and **place** of **dispatch** and **receipt** of **Internet communications**[346].

The Electronic Transactions Act 1999 (Cth) has now removed some of these legal risks in relation to Internet transactions governed by Commonwealth law (At the very least, such Internet transactions are those that involve interstate trade or overseas trade, Internet transactions between corporations, Internet transactions between businesses and Commonwealth government departments and entities and Internet transactions that involve individuals or businesses residing in the Territories. The Commonwealth law may extend all Internet transactions depending on constitutional interpretation of the extent of the Commonwealth government's telecommunications

---

340 *Electronic Commerce: Building the Legal Framework*, paras 2.6.16-2.6.31; 4.1.8-4.1.9.
341 *Electronic Commerce: Building the Legal Framework*, paras 2.7.28-2.7.36; 4.1.8.
342 *Electronic Commerce: Building the Legal Framework*, paras 2.8.20-2.8.29.
343 *Electronic Commerce: Building the Legal Framework* , paras 2.9.13-2.9.27; 4.1.10.
344 *Electronic Commerce: Building the Legal Framework*, paras 2.10.13-2.10.29; 4.1.11.
345 *Electronic Commerce: Building the Legal Framework*, paras 2.11.9-2.11.15; 4.1.12.

powers). For example, section 14 of the Act specifies rules for determining the time and place of dispatch and receipt of Internet communications. Similarly, records, documents and signatures will not be denied legal effect solely on the grounds that they are in electronic form: see sections 8-12. The extent to which the Electronic Transactions Act 1999 (Cth) has removed certain legal risks is discussed in more detail in Chapter 5.

An earlier key Australian government (Commonwealth) report of the Corporate Law Economic Reform Program entitled "Electronic Commerce: Cutting cybertape-building business" considered the need for law reform of the Corporations Law to facilitate the adoption and use of electronic commerce. Many of the law reforms discussed, however, did not directly relate to electronic commerce. For example, the Report considered accepting company returns and other regulatory imposed information required to be lodged by companies in an electronic form. Some issues relating to electronic commerce were raised, and, viewed from an Australian business perspective, the following legal risks are identified:

Table 46 LEGAL RISKS ASSOCIATED WITH INTERNET COMMERCE IDENTIFIED THROUGH REVIEWING THE REPORT OF THE CORPORATE LAW ECONOMIC REFORM PROGRAM "ELECTRONIC COMMERCE: CUTTING CYBERTAPE- BUILDING BUSINESS"
Risk that a **legal offering of shares** in one jurisdiction **may be illegal** in another and may be innocently communicated to the second jurisdiction[347].
Where a business trades in debt securities, risk that **certain transactions of debt securities traded electronically are unenforceable** for **failure to satisfy the Statute of Frauds writing**

346 *Electronic Commerce: Building the Legal Framework*, paras 2.15.13-2.15.17.

347 Corporate Law Economic Reform Program, Electronic Commerce: Cutting Cybertape- Building Business, Proposals for Reform, Paper No 5, Commonwealth of Australia, AGPS, 1997, page 16.

requirement[348].

The OECD report entitled "Electronic Commerce Opportunities and Challenges for Government" (the Sacher Report) identified what it termed "fundamental questions" in relation to electronic commerce:

> Where does an electronic transaction actually take place in terms of contractual obligations, assignment of liabilities and tax responsibilities?
>
> Where are companies that trade electronically registered and regulated, and to which legal regimes are they subject?
>
> How are rights in tangible and intangible forms of properly to be protected?
>
> What happens when a transaction goes wrong-who has responsibility and liability?[349]

Viewed from a business perspective, these risks were characterised as follows:

Table 47 LEGAL RISKS ASSOCIATED WITH INTERNET COMMERCE IDENTIFIED THROUGH REVIEWING THE OECD REPORT "ELECTRONIC COMMERCE OPPORTUNITIES AND CHALLENGES FOR GOVERNMENT" (THE SACHER REPORT)
Risk that a business is **subject to tax in multiple jurisdictions**.
Risk that a business is **subject to liability for negligence** and for **statutory non-compliance in multiple jurisdictions**.
Risk that a business is subject to **multiple regulatory frameworks**.
Risk of **failure** to adequately **protect intellectual property rights** traded on the Internet.
Risk of **liability in negligence** or **contract** in relation to **a transaction that fails**.

348 Corporate Law Economic Reform Program, page 48.

349 OECD, "Electronic Commerce Opportunities and Challenges for Government" (the Sacher Report), 12 June 1997, OECD, p 43.

The International Chamber of Commerce in a document entitled "General Usage for Internationally Ensured Commerce (GUIDEC)" identified a number of legal issues relating to electronic commerce[350]. After having considered GUIDEC from a business perspective, the following legal risks to businesses are identified:

Table 48 LEGAL RISKS ASSOCIATED WITH INTERNET COMMERCE IDENTIFIED THROUGH REVIEWING THE INTERNATIONAL CHAMBER OF COMMERCE DOCUMENT "GENERAL USAGE FOR INTERNATIONALLY ENSURED COMMERCE (GUIDEC)"
Risk that some of the formalities required in relation to certain transactions such as the **Statute of Frauds writing requirement** or the **requirement for a signature cannot be satisfied** in the context of Internet commerce[351].
Risk that a **digital signature does not constitute a signature** at law[352].

The Electronic Commerce Taskforce, in a report entitled "Report of the Electronic Commerce Task Force to the Commonwealth Law Enforcement Board", considered a number of law enforcement related issues concerning electronic commerce. Some of these issues, when viewed from a business perspective, give rise to the following risks facing businesses conducting Internet commerce:

Table 49 LEGAL RISKS ASSOCIATED WITH INTERNET COMMERCE IDENTIFIED THROUGH REVIEWING THE ELECTRONIC COMMERCE TASKFORCE REPORT "REPORT OF THE ELECTRONIC COMMERCE TASK FORCE TO THE COMMONWEALTH LAW ENFORCEMENT BOARD"
Risk that an **Internet transaction cannot be proved** because electronic records of the transaction were not generated by the business and the use of secondary records such as a

350 International Chamber of Commerce, "General Usage for Internationally Ensured Commerce (GUIDEC)", 1997, http://www.iccwbo.org/guidec2.htm.
351 International Chamber of Commerce, para IV.2.
352 International Chamber of Commerce, para IV.2.

record held by a bank showing that the business communicated with a customer's bank in order to get payment is not admissible because such record constitutes hearsay[353].
Risk that an **Internet transaction cannot be proved** because it is necessary for that proof to rely on evidence from an overseas jurisdiction[354].

The New Zealand Law Commission, in a report entitled "Electronic Commerce Part One- A guide for the Legal and Business Community", considered in some detail a large range of legal issues relating to the conduct of Internet commerce[355]. The following risks facing businesses conducting Internet commerce were identified:

Table 50 LEGAL RISKS ASSOCIATED WITH INTERNET COMMERCE IDENTIFIED THROUGH REVIEWING THE NEW ZEALAND LAW COMMISSION REPORT "ELECTRONIC COMMERCE PART ONE- A GUIDE FOR THE LEGAL AND BUSINESS COMMUNITY"
Risk that the business is **contractually bound on terms that it did not intend** because the **business's computer software** used for conducting Internet commerce was **erroneously programmed or malfunctions** so it makes or accepts offers in circumstances unauthorised by the business[356]. For example, due to an error in the business's hardware or software, an offer of a customer conveyed by e-mail or a form in a business's web page is accepted by the business's computer system on conditions or terms contrary to those which the software or hardware was presumed to have been programmed to accept.
Risk that the business is **contractually bound on terms that it did not intend** because the **business's computer software** used for conducting Internet commerce **transmits an incorrect or corrupted offer** in such a way as to remain apparently correct[357]. For example, due to a programming error the purchase price for products supplied or sold by the business has a decimal point put in the wrong place. If a customer fills in web page order form ordering product on that basis, and such action constitutes acceptance of an offer made by the business, at law the business would be bound by such acceptance.
Risk that the business is **contractually bound to a transaction** because **although revocation** of the business's **offer was received by the customer's computer** it was not accessed and read

353 Electronic Commerce Taskforce, "Report of the Electronic Commerce Task Force to the Commonwealth Law Enforcement Board", Commonwealth of Australia, November 1996, p 67, paras 6.5.6-6.5.10.
354 Electronic Commerce Taskforce, pp 69-70, paras 6.8.1-6.8.12.
355 Law Commission, "Electronic Commerce Part One- A guide for the Legal and Business Community", NZLC R50, October 1998, Wellington, New Zealand.
356 Law Commission, para 58.
357 Law Commission, para 60.
358 Law Commission, para 83.

by **the customer** who **in the meantime** had **communicated acceptance** of the business's offer[358].
Risk that a **customer repudiates** a **contract** on the basis that the **customer's offer** to purchase **lapsed or was revoked** as a consequence of the delay of the customer's offer having reached the business due to no fault of either transacting party[359].
In the event that a business unintentionally transmits a computer virus to a customer during the course of conducting Internet commerce, risk of **liability in trespass for wrongfully transmitting a computer virus**[360].
In the event that a business unintentionally transmits a computer virus to a customer during the course of conducting Internet commerce, risk of **liability in negligence for wrongfully transmitting a computer virus**[361].
Where the business provides advice on the Internet which is incorrect or false, risk of **liability for negligent misstatement**[362].
Risk that the business's **electronic records of Internet commerce** conducted with customers is **not admissible** under the rules of evidence by reason of having been created or stored electronically[363].
Risk of **infringing intellectual property laws** such as copyright and passing off **by hyperlinking to other web sites** or using frames to provide access to other party's web sites but retaining some elements of the business's web site[364].
Risk of **infringing a competitor's trade mark by referring to that competitor's trade mark in meta-tags** embedded in the business's web site in order that searches made for the competitor's web site will also result in a search result that includes the business's web site.
Risk of **statutory non-compliance in respect of consumer protection laws that prohibit misleading and deceptive conduct** (such as section 52 of the Trade Practices Act 1974 (Cth)) by hyperlinking to other web sites or using frames to provide access to other party's web sites but retaining some elements of the business's web site or embedding meta-tags on the business's web site that refer to competitors' trade marks[365].

4.3.9 REVIEWING RELEVANT CASE LAW

A review of the case law can reveal legal risks to which a business is exposed in the conduct of Internet commerce. There is presently limited Australian case law in

---

359 Law Commission, para 87.
360 Law Commission, para 153.
361 Law Commission, paras 172-175.
362 Law Commission, para 183.
363 Law Commission, paras 226-237.
364 Law Commission, paras 375-381.
365 Law Commission, paras 375-381.

relation to the conduct of Internet commerce. A search of Australian case law relating to Internet commerce revealed but a handful of cases that arose in the context of the Internet and Internet commerce. From these cases the following legal risk to Australian businesses was identified:

Table 51 LEGAL RISKS ASSOCIATED WITH INTERNET COMMERCE IDENTIFIED THROUGH REVIEWING AUSTRALIAN CASE LAW

Where a business has hired a **third party to develop its Internet transaction software**, risk that the business **fails to protect its intellectual property rights** by ensuring that **all intellectual property rights** in the software developed **are assigned to the business**[366].
Risk that a business is liable for contravention of sections 52 and 53 of the Trade Practices Act 1974(Cth) and for trademark infringement where the business offers its Internet services under a name that can be confused with a registered trademark[367].
Risk that the **business's web page** contains **material** that is **defamatory**[368].

The overseas case law is much more extensive, particularly the case law of the United States and the United Kingdom, but much less likely to be relevant to Australian conditions. A suitable assessment could only be made in light of a particular business's operations and the particular overseas counties in which it

366 See for example, *Hotline Communications Ltd v Hinkley & Ors* [1999] VSC 74 where the plaintiffs sought to prevent the defendant from re-using computer code developed by the defendant for the plaintiffs to develop other competing software.

367 *Paramount Pictures Corporation v Starwon Enterprises Pty Ltd, Graeme Ross Chinnery, Heribert Hermann Ortheil, Brian Strangways Young, David Craig Knowles and Geoffrey William Durkin*, Federal Court of Australia, No. NG 551 of 1998, Fed no 1054/98. In this case the defendant, an Internet Service Provider operating in Perth, registered its business name as Star Trek Net Services and used the words Star Trek in connection with its supply and offering to supply Internet services. As this judgment was interlocutory it is unknown whether the plaintiff's claim that the defendant contravened sections 52 and 53 of the Trade Practices Act 1974(Cth) and infringed the plaintiff's trademark was upheld.

368 *David Rindos v Gilbert John Hardwick*, Supreme Court of Western Australia, No 1994 of 1993 (Unreported Judgement 940164).

proposed to do business. Such an assessment of relevant overseas case law would be required in any real-life legal risk assessment but would serve little purpose in this thesis.

4.3.10 REVIEWING RELEVANT LEGISLATION AND VOLUNTARY CODES OF CONDUCT

At the time of writing, only one piece of legislation in Australia, the Electronic Transactions Act 1999 (Cth), specifically regulates Internet commerce although several Acts such as the Trade Practices Act 1974 (Cth) and the State and Territory Fair Trading Acts, the Corporations Law and other legislation that regulates commercial transactions, such as consumer credit legislation, regulate Internet commerce by virtue of the fact that they apply generally to commerce and commercial transactions.

Broadly, the Electronic Transactions Act (Cth) 1999 provides that, as at 1 July 2001[369], in respect of all Commonwealth law[370] including legislation and common law, any requirement to give information in writing, to provide a signature to produce a document, to record information or to retain a document will be satisfied if undertaken in electronic form[371]. In addition, the Act contains a provision for determining the time and place of the dispatch and receipt of an electronic

---

369 Prior to this date, the legislation will only apply to those laws that have been specified in the regulations.

370 The legislation will not apply to those laws from which its application has been specifically excluded.

371 Sections 8-12, Electronic Transactions Act 1999.

communication[372]. The Act also contains a provision regulating the attribution of electronic communications[373].

In addition, other legislation targeted at removing particular impediments to Internet commerce is anticipated. The Commonwealth Government announced on 16 December 1998 that it would implement "light-touch" privacy legislation based on the National Principles for the Fair Handling of Personal Information. It is anticipated that this legislation will affect Australian businesses conducting Internet commerce. At the time of writing, this legislation has yet to reach the Bill form.

The Victorian State Government has also released draft legislation, the Electronic Commerce Framework Bill 1998, that provides for legal recognition of electronic signatures, equivalence to documents in electronic form, presumptions for time of sending and receipt of an electronic communication and criminal offences relating to misuse of computers (eg hacking). It is unclear at this stage whether the Victorian draft legislation will now proceed given the impetus for achieving a uniform Australian approach to regulating Internet commerce. It is believed that all State Attorney-Generals have, in principle, agreed to use the Commonwealth Electronic Transactions Act as a model for any State legislation, although this is subject to the Commonwealth legislation being assessed as a satisfactory model.

Finally, whilst mostly voluntary, there are a number of Australian industry codes that affect the conduct of Internet commerce by Australian businesses. Some

---

372 Section 14, Electronic Transactions Act 1999.
373 Section 15, Electronic Transactions Act 1999.

important codes are the Internet Industry Association Code of Practice **("IIA Code of Practice")**, Australian Direct Marketing Association's Standards of Practice **("ADMA Code of Conduct")**, the Ministerial Council on Consumer Affairs Direct Marketing Model Code of Practice and the Privacy Commission National Principles for the Fair Handling of Personal Information.

So what legal risks to Australian businesses can be identified from a review of the Australian legislation and voluntary codes of practice? Several legal risks were identified, most of which arose due to the operation of legislation that is not specifically aimed at Internet commerce. In other words, the vast majority of the identified legal risks also arise in relation to commerce that is conducted off-line. The Commonwealth Electronic Transactions Act 1999 (Cth), not surprisingly given that it aims to remove certain legal risks associated with Internet commerce, does not give rise to new legal risks although whether the Act effectively eliminates the legal risks that it seeks to remove will be discussed in the next chapter on legal risk management strategies. Similarly, the Victorian Electronic Commerce Framework Bill 1998 (Vic) does not in itself create additional legal risks to Australian businesses conducting Internet commerce with the exception of the risks associated with contravention of the criminal offence (anti-hacking) provisions of the Bill. Several of the legal risks identified arise in relation to non-compliance with voluntary codes. The principles set out in the codes often overlap. For example, the ADMA Code of Conduct adopts or conforms with the principles set out by the Privacy Commission's National Principles for the Fair Handling of Personal Information. Similarly, the Ministerial Council on

Consumer Affairs Direct Marketing Model Code of Practice is designed to serve as a model for industry associations to follow when establishing their own codes of practice. To eliminate repetition, the identified legal risks are described only once, although the same legal risk may arise by virtue of one or more voluntary codes. The legal risks identified from a review of the Australian legislation and voluntary codes are:

Table 52 LEGAL RISKS ASSOCIATED WITH INTERNET COMMERCE IDENTIFIED THROUGH REVIEWING VOLUNTARY CODES OF CONDUCT
Risk that the business's **promotional and advertising material on** its **web site** constitutes **misleading and deceptive** conduct under s 52, or **a false representation** under s 53, or constitutes engaging in **unconscionable conduct** under s 51AA, s 51AB or s 51AC, or **contravenes the implied warranties and conditions** set out in Part V Division 2 of the Trade Practices Act 1974 (Cth).
Risk that the business's **web site** constitutes **misleading and deceptive conduct** under s 52 of the Trade Practices Act 1974 (Cth).
Where the business provides credit in relation to its Internet transactions, risk of **non-compliance with the consumer credit legislation (Consumer Credit Code)**.
Risk of **non-compliance** with the **Part IV (restrictive trade practices)** of the Trade Practices Act 1974 (Cth).
Risk of **contravening the ADMA Code of Conduct** by **failing to provide complete and current information about the identity of the business** and the goods or services the business offers to customers including, where goods and services are digitised, information such as technical requirements or transmission details[374].
Risk of **contravening the ADMA Code of Conduct** when accepting an offer online for **failing to inform and unambiguously express the offer** in a format **that allows the parties to maintain and complete and accurate record of the transaction**[375].
Risk of **contravening the ADMA Code of Conduct** for **failing to provide online information about making complaints** or failing to develop mechanisms and procedures to facilitate handling complaints, providing redress and pursuing dispute resolution online[376].
Risk of **contravening the ADMA Code of Conduct for failing to develop** and use internationally

[374] Clause D2 ADMA Code of Conduct.
[375] Clause D3 ADMA Code of Conduct.
[376] Clause D4 ADMA Code of Conduct.

interoperable **security and authentication mechanisms** for electronic commerce[377].
Risk of **contravening the ADMA Code of Conduct for collecting personal information** that is not necessary for one or more of the business's legitimate functions or activities[378].
Risk of **contravening the ADMA Code of Conduct for collecting personal information otherwise than by lawful or fair means** and not in an unreasonably intrusive way[379].
Risk of **contravening the ADMA Code of Conduct for collecting personal information** about a customer and **failing to** take reasonable steps to **ensure that the customer is aware of the identity of the business and how to contact the business**, the fact that the customer is able to gain access to the information, the purpose for which the information is collected, to whom the business usually discloses information of the kind collected, any law that requires the particular information to be collected and the main consequences (if any) for the individual if all or part of the information is not provided[380].
Risk of **contravening the ADMA Code of Conduct for collecting information from a third party about a customer** and for failing to take reasonable steps to ensure that the customer is or has been made aware of the identity of the business and how to contact the business, the fact that the customer is able to gain access to the information, the purpose for which the information is collected, to whom the business usually discloses information of the kind collected, any law that requires the particular information to be collected and the main consequences (if any) for the individual if all or part of the information is not provided[381].
Risk of **contravening the ADMA Code of Conduct for using information collected from a customer for "secondary purposes"** unrelated to the primary purpose for which the information was collected[382] unless the customer has consented to its use or disclosure[383], or the business uses the secondary information for the purpose of direct marketing and it is impracticable for the business to seek the customer's consent and the business gives the customer the express opportunity, at the time of first contact or thereafter upon request, and at no cost, to decline to receive any further direct marketing communications and, if at any time the customer declines to receive further direct marketing communications, the business sends no more communications[384].
Risk of **contravening the ADMA Code of Conduct for failing** to take reasonable steps **to make sure that customer information** that it collects, uses or discloses **is accurate, complete and up to date**[385].
Risk of **contravening the ADMA Code of Conduct for failing** to take reasonable steps **to protect customer information** held by the business from misuse and loss and from unauthorised access, modification or disclosure[386].
Risk of **contravening the ADMA Code of Conduct for failing** to take reasonable steps **to destroy or permanently suppress customer information the business no longer needs**[387].

377 Clause D6 ADMA Code of Conduct.
378 Clause E1 ADMA Code of Conduct.
379 Clause E2 ADMA Code of Conduct.
380 Clause E3 ADMA Code of Conduct.
381 Clause E8 ADMA Code of Conduct.
382 Clause E9.1 ADMA Code of Conduct.
383 Clause E9.2 ADMA Code of Conduct.
384 Clause E9.3(a)(b)(c)(d) ADMA Code of Conduct.
385 Clause E14 ADMA Code of Conduct.
386 Clause E15 ADMA Code of Conduct.

Risk of **contravening the ADMA Code of Conduct for failing to have** clearly expressed and readily available **policies on the** business's **management of customer information**[388].
Risk of **contravening the ADMA Code of Conduct for failing**, when requested, to take reasonable steps **to let individuals know, what sort of personal information the business holds**, for what purposes, and how the business collects, holds, uses and discloses that information[389].
Risk of **contravening the ADMA Code of Conduct for transferring customer information to a third party** except: where the business reasonably believes that the third party is subject to a statute, binding scheme or contract which effectively upholds principles for fair information handling that are substantially similar to those set out in the ADMA Code of Conduct; or the customer consented to such transfer, or the transfer is necessary for the performance of a contract between the customer and the business, or for the implementation of pre-contractual measures taken in response to the customer's request; or the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the customer between the business and a third party; or the transfer is for the benefit of the customer and it is not practicable to obtain the consent of the customer to that transfer; and if it were practicable to obtain such consent, the customer would be likely to give it; or the business has taken reasonable steps to ensure that the information which it has transferred will not be collected, held, used or disclosed by the third party inconsistently with the principles set out in the ADMA Code of Conduct[390].
Risk of **contravening the ADMA Code of Conduct for collecting "sensitive" customer information** that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, or details of health or sex life unless the customer has consented or in other limited circumstances[391].
Risk of **contravening the ADMA Code of Conduct for failure to use the "Do Not Mail/Do Not Call" services of the Australian Direct Marketing Association** when conducting a direct marketing campaign in order to remove the name of a consumer (other than a current customer who has made a purchase within the last six months or during a normal selling cycle) who has requested that they not receive direct marketing offers[392].
Risk of **contravening the ADMA Code of Conduct for failure to remove a consumer's name from the business's internal marketing lists** or lists for transfer to a third party **at the request of the consumer**[393].
Risk of **contravening the IIA Code of Practice for failing to provide** a customer when first entering into a transaction **the name of the business's trading entity** and, if the business is a corporation, **the ACN of the corporation**; **the physical location of the business's office and a contact telephone number**; and a **copy of an acceptable use policy** containing guidelines for the lawful and technical use of the Internet as recommended by the Administrative Council (a body

387 Clause E16 ADMA Code of Conduct.
388 Clause E17 ADMA Code of Conduct.
389 Clause E18 ADMA Code of Conduct.
390 Clause E30 ADMA Code of Conduct.
391 Clause E31 ADMA Code of Conduct.
392 Clause E33 ADMA Code of Conduct.
393 Clause E34 ADMA Code of Conduct.
394 Clause 7.1 IIA Code of Practice.

described in clause 15 of the IIA Code of Practice)[394].
Risk of **contravening the IIA Code of Practice for failing to comply with the Australian Association of National Advertisers Code of Ethics**[395].
Risk of **contravening the IIA Code of Practice for failing to provide customers with contact details of relevant Australian authorities** in relation to any service or content available on the Internet that the customer considers is fraudulent, misleading or deceptive and likely to cause loss or damage to third parties, or is illegal[396].
Risk of **contravening the IIA Code of Practice for failing to comply with the National Principles for the fair handling of personal information**[397].
Risk of **contravening the IIA Code of Practice for failing to keep confidential customer information and communications**[398].
Risk of **contravening the IIA Code of Practice for collecting customer information that is not relevant and necessary** for the service or product that the business is providing to the customer or collecting customer information for a legitimate purpose without making it known to the customer at the time the details were collected[399].
Risk of **contravening the IIA Code of Practice for using customer information other than for the business's internal marketing, billing or purposes made known to the customer** prior to the time the information was collected or other purposes with the prior consent of the customer[400].
Risk of **contravening the IIA Code of Practice by** knowingly **placing illegal content** on the Internet, or **allowing illegal content** to remain on the Internet in an area over which the business has control and the technical ability to remove or block such content[401].
Risk of **contravening the IIA Code of Practice by** knowingly **placing invitations or directions** including hyperlinks **to illegal content**[402].
Risk of **contravening the IIA Code of Practice by knowingly placing** descriptors in **meta-tags or other coding** by which means the business's web pages can be located by automated general-purpose search engines, **so as to misrepresent the content contained on the business's web pages**[403].
Risk of **contravening the IIA Code of Practice by failing to**, where technically feasible, **ensure** that services the business provides that contain **content unsuitable for underage customers** are: **segregated** and have clearly **identifiable labels which can be recognised by filter software or technologies**, **or accompanied by suitable on-screen warnings** which appear to

395 Clause 7.4 IIA Code of Practice.
396 Clause 7.5 IIA Code of Practice.
397 Clause 8.1 IIA Code of Practice.
398 Clause 8.2 IIA Code of Practice.
399 Clause 9.1 IIA Code of Practice.
400 Clause 9.2 IIA Code of Practice.
401 Clause 10.1 IIA Code of Practice.
402 Clause 10.2 IIA Code of Practice.
403 Clause 10.3 IIA Code of Practice.
404 Clause 10.4 IIA Code of Practice.

the user before the content can be viewed, or access-managed by subscription enrolments to exclude under age customers[404].
Risk of **contravening the IIA Code of Practice by failing** to take reasonable steps **to ensure that technologies that rate web page content can classify the business's web site**[405].
Risk of **contravening the IIA Code of Practice** by **knowingly placing material** on the Internet **that infringes copyright**[406].
Risk of **contravening the IIA Code of Practice by failing to advise a customer** before a sale or agreement to sell is concluded on the Internet: **if the method of payment** chosen by the customer **is not secure** according to guidelines made available by the Administrative Council Council (a body described in clause 15 of the IIA Code of Practice**), the refund or exchange policy applicable to the sale and the legal jurisdiction which applies to the sale**[407].
Risk of **contravening the IIA Code of Practice** by **failing to advise a customer** before a sale or agreement to sell is concluded on the Internet: **the costs** which the customer will incur as a result of the purchase, including delivery costs; **of any specification** or characteristic **of the product** which might reasonably be expected to be relevant to the customer's decision to buy the product if that specification or characteristic is materially different from the specification or characteristic that a reasonable customer might assume the product to have having regard to the information supplied by the business on the Internet; **the time within which the product will be delivered to the customer; a copy of any other applicable terms and conditions of sale**[408].
Risk of **contravening the IIA Code of Practice**, where the business sells software on the Internet, **by failing to make available** to a customer before a sale or agreement to sell is concluded: **the terms of the software licence agreement**; and **a specification of the size of the program and the operating system and equipment required to run it efficiently**[409].
Risk of **contravening the IIA Code of Practice**, where the business sells content on the Internet to be delivered on the Internet, **for failing to advise a customer**, before a sale or agreement to sell is concluded: **particulars of the content** including an accurate description, synopsis or sample, the form in which the content exists (written, illustrated, video, animated etc), **the size of the file containing the content; any restrictions that will apply to the customer's right to use the content that is downloaded; and the operating system and equipment required to view or otherwise use the content**[410].
Risk of **contravening the IIA Code of Practice**, where the business sends **unsolicited e-mail**, **for failing to establish a toll-free telephone number, valid sender operated return e-mail address or postal address** that the recipient of the unsolicited mail may call, e-mail or write to, as the case may be, to notify the business not to send any further unsolicited e-mail; or for failure to include in all unsolicited e-mail a statement informing the recipient of the toll-free telephone number that the recipient may call, or a valid return address to which the recipient may write or e-mail, as the case may be, notifying the business not to send the recipient any further unsolicited e-mail to any of the addresses of the recipient, or if the recipient is an employer, not to send any further unsolicited mail to the addresses provided by the employer; or for failure, upon notification of a request to receive further unsolicited e-mail, to cease sending any more unsolicited e-mail; or

405 Clause 10.6 IIA Code of Practice.
406 Clause 10.7 IIA Code of Practice.
407 Clause 11.1 IIA Code of Practice.
408 Clause 11.2 IIA Code of Practice.
409 Clause 11.3 IIA Code of Practice.
410 Clause 11.4 IIA Code of Practice.

for failure to include in the subject line of each unsolicited e-mail "ADV:" as the first four characters[411].

Risk of **contravening the IIA Code of Practice** for sending **unsolicited e-mail** which contains **content unsuitable for underage recipients** or for sending unsolicited e-mail that contains a link or links to content unsuitable for underage recipients but **without including in the subject line "ADV:ADLT"** as the first eight characters and without including in the body of the message that the e-mail is intended for adults only[412].

Internet commerce is becoming increasingly regulated in overseas jurisdictions, particularly in the US in relation to recognition of digital and electronic signatures[413], and in the European Union in relation to privacy concerns[414].

In addition, there are now moves to implement uniform laws (harmonize national laws) on some aspects of Internet commerce, such as electronic signatures. For example, the United Nations Commission on International Trade Law **("UNCITRAL")**, in 1996 adopted the Model Law on Electronic Commerce, which several countries including Australia have used as a basis for enacting national laws on electronic commerce. In addition, UNCITRAL is developing Uniform Rules on Electronic Signatures which it is believed will again be influential in the development of national laws on electronic signatures. Other organisations, such as the International Chamber of Commerce are developing international guidelines on the legal aspects of electronic commerce and on the establishment of an international

---

411 Clause 11.5 IIA Code of Practice.

412 Clause 11.6 IIA Code of Practice.

413 For a comprehensive and up-to-date description of US and some foreign legislation (including Australia) on electronic and digital signatures see the "Summary of Electronic and Digital Signature Legislation" sponsored and maintained by the Information Technology and Electronic Commerce (ITEC) Law Department of the Chicago law firm McBride Baker & Coles: http://www.mbc.com/ds_sum.html.

414 European Union Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data 95/46/EC.

chain of registration and certification authorities[415]. Also, the Organisation for Economic Co-operation and Development **("OECD")** has developed Guidelines Governing the Protection of Privacy and Trans-border Flows of Personal Data[416] and issued a Draft Recommendation of the Council Concerning Guidelines for Consumer Protection in the Context of Electronic Commerce[417]. The International Chamber of Commerce has also developed Guidelines on Advertising and Marketing on the Internet[418].

Where Australia harmonises national law in accordance with these international regulatory frameworks, they will clearly affect Australian businesses conducting Internet commerce. Moreover, Australian businesses are likely to be affected by foreign legislative frameworks regulating Internet commerce. For example, in several cases US courts have held that they have jurisdiction to hear cases involving a breach of State law even though the only connection the business has with the particular State is that the business's web site can be accessed in the State in which jurisdiction has been established[419]. If these judgments continue to be followed and upheld in the

---

415 See the International Chamber of Commerce web site which sets out its activities in relation to the development of international guidelines in respect of the conduct of e-commerce: http://www.iccwbo.org/Business_World/1998/Setting_business_ground_rules.htm. Guidelines developed by the International Chamber of Commerce include ICC Revised Guidelines on Advertising and Marketing on the Internet, General Usage for International Digitally Ensured Commerce (GUIDEC) (6 November 1997) and General Usage for International Digitally Ensured Commerce (GUIDEC) (6 November 1997), ICC International Code of Advertising Practice, ICC International Code of Direct Marketing (1998), ICC International Code of Sales Promotion and Model clauses for use in contracts involving transborder data flows (23 September1998).

416 See http://www.oecd.org.

417 See http://www.oecd.org.

418 See http://www.iccwbo.org/Comissions/Marketing/Internet_Guidelines.html.

419 See for example *Zippo Manufacturing Inc v Zipp.Dot.Com Inc* No 96-397 (W.D. Pa. 16 January 1997) where the United States district Court for the Western District of Pennsylvania held that it had jurisdiction to hear a matter involving a defendant whose connection with Pennsylvania was

US, it would mean that an Australian business could be found subject to the jurisdiction of a US court even if the only connection the Australian business has with that jurisdiction is that the business's web site can be accessed from within that jurisdiction.

Accordingly risks that Australian businesses are exposed to by virtue of overseas legislation or uniform laws include:

Table 53 LEGAL RISKS ASSOCIATED WITH INTERNET COMMERCE IDENTIFIED THROUGH REVIEWING OVERSEAS LEGISLATION OR UNIFORM LAWS

Risk of being **prohibited from transacting** with a customer on the basis that the customer is **subject to the European Community Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data**

almost exclusively over the Internet. As reported by Stephen Saxby in "CLSR Briefing: Lack of jurisdiction defence rejected in Domain Name Dispute", *Computer Law and Security Report*, Vol 13, no 3 1997, p 210. Similarly, in the *State of Minnesota v Granite Gate Resorts Inc*, 568 N.W.2d 715 (Minn. Ct. App. Sept. 5, 1997) a District Court for the State of Minnesota ruled that it had jurisdiction to hear a matter involving the defendant whose sole connection with Minnesota was through its Internet advertisements which could be accessed by residents of Minnesota that linked to a gambling web site. As reported by Stephen Saxby in "CLSR Briefing: Minnesota successfully claims jurisdiction over Internet services" *Computer Law and Security Report*, Vol. 13 no 2 1997, p 142. See also *Maritz, Inc. v. Cybergold, Inc.*, 1996 U.S. Dist. Lexis 14978 (E.D. Mo. 1996), 568 N.W.2d 715 (Minn. Ct. App. Sept. 5, 1997), *Telco Communications v. An Apple A Day*, 977 F.Supp. 404 (E.D. Va. Sept. 24, 1997) and *Superguide v. Kegan*, 44 U.S.P.Q.2d 1770, 1997 WL 754467 (W.D.N.C. Oct. 8, 1997). Note that other cases have taken the opposite view, that is where a business's sole connection with a jurisdiction is due to its web page being accessible in that jurisdiction this will not be sufficient for the court to exercise jurisdiction. See for example, *Cybersell Inc. v Cybersell Inc*, No CV-96-00089-EHC, 9th Cir, C.A. 2 December 1997 as reported by Stephen Saxby in "CLSR Briefing: No personal jurisdiction found in web site dispute", *Computer Law and Security Report*, Vol 14 no 2. 1998, p 143. In this case the US 9th Circuit Court of Appeals held it did not have jurisdiction to hear a matter where the defendant's sole connection with the jurisdiction was through its Internet advertisements. The plaintiff, an Arizona business sought to bring a trademark infringement action against the defendant in Arizona. The defendant was a business physically located in Florida and which operated in Florida. The defendant's only connection with Arizona was it advertised its services on the Internet and these advertisements could be accessed by Arizona residents. See also: *Bensusan Restaurant Corp. v. King*, 1997 WL 560048 (2nd Cir. (N.Y.) (Sept. 10, 1997)), *McDonough v. Fallon McElligott*, 1996 U.S. Dist. Lexis 15139 (S.D. Cal. 1996), *Hearst Corp. v. Goldberger*, 1997 WL 97097, 1997 US Dis. Lexis 2065) (SDNY Feb. 26, 1997), *Weber v. Jolly Hotels*, 977 F.Supp. 327 (D. N.J. Sept. 12, 1997).

95/46/EC which prohibits transferring data to jurisdictions that do not provide adequate level of protection[420].
Risk of **contravening US laws protecting privacy of on-line customers** such as the Children's Online Privacy Protection Act.
Risk that the business's **promotional activities contravene anti-spam legislation** in some US States.

4.3.11 MAKING JUDGMENTS BASED ON EXPERIENCE, BRAINSTORMING

Legal risks can also be identified through brainstorming or through judgments based on experience made by employees of the business that are involved with the Internet commerce activities of the business, or made by the risk management consultants or legal advisers retained by the business to give legal risk management advice. Whilst it is not possible in this thesis to consult and brainstorm with employees in this thesis or for that matter risk management consultants or other legal advisers, it is clear that these techniques for identifying the legal risks associated with Internet commerce are useful. It is however, possible (assuming the role of a legal adviser) to use brainstorming techniques and to make judgments based on experience to identify the legal risks associated with Internet commerce. To illustrate the usefulness of such techniques the following legal risks associated with Internet commerce were identified by applying techniques such as brain-storming and through judgments based on experience:

---

420 Article 25 of the Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data 95/46/EC of the European Parliament and of the Council of 24 October 1995.

Table 54 LEGAL RISKS ASSOCIATED WITH INTERNET COMMERCE IDENTIFIED THROUGH JUDGMENTS BASED ON EXPERIENCE AND BRAINSTORMING
Risk of **liability for statutory non-compliance** with sections 52 (misleading and deceptive conduct) and 53 (false representations) of the **Trade Practices Act 1974 (Cth)** in relation to **advertising material** transmitted through the Internet whether it be e-mail or on the business's web page.
Risk of **contractual liability** such as for **misrepresentation**, **or breach of a term** in relation to **advertising material** transmitted through the Internet whether it be e-mail or on the business's web page.
Risk of liability for **breach of duty of confidentiality** for **using information obtained from customers** who have transacted with the business on the Internet for purposes other than the purpose for which the information was disclosed eg for marketing purposes or by selling such market information to a third party.
Risk of **liability (potentially criminal liability) for statutory non-compliance** with **laws regulating content** such as child pornography laws, gambling laws and securities laws both in Australia and in overseas jurisdictions where the business offers to trade with customers residing overseas.
Risk of **statutory non-compliance with consumer protection laws** both in Australia and in overseas jurisdictions where the business offers to trade with customers residing overseas.
Risk that the Internet **transactions** entered into by a business are **governed by the law of the jurisdiction in which the customer resides** rather than the jurisdiction from which the business operates.
Risk that an Internet transaction is unenforceable for failure to satisfy the requirement in relation to certain transactions that they be evidenced in writing.
Risk that that a business becomes **contractually bound to terms unintentionally** such as (a) where a business's **marketing and promotional activities** (whether through the web or by e-mail) **constitutes making an "offer"** rather than an "invitation to treat"; (b) where a business's purported **withdrawal of an "offer" to a customer is precluded** because the business's "offer" has been accepted by a customer; (c) where during the course of negotiating the terms of an Internet transaction **a "battle of the forms" situation arises** such that the customer's terms override the business's; (d) where the **terms** of the contract negotiated between the business and a customer **are altered by erroneous transmission**; (e) where the **business's computer software** used for conducting Internet commerce **is erroneously programmed or malfunctions** so it makes or accepts offers in circumstances unauthorised by the business.
Risk that an **acceptance** communicated by a business **does not give rise to a binding contract**.
The risk that a **customer is not contractually bound** to **standard terms** purportedly incorporated by a business.
The risk that a business enters into a **contract that is invalid because** it was unauthorised (i) where the party with whom the business is transacting is **unauthorised to enter into the transaction** due to laws prohibiting or otherwise regulating the type of goods or services offered by a business to that party **or**, (ii) where the party with whom the business is transacting is purportedly acting for a principal but **lacks actual, ostensible, or implied actual authority to do so**.

In relation to the acceptance of on-line payments by a business, risk that the **payment made will be dishonoured by the issuer of the form of payment** used by the customer (for example, where payment has been accepted in the form of digital cash, the digital cash issuer may refuse to honour the payment on the ground that the digital cash proffered by the business's customer was forged, or, if payment was effected by electronic cheque, the cheque bounced).
Risk of **statutory non-compliance with copyright laws both in Australia and in overseas jurisdictions** in relation to **images and text used** on the business's web site (including meta-tagging) or for framing or linking to other web sites.
Risk of **failure to adequately protect intellectual property rights** such as copyright and trademarks.
Risk **of failure to adequately protect use of business's name as a domain name**.
Risk of **liability in negligence** to customers **for failure to adequately protect personal and financial information about customers** when such information is hacked and used fraudulently by third parties.
Risk of **liability to pay an "Internet" tax** in **overseas jurisdictions**.
Risk of **liability for statutory non-compliance** in relation to the obligation to pay taxes such as **sales tax, customs, stamp duties tax both in Australia and in overseas jurisdictions**.
Risk of **liability for statutory non-compliance** in relation to legislation prohibiting **transmission of unsolicited e-mail in overseas jurisdictions**.
Risk of **liability under the Trade Practices Act 1974 (Cth) for misleading and deceptive conduct** and or **liability for trademark infringement** where the business uses the **names of competitors** in its web pages in order that customers searching for a competitor of the business will also receive a search "hit" on the business's web site.

4.3.12 USING SYSTEMS ANALYSIS, SCENARIO ANALYSIS AND SYSTEMS ENGINEERING TECHNIQUES OR CONSTRUCTING FLOWCHARTS OF THE BUSINESS'S OPERATIONS

Systems analysis, scenario analysis, systems engineering techniques and constructing flow charts of the business's operations refer to risk identification techniques which involve examining a business's processes and operating procedures and, from such examination, forecasting possible causes of accidents or system errors or failures. These techniques often employ logical and mathematical methods for identifying risk. For example, systems safety techniques are described as:

> …a collection of logical and mathematical techniques that are continually applied to the detection and correction of hazards from the early conceptual state of a product right on through its detailed design and operation. It includes a study of operating procedures, test procedures, inspections, scheduled top management reviews, and attention to nontechnical areas such as readability of manuals and motivation of workers.[421]

Systems analysis, scenario analysis and systems engineering techniques can be useful for determining some legal risks associated with Internet commerce. More specifically, these techniques can be particularly useful in identifying those legal risks that arise in relation to the software and hardware used by the business in order to conduct Internet commerce. Thus, an examination of the transactions conducted by a business on the Internet at a technical level can reveal aspects of the business's Internet activities that expose the business to legal risk. Given the multitude of Internet commerce software and hardware systems[422] available it is not possible here to undertake a systems analysis of each and every Internet commerce system available. Instead, the research will focus on the process and operating procedures associated with a typical Internet commerce system with a view to identifying some legal risks. First, it is necessary to outline what constitutes an Internet commerce system. At the very least an Internet commerce system will involve software that links a business's existing sales, inventory and billing systems with the software used to enable the conduct of Internet commerce and relevant hardware such as an Internet commerce server to enable the an Internet presence and manage payments made

---

421 Emmett J Vaughan, *Risk Management*, John Wiley & Sons, Inc, New York, 1997, Ch 6, p 110.

422 For example, Forrester Research estimates that there are more than 100 choices available to Internet businesses in relation to commerce-server software. As reported in John Berry, "Mining for E-Commerce Gold", in www.cmpnet.com, the Technology Network, 8 October 1998, http://www.webtools.com/story/TLS19981998S0001.

through the Internet. A more comprehensive Internet system involves much more and can include provision for inventory, customer-profiling (such as session profiles of a customer's behaviour on entering a web site), billing, direct connections with supply-chain partners and management of pricing, shipping and taxation information[423].

Based on a consideration of the mechanics of conducting Internet commerce, the following legal risks are identified. It should be noted that most of these legal risks have been already identified in this chapter using other techniques for identifying legal risk.

Table 55 LEGAL RISKS ASSOCIATED WITH INTERNET COMMERCE IDENTIFIED THROUGH USING SYSTEMS ANALYSIS, SCENARIO ANALYSIS AND SYSTEMS ENGINEERING TECHNIQUES OR CONSTRUCTING FLOWCHARTS OF THE BUSINESS'S OPERATIONS
Risk that a business is **contractually bound to terms** on which it did not intend as a result of **a fault or defect in** the business's Internet commerce **hardware or software** which caused the business's Internet commerce software to make an unauthorised offer to or acceptance from a customer.
Risk of **tortious liability or liability under the product liability provisions of the Trade Practices Act 1974 (Cth) and State and Territory equivalents for injury and loss** caused as a consequence of a **fault or defect** in the business's Internet commerce **hardware and software**.
Risk of **liability in negligence** to customers **for failing to ensure adequate computer security** if the security protection of the business is such that a customer's credit card information is hacked into and misappropriated and misused by third parties.
Where the business hasn't implemented non-repudiation mechanisms, risk of **repudiation** of an Internet transaction **by a party on the false basis** that it was a third party imposter not the customer who fraudulently appropriated the identity and credit card information of the customer when transacting with the business.
Liability for **failure to** impose on behalf of and to **pay** to relevant regulatory authorities any **taxes** payable on Internet transactions conducted with customers.
Liability for defamation or for **regulatory non-compliance** in relation to **content legislation** if the business allows material to appear on its web site that is defamatory or contravenes content legislation. This liability can also arise when the business allows customers or other parties to add

[423] John Berry, "Mining for E-Commerce Gold", in www.cmpnet.com, the Technology Network, 8 October 1998, http://www.webtools.com/story/TLS19981998S0001.

material to the business's web eg by way of chat areas or threaded discussions.

4.4 Overview of legal risks that are particular to Internet commerce

Having applied several techniques for identifying the legal risks associated with Internet commerce it can be seen that many of the identified legal risks equally affect businesses that conduct Internet commerce and businesses that conduct off-line commerce. Also, many of the legal risks identified have been identified more than once, having been identified by more than one risk identification technique.

It is relevant at this point therefore to eliminate any "duplicate" identified risks. It is also relevant at this point to distinguish between those risks that are particular to Internet commerce and those legal risks that equally arise in relation to the conduct of off-line commerce. Whilst a business applying risk management should identify and apply risk management strategies in relation to all legal risks it faces regardless of whether such legal risks also equally arise in relation to the conduct of commerce off-line it is not proposed in this thesis to go beyond identifying such legal risks. The reasoning for such an approach is simple. As can be seen from the discussion in this chapter, there are a considerable number of legal risks facing a business conducting Internet commerce. For reasons of word limits it is not possible in this thesis to evaluate each identified legal risk and discuss appropriate risk management strategies. Accordingly, it is proposed to consider only a representative number of legal risks in order to examine the extent to which the remaining steps in the risk management procedure can apply in the context of managing legal risk. It follows that it would be a more useful contribution to legal research if those legal risks that

differ from or are additional to the legal risks associated with off-line commerce are the subject of further investigation. Many businesses are already aware of the legal risks they face in conducting commerce off-line and are more interested in discovering what additional legal risks if any they face in relation to the conduct of Internet commerce. Similarly, from an academic viewpoint it is arguably more important to examine and evaluate the additional legal risks facing businesses that conduct Internet commerce.

The legal risks associated with the conduct of Internet commerce that differ from or are additional to the legal risks associated with off-line commerce can be attributed to three key characteristics of Internet commerce, that is: (i) Internet commerce operates in a digital and paperless environment, (ii) Internet commerce involves distance (non-face-to-face) commerce and (iii) Internet commerce can involve cross jurisdictional commerce.

4.4.1 INTERNET COMMERCE OPERATES IN A DIGITAL AND PAPERLESS ENVIRONMENT

The fact that Internet commerce operates in a digital and paperless environment does give rise to a number of legal risks that differ from or are additional to the legal risks associated with off-line commerce. The legal risks are listed in figure Table 57 at p223.

The fact that Internet commerce operates in a digital and paperless environment gives rise to a new set of legal risks that are not faced by businesses conducting business off-line and these legal risks stem from legislation or other frameworks that regulate Internet commerce. Because Internet commerce is undertaken in a digital

and paperless environment, there is a perception that consumers are more vulnerable to fraud and abuse of consumer privacy because, as the argument goes, sham businesses can use digital technology to convincingly appear to be a legitimate business (such as by appropriating legitimate business's e-mail addresses) and to extract much more personal information about a consumer than is possible without digital technology. Moreover, the absence of a paper trail makes it difficult for a consumer to prove that the consumer transacted with a business, consequently hampering enforcement. Consequently, legislation has been enacted or other regulatory frameworks, such as voluntary codes of practice, have been implemented that impose practices aimed at protecting consumers that purchase on the Internet. Where a business conducting commerce is regulated by such legislation or voluntary codes, this gives rise to a new set of legal risks facing a business that conduct Internet commerce, such as those listed at Table 57 at p223.

4.4.2 INTERNET COMMERCE INVOLVES DISTANCE (NON-FACE-TO-FACE) COMMERCE

A number of the legal risks identified earlier in this chapter arise because Internet commerce lacks face-to-face contact. It is argued here that such legal risks (collectively referred to here as the **"legal risks associated with establishing identity"**), are not, however, particular to Internet commerce. Contracts take place every day off-line when the identities of the contracting party are simply unknown and off-line businesses that transact on that basis are surely exposed to the same legal risks associated with establishing identity as those businesses that conduct Internet commerce.

There is a perception, however, that there are additional legal risks in relation to Internet commerce or that existing legal risks are in some way amplified. So why does contracting on the Internet make a difference? In an effort to pinpoint why the risks associated with establishing identity are perceived to be different from the risks associated with establishing identity in relation to off-line distance commerce, it is useful to consider the circumstances in which establishing identity is important in relation to Internet commerce. A business conducting Internet commerce will be concerned about establishing identity in the following instances:

Table 56 INSTANCES WHERE A BUSINESS CONDUCTING INTERNET COMMERCE WILL BE CONCERNED WITH ESTABLISHING IDENTITY BECAUSE INTERNET COMMERCE INVOLVES DISTANCE (NON-FACE-TO-FACE) COMMERCE
When a business seeks to enforce an Internet transaction. Identity needs to be proved. Otherwise a party could repudiate a contract on the basis that the party with whom the business transacted was an imposter who assumed the identity of the party with whom the business thought it was contracting.
Where a business transacts with a party purporting to act on behalf of another (a typical agency problem). A business is interested in proving identity and authorship of a message in such circumstances either to ascertain that the transacting party is legitimately acting as an agent, or in the event that a business seeks to enforce a transaction, to prove that the business was justified in concluding that the party with whom the business transacted had actual, ostensible or implied authority to transact with the business on behalf of another party.
Establishing identity is important where payments are made on the Internet and a business wants to ensure that the payment will not be disputed by a transacting party arguing that the payment was made by an imposter purporting to be the transacting party or by the transacting party falsely repudiating the payment by claiming it was made by an imposter. This situation is arguably just a subset of the "enforcement" situation.
Where a business is subject to some regulatory provision that prohibits transacting with certain parties (eg parties residing in a certain jurisdiction, underage individuals etc). In this instance, a business is concerned with identity as it does not want to break the law. Here the business is not so concerned with knowing the name of the contracting party but is concerned with factors such as the age of the transacting party or jurisdiction in which the contracting party resides.

Clearly, the types of legal risks identified above are also faced by businesses that conduct business off-line, particularly those businesses that conduct distance commerce. So why is there a perception that Internet commerce gives rise to additional legal risk in respect of the legal risks associated with establishing identity? One argument is that when businesses are unsure of a customer's identity off-line and want to verify it they usually ask to look at third party verified forms of identification such as driver's licences or passports; this type of third party verification can't occur in respect of Internet commerce. There are two points that need to be made in respect of this argument. First, this problem arises equally in relation to distance commerce conducted off-line where it is not possible to ask a customer ordering through mail order or by telephone to provide a form of identification that has been verified by a third party. Secondly, although a customer can't show a passport or driver's licence during the course of an Internet transaction, a customer could provide a digital certificate, certified by a trusted third party which has the effect of confirming the identity of the customer (Digital certificates, how they work and how they can be used to minimise legal risk, are discussed in detail in the next chapter).

Another argument in favour of the view that there are additional legal risks associated with establishing identity in relation to the conduct of Internet commerce is that it is easier to appropriate the credit card information of a third party and that party's identity, or to falsely purport to act on behalf of a principal through access to the principal's computer and e-mail in the context of Internet commerce. This is because it is easier to forge identification and commit identity fraud in a digital

environment. Whilst that may be the case (arguably it is equally easy to effect forgery and misappropriate another's identity in relation to commerce conducted off-line given the availability of scanners, laser printers and image manipulation software that enables convincing paper-based forgeries to be created) this does not create an additional legal risk that affects those businesses that conduct Internet commerce. Instead this factor influences the likelihood of a legal risk eventuating, such legal risk equally occurring in relation to off-line commerce.

A further argument that supports the view that there are additional legal risks associated with establishing identity in relation to the conduct of Internet commerce is that more forms of payment can be used in respect of Internet commerce than can be used in respect of commerce conducted off-line and that this in turn creates additional legal risk. Payment can be effected on the Internet by way of digital cash and electronic cheque in addition to the forms of payment that are used in relation to commerce conducted off-line (that is credit card, cheque and money order, but with the exception of cash). But does this create legal risks? Admittedly this analysis turns on how one chooses to characterise a given legal risk. Here the legal risk that a business faces in accepting online forms of payment that do not exist in relation to commerce conducted off-line is characterised as the legal risk that the form of payment used (that is digital cash or electronic cheque) is dishonoured or that the customer has fraudulently or, where the customer purports to be an agent of a third party, without authority of the principal, taken on the identity of another and used the third party's payment mechanism (digital cash or electronic cheque) without

authority. This legal risk is arguably experienced by businesses accepting the other forms of payment that are used for effecting payment in commerce. So again, it is arguable that there is no additional legal risk associated with accepting payment on the Internet although the likelihood of such risk is affected by the fact that there are additional methods by which payment can be effected through the Internet.

Finally, it is arguable that businesses conducting Internet commerce face an additional legal risk. that being the legal risk of unlawfully transacting with minors or parties with whom it is illegal or unauthorised to contract. This argument is based on the premise that when commerce is conducted off-line and face-to-face such a risk is practically non-existent. There are a few points that need to be made in response to this type of argument. Firstly, a business conducting off-line face-to-face commerce that is prohibited from transacting, or who does not want to transact, with a certain class of customer (eg minors) still faces the risk of unlawfully transacting with minors or parties with whom it is illegal or unauthorised to act. It is just that in face-to-face commerce the likelihood of such risk eventuating is less than when the same type of transaction is conducted on the Internet as, presumably, some customers (particularly underage customers) can be eliminated when the customer is sighted. Secondly, this supposed "additional" risk equally arises in relation to businesses who conduct commerce off-line but who conduct distance commerce such as mail order or telephone order. In such instances, it is argued the legal risk of unlawfully transacting with minors or parties with whom it is illegal or unauthorised to contract is exactly

the same whether the business conducts distance off-line commerce or Internet commerce.

In conclusion, although it may at first appear that there are additional legal risks associated with establishing identity in relation to Internet commerce in fact this is not the case. What however does exist is an increased likelihood that the legal risks associated with establishing identity eventuate when businesses conducting Internet commerce accept online forms of payment. In other words, the legal risks associated with establishing identity are equally shared by businesses that conduct Internet commerce and businesses that conduct commerce off-line. As noted by the Professional Development Committee of the council of the Law Society (UK) in its comments on the European Parliament Council Directive on a Common Framework for Electronic Signatures:

> Trade, whether national or international, has for hundreds of years been carried on between parties at a distance from each other, relying on communications by letter, and then more recently by cable, telephone, telex and fax. Remote trading of this kind has been successfully carried on without any system for authenticating signatures, whether hand-written, or in type, on cables, telex or fax, or, indeed in the form of voice, by telephone.
>
> It is not difficult to forge a signature well enough to deceive a casual reader, letterheads are generally not very difficult to copy, or headed paper may be stolen. "Signatures" on cables or telex have no identifying qualities and it is probably easier to forger a signature for faxing than an original one, because of the loss of quality in reproduction.
>
> None of this, however, provided a significant barrier to trade.
>
> …
>
> The arrival of new forms of electronic communication, e-mail and the Internet, has not created a need which did not hitherto exist for an authentication system for documents created for the purposes of trade.

> Indeed, trade is already being carried on electronically unobstructed by the absence of such a system.[424]

Although it has just been concluded that Internet commerce does not give rise to any additional legal risks in relation to identification, given the lack of consumer and business confidence it is nevertheless useful to list the legal risks associated with establishing identity, which have arguably an increased likelihood of eventuating when arising in the context of Internet commerce. These are listed at Table 57 at p223.

4.4.3 INTERNET COMMERCE CAN INVOLVE CROSS-JURISDICTIONAL COMMERCE

Additionally, the fact that Internet commerce can involve cross-jurisdictional transactions (interstate and international transactions) gives rise to legal risks. Again, however, many of these legal risks are faced by businesses that conduct distance commerce that involves conducting commerce across jurisdictions. Eliminating those legal risks that are shared (that is, excluding those legal risks that arise equally in relation to the conduct of Internet commerce and the conduct of distance, cross-jurisdictional, commerce off-line), the legal risks that are additional to Internet commerce are set out at Table 57 at p223.

4.4.4 TABLE OF LEGAL RISKS PARTICULAR TO INTERNET COMMERCE (STEP 2)

It is useful to list in one table the legal risks that are particular to Internet commerce:

---

[424] Professional Development Committee of the Council of the Law Society, "Proposal for a European Parliament and Council Directive on a Common Framework for Electronic Signatures- Comments by the Professional Development Committee of the Council of the Law Society", June 1998, http://techpolicy.ise.ac.uk/carc/sign/lawsoc.html.

Table 57 LEGAL RISK MANAGEMENT IN RELATION TO INTERNET COMMERCE- STEP 2

STEP 2	LEGAL RISKS THAT ARISE BECAUSE INTERNET COMMERCE OPERATES IN A DIGITAL AND PAPERLESS ENVIRONMENT
IDENTIFY-ING THE LEGAL RISKS	Risk that a business **cannot enforce a contract** against a customer **because the business seeks to rely on electronic records** which are not acceptable according to the standards of proof currently required under law to prove that it transacted with a particular party.
	Risk that the business **is contractually bound to a transaction** because **although revocation** of the business's **offer was received by the customer's computer** it was not accessed and read by **the customer** who, in the meantime, **had communicated acceptance of the business's offer**[425].
	Risk that a **customer repudiates a contract on the basis that the** customer's **offer** to purchase **lapsed or was revoked** as a consequence of the delay of the customer's offer having reached the business due to no fault of either transacting party[426].
	In the event that a business unintentionally transmits a computer virus to a customer during the course of conducting Internet commerce, risk of **liability** in **trespass for wrongfully transmitting a computer virus**[427].
	In the event that a business unintentionally transmits a computer virus to a customer during the course of conducting Internet commerce, risk of **liability** in **negligence for wrongfully transmitting a computer virus**[428].
	Risk that **information, records and signatures that are in an electronic form are denied legal effect** solely on the grounds that they are in an electronic form[429].
	Risk that an **Internet transaction cannot be proved** because electronic records of the transaction were not generated by the business and the use of secondary records such as a record held by a bank showing that the vendor communicated with a customer's bank in order to get payment is not admissible because such record constitutes hearsay[430].

425 Law Commission, "Electronic Commerce Part One- A guide for the Legal and Business Community", NZLC R50, October 1998, Wellington, New Zealand, p 32, para 83.

426 Law Commission, para 87.

427 Law Commission, para 153.

428 Law Commission, paras 172-175.

429 *Electronic Commerce: Building the Legal Framework* Report of the Electronic Commerce Expert Group to the Attorney-General, 31 March 1998, http://law.gov.au/aghome/advisory/eceg/ecegreport.html, para 2.5.8; International Chamber of Commerce, "General Usage for Internationally Ensured Commerce (GUIDEC)", 1997, http://www.iccwbo.org/guidec2.htm, para IV.2.

430 Electronic Commerce Taskforce, "Report of the Electronic Commerce Task Force to the Commonwealth Law Enforcement Board", Commonwealth of Australia, November 1996, p 67, paras 6.5.6-6.5.10.

	Risk that **storage of records in electronic form does not comply with laws** requiring records to be retained[431].
	Risk, if the Internet transaction were subject to the **requirement that it be in writing**, that **an Internet communication would not satisfy** the requirement if the transaction were evidenced only in electronic form[432].
	Risk that a **signature signed electronically** (eg by using a digital signature) **does not have legal effect**[433].
	Risk that an **Internet communication** evidenced only in electronic form **does not** satisfy the requirements to **constitute an original for evidential purposes** in jurisdictions other than the Commonwealth and NSW, where the common law principles and rules relating to the means of proving the contents of documents have been abolished[434].
	Risk of **legal uncertainty concerning the use and validity of Internet communications in contract formation**[435].
	Risk of **legal uncertainty concerning** the **time and place of dispatch** and **receipt of Internet communications**[436].
	Risk that that a business becomes **contractually bound to terms unintentionally** such as (a) where a business's **marketing and promotional activities** (whether through the web or by e-mail) **constitutes making an "offer"** rather than an "invitation to treat"; (b) where a business's purported **withdrawal of an "offer" to a customer is precluded** because the business's "offer" has been accepted by a customer; (c) where during the course of negotiating the terms of an Internet transaction **a "battle of the forms" situation arises** such that the customer's terms override the business's; (d) where the **terms of the contract** negotiated between the business and a customer **are altered by erroneous transmission**; (e) where the **business's computer software** used for conducting Internet commerce **is erroneously programmed or malfunctions** so it makes or accepts offers in circumstances unauthorised by the business.
	The risk that a **customer is not contractually bound** to **standard terms** purportedly incorporated by a business.
	LEGAL RISKS THAT ARISE BECAUSE INTERNET COMMERCE INVOLVES DISTANCE (NON-FACE-TO-FACE) COMMERCE AND LEGISLATION HAS BEEN ENACTED OR OTHER REGULATORY FRAMEWORKS, SUCH AS VOLUNTARY CODES OF PRACTICE, HAVE BEEN IMPLEMENTED THAT IMPOSE PRACTICES AIMED AT PROTECTING CONSUMERS THAT PURCHASE ON THE INTERNET.
	Risk of being **prohibited from transacting** with a customer on the basis that the **customer is subject to the European Community Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data 95/46/EC** which prohibits transferring data to jurisdictions that

431 *Electronic Commerce: Building the Legal Framework*, paras 2.10.13-2.10.29; 4.1.11.
432 *Electronic Commerce: Building the Legal Framework*, paras 2.6.16-2.6.31; 4.1.8-4.1.9.
433 *Electronic Commerce: Building the Legal Framework*, paras 2.7.28-2.7.36; 4.1.8.
434 *Electronic Commerce: Building the Legal Framework*, paras 2.8.20-2.8.29.
435 *Electronic Commerce: Building the Legal Framework*, paras 2.11.9-2.11.15; 4.1.12.
436 *Electronic Commerce: Building the Legal Framework*, paras 2.15.13-2.15.17.

	do not provide adequate level of protection[437].
	Risk of **contravening US laws protecting privacy of on-line customers** such as the Children's Online Privacy Protection Act.
	Risk that the business's **promotional activities contravene anti-spam legislation** in some US States.
	Risk of **contravening the ADMA Code of Conduct by failing to provide** complete and current **information about the identity of the business** and the goods or service the business offers to customers including, where goods and services are digitised, information such as technical requirements or transmission details[438].
	Risk of **contravening the ADMA Code of Conduct** when accepting an offer online **for failing to** inform and unambiguously **express the offer in a format that allows the parties to maintain and complete and accurate record of the transaction**[439].
	Risk of **contravening the ADMA Code of Conduct for failing to provide online information about making complaints** or failing to develop mechanisms and procedures to facilitate handling complaints, providing redress and pursuing dispute resolution online[440].
	Risk of **contravening the ADMA Code of Conduct for failing to develop** and use **internationally interoperable security and authentication mechanisms** for electronic commerce[441].
	Risk of **contravening the ADMA Code of Conduct for collecting personal information** that is not necessary for one or more of the business's legitimate functions or activities[442].
	Risk of **contravening the ADMA Code of Conduct for collecting personal information otherwise than by lawful or fair means** and not in an unreasonably intrusive way[443].
	Risk of **contravening the ADMA Code of Conduct for collecting personal information** about a customer **and failing to** take reasonable steps to **ensure that the customer is aware of the identity of the business** and how to contact the business, the fact that the customer is able to gain access to the information, the purpose for which the information is collected, to whom the business usually discloses information of the kind collected, any law that requires the particular information to be collected and the main consequences (if any) for the individual if all or part of the information is not provided[444].
	Risk of **contravening the ADMA Code of Conduct for collecting information from a third party about a customer** and for failing to take reasonable steps to ensure that the

[437] Article 25 of the Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data 95/46/EC of the European Parliament and of the Council of 24 October 1995.
[438] Clause D2 ADMA Code of Conduct.
[439] Clause D3 ADMA Code of Conduct.
[440] Clause D4 ADMA Code of Conduct.
[441] Clause D6 ADMA Code of Conduct.
[442] Clause E1 ADMA Code of Conduct.
[443] Clause E2 ADMA Code of Conduct.
[444] Clause E3 ADMA Code of Conduct.

	customer is or has been made aware of the identity of the business and how to contact the business, the fact that the customer is able to gain access to the information, the purpose for which the information is collected, to whom the business usually discloses information of the kind collected, any law that requires the particular information to be collected and the main consequences (if any) for the individual if all or part of the information is not provided[445]. Risk of **contravening the ADMA Code of Conduct for using information collected from a customer for "secondary purposes"** unrelated to the primary purpose for which the information was collected[446] unless the customer has consented to its use or disclosure[447], or the business uses the secondary information for the purpose of direct marketing and it is impracticable for the business to seek the customer's consent and the business gives the customer the express opportunity, at the time of first contact or thereafter upon request, and at no cost, to decline to receive any further direct marketing communications and, if at any time the customer declines to receive further direct marketing communications, the business sends no more communications[448].
	Risk of **contravening the ADMA Code of Conduct for failing to** take reasonable steps to **make sure that customer information** that it collects, uses or discloses **is accurate, complete and up to date**[449]. Risk of **contravening the ADMA Code of Conduct for failing to** take reasonable steps to protect customer information held by the business from misuse and loss and from unauthorised access, modification or disclosure[450]. Risk of **contravening the ADMA Code of Conduct for failing to** take reasonable steps to **destroy or permanently suppress customer information** the business no longer needs[451].
	Risk of **contravening the ADMA Code of Conduct for failing to have** clearly expressed and readily available **policies on the business's management of customer information**[452]. Risk of **contravening the ADMA Code of Conduct for failing**, when requested, to take reasonable steps **to let individuals know, what sort of personal information the business holds**, for what purposes, and how the business collects, holds, uses and discloses that information[453]. Risk of **contravening the ADMA Code of Conduct for transferring customer information to a third party** except: where the business reasonably believes that the third party is subject to a statute, binding scheme or contract which effectively upholds principles for fair information handling that are substantially similar to those set out in the ADMA Code of Conduct; or the customer consented to such transfer, or the transfer is necessary for the performance of a contract between the customer and the business, or for the implementation of pre-contractual measures taken in response to the customer's

445 Clause E8 ADMA Code of Conduct.
446 Clause E9.1 ADMA Code of Conduct.
447 Clause E9.2 ADMA Code of Conduct.
448 Clause E9.3(a)(b)(c)(d) ADMA Code of Conduct.
449 Clause E14 ADMA Code of Conduct.
450 Clause E15 ADMA Code of Conduct.
451 Clause E16 ADMA Code of Conduct.
452 Clause E17 ADMA Code of Conduct.
453 Clause E18 ADMA Code of Conduct.

	request; or the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the customer between the business and a third party; or the transfer is for the benefit of the customer and it is not practicable to obtain the consent of the customer to that transfer; and if it were practicable to obtain such consent, the customer would be likely to give it; or the business has taken reasonable steps to ensure that the information which it has transferred will not be collected, held, used or disclosed by the third party inconsistently with the principles set out in the ADMA Code of Conduct[454].
	Risk of **contravening the ADMA Code of Conduct for collecting "sensitive" customer information** that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, or details of health or sex life unless the customer has consented or in other limited circumstances[455].
	Risk of **contravening the ADMA Code of Conduct for failure to use the "Do Not Mail/Do Not Call" services of the Australian Direct Marketing Association** when conducting a direct marketing campaign in order to remove the name of a consumer (other than a current customer who has made a purchase within the last six months or during a normal selling cycle) who has requested that they not receive direct marketing offers[456].
	Risk of **contravening the ADMA Code of Conduct for failure to remove a consumer's name from the business's internal marketing** lists or lists for transfer to a third party at the request of the consumer[457].
	Risk of **contravening the IIA Code of Practice for failing to provide** a customer when first entering into a transaction **the name of the business's trading entity** and, if the business is a corporation, **the ACN of the corporation**; **the physical location of the business's office and a contact telephone number**; **and a copy of an acceptable use policy** containing guidelines for the lawful and technical use of the Internet as recommended by the Administrative Council (a body described in clause 15 of the IIA Code of Practice)[458].
	Risk of **contravening the IIA Code of Practice for failing to comply with the Australian Association of National Advertisers Code of Ethics**[459].
	Risk of **contravening the IIA Code of Practice for failing to provide customers with contact details of relevant Australian authorities** in relation to any service or content available on the Internet that the customer considers is fraudulent, misleading or deceptive and likely to cause loss or damage to third parties, or is illegal[460].
	Risk of **contravening the IIA Code of Practice for failing to comply with the National Principles for the fair handling of personal information**[461].
	Risk of **contravening the IIA Code of Practice for failing to keep confidential customer information and communications**[462].

454 Clause E30 ADMA Code of Conduct.
455 Clause E31 ADMA Code of Conduct.
456 Clause E33 ADMA Code of Conduct.
457 Clause E34 ADMA Code of Conduct.
458 Clause 7.1 IIA Code of Practice.
459 Clause 7.4 IIA Code of Practice.
460 Clause 7.5 IIA Code of Practice.
461 Clause 8.1 IIA Code of Practice.

	Risk of **contravening the IIA Code of Practice for collecting customer information that is not relevant** and necessary for the service or product that the business is providing to the customer or collecting customer information for a legitimate purpose without making it known to the customer at the time the details were collected[463].
	Risk of **contravening the IIA Code of Practice for using customer information other than for the business's internal marketing, billing or purposes made known to the customer** prior to the time the information was collected or other purposes with the prior consent of the customer[464].
	Risk of **contravening the IIA Code of Practice by knowingly placing illegal content on the Internet**, **or allowing illegal content to remain on the Internet** in an area over which the business has control and the technical ability to remove or block such content[465].
	Risk of **contravening the IIA Code of Practice by knowingly placing invitations or directions including hyperlinks to illegal content**[466].
	Risk of **contravening the IIA Code of Practice by** knowingly **placing descriptors in meta-tags or other coding** by which means the business's web pages can be located by automated general-purpose search engines, **so as to misrepresent the content contained on the business's web pages**[467].
	Risk of **contravening the IIA Code of Practice by failing to**, where technically feasible, **ensure that services** the business provides **that contain content unsuitable for underage customers are: segregated and have clearly identifiable labels which can be recognised by filter software** or technologies, or accompanied by suitable on-screen warnings which appear to the user before the content can be viewed, or access-managed by subscription enrolments to exclude under age customers[468].
	Risk of **contravening the IIA Code of Practice by failing to take reasonable steps to ensure that technologies** that rate web page **content can classify the business's web site**[469].
	Risk of **contravening the IIA Code of Practice by knowingly placing material on the Internet that infringes copyright**[470].
	Risk of **contravening the IIA Code of Practice by failing to advise a customer** before a sale or agreement to sell is concluded on the Internet: **if the method of payment** chosen by the customer **is not secure** according to guidelines made available by the Administrative Council (a body described in clause 15 of the IIA Code of Practice), **the refund or exchange policy applicable to the sale and the legal jurisdiction which**

462 Clause 8.2 IIA Code of Practice.
463 Clause 9.1 IIA Code of Practice.
464 Clause 9.2 IIA Code of Practice.
465 Clause 10.1 IIA Code of Practice.
466 Clause 10.2 IIA Code of Practice.
467 Clause 10.3 IIA Code of Practice.
468 Clause 10.4 IIA Code of Practice.
469 Clause 10.6 IIA Code of Practice.
470 Clause 10.7 IIA Code of Practice.
471 Clause 11.1 IIA Code of Practice.

	applies to the sale[471].
	Risk of **contravening the IIA Code of Practice by failing to advise** a customer before a sale or agreement to sell is concluded on the Internet: **the costs which the customer will incur as a result of the purchase**, including delivery costs; **of any specification or characteristic of the product** which might reasonably be expected to be relevant to the customer's decision to buy the product if that specification or characteristic is materially different from the specification or characteristic that a reasonable customer might assume the product to have having regard to the information supplied by the business on the Internet; **the time within which the product will be delivered to the customer; a copy of any other applicable terms** and conditions of sale[472].
	Risk of **contravening the IIA Code of Practice**, where the business sells software on the Internet, **by failing to make available** to a customer before a sale or agreement to sell is concluded: **the terms of the software licence agreement; and a specification of the size of the program and the operating system and equipment required to run it efficiently**[473].
	Risk of **contravening the IIA Code of Practice**, where the business sells content on the Internet to be delivered on the Internet, **for failing to advise** a customer, before a sale or agreement to sell is concluded: **particulars of the content including an accurate description**, synopsis or sample, the form in which the content exists (written, illustrated, video, animated etc), **the size of the file containing the content; any restrictions that will apply to the customer's right to use the content that is downloaded; and the operating system and equipment required to view or otherwise use the content**[474].
	Risk of **contravening the IIA Code of Practice**, where the business sends **unsolicited e-mail**, **for failing to establish a toll-free telephone number**, **valid sender operated return e-mail address or postal address** that the recipient of the unsolicited mail may call, e-mail or write to, as the case may be, to notify the business not to send any further unsolicited e-mail; or for failure to include in all unsolicited e-mail a statement informing the recipient of the toll-free telephone number that the recipient may call, or a valid return address to which the recipient may write or e-mail, as the case may be, notifying the business not to send the recipient any further unsolicited e-mail to any of the addresses of the recipient, or if the recipient is an employer, not to send any further unsolicited mail to the addresses provided by the employer; or for failure, upon notification of a request to receive further unsolicited e-mail, to cease sending any more unsolicited e-mail; or a for failure to include in the subject line of each unsolicited e-mail "ADV:" as the first four characters[475].
	Risk of contravening the Broadcasting Services Act 1992 (Cth) (Regulation of Online Content-Schedule 5) in relation to prohibited online content.
	Risk of **contravening the Privacy Act (Cth)** to the extent that it applies to the private sector.
	Risk of **contravening the IIA Code of Practice for sending unsolicited e-mail which contains content unsuitable for underage recipients or for sending unsolicited e-mail that contains a link** or links **to content unsuitable for underage recipients but without including in the subject line "ADV: ADLT"** as the first eight characters and

[472] Clause 11.2 IIA Code of Practice.
[473] Clause 11.3 IIA Code of Practice.
[474] Clause 11.4 IIA Code of Practice.
[475] Clause 11.5 IIA Code of Practice.

without including in the body of the message that the e-mail is intended for adults only[476].

LEGAL RISKS ASSOCIATED WITH ESTABLISHING IDENTITY THAT ARISE BECAUSE INTERNET COMMERCE INVOLVES DISTANCE (NON-FACE-TO-FACE) COMMERCE

Risk of **liability for statutory non-compliance where the business transacts with minors or parties with whom it is illegal or unauthorised** to contract[477].

Risk that an **Internet transaction** is **repudiated** by a party **because** the party with whom the business conducted Internet commerce was **an imposter or an agent acting without ostensible, actual or implied authority** who **effected payment using a third party's credit card and identity** in order to incur liability on the third party's behalf.

Risk that **a transacting party** will **fraudulently deny contractual liability** on the basis that communications from the transacting party were not actually communications of the transacting party but were that of an imposter.

The risk that a business enters into **a contract that is invalid** and consequently unenforceable **because it was unauthorised** (i) where the party with whom the business is transacting is unauthorised to enter into the **transaction due to laws prohibiting** or otherwise regulating **the type of goods or services** offered by a business to that party **or**, (ii) where **the party** with whom the business is transacting is **purportedly acting for a principal but lacks actual, ostensible, or implied actual authority** to do so.

LEGAL RISKS THAT ARISE BECAUSE INTERNET COMMERCE CAN INVOLVE CROSS-JURISDICTIONAL COMMERCE

Risk of **liability for statutory non-compliance in a jurisdiction other than the jurisdiction from which the business operates** its Internet commerce business in respect of legislation specifically governing Internet commerce. For example, if the business's Internet activities involve advertising, and advertising is achieved by way of e-mail, and such advertising is distributed to recipients in the US, the business faces the risk of contravening US legislation prohibiting the use of unsolicited e-mail to sell products.

Risk of **liability to pay damages or to pay a penalty**, **where there is legislation** specifically governing Internet commerce, such as the anti-spam legislation in the US, mentioned above where such legislation **provides for affected parties or interested third parties to take action** to stop the business from contravening the legislation or to claim damages from the business as a consequence of the business contravening the legislation.

Risk of **liability to pay an Internet tax**, that is a tax that applies specifically to Internet transactions.

---

476 Clause 11.6 IIA Code of Practice.

477 See for example, Graham JH Smith et al, *Internet Law and Regulation*, A Specially Commissioned Report, FT Law & Tax, London, 1996, Ch 8, p 103, para 8.2.8; Central Computer and Telecommunications Agency, *Legal Issues and the Internet*, HMSO, London, 1996, Ch 8, p 104, para 8.2.

4.5 Legal risks examined in this thesis

After identifying the legal risks associated with Internet commerce the next steps are to undertake assessment of each legal risk and to evaluate and put forward risk management strategies. It is beyond the scope of this thesis to undertake these steps in relation to every legal risk that has been identified in this chapter. It is even too large a task to apply these steps to only those legal risks that have been identified as being particular to the conduct of Internet commerce.

Instead, the remaining steps of legal risk management will be applied to only certain legal risks, those legal risks that constitute contractual risks. Contractual risks were selected for a number of reasons. First, unlike some of the other legal risks identified, such as the risks associated with extra-jurisdictional enforcement, which, for example, was the subject of a Law Reform Commission Report[478], the contractual risks associated with Internet commerce have not been the subject of detailed research in the Australian context. It should, however, be noted that subsequent to the research for this thesis having been undertaken the Report of the Electronic Commerce Expert Group to the Attorney-General, *Electronic Commerce: Building the Legal Framework,* 31 March 1998, considered a number of contractual issues associated with Internet commerce, although the discussion focussed on considering the need for law reform and not on legal risk management. Secondly, there is a perception held by many, particularly those in the general community, but also amongst academic commentators that there is a great degree of contractual

uncertainty in relation to Internet commerce, and that such contractual risks constitute a legal impediment to Internet commerce[479]. To apply the remaining steps of risk

---

[478] Australian Law Reform Commission, *Legal risk in international transactions*, Australian Government Publishing Service, Canberra, 1996.

[479] See for example the following authors who have identified the following aspects of Internet commerce that give rise to contractual uncertainty. Much of the discussion, in this regard, has focussed on the role and function of paper-based transactions (such as, authenticating the existence of a contract, authenticating the terms on which the parties have agreed to transact, protecting against non-repudiation of a contract and identifying the parties to a contract), and the extent to which these features can be replicated in the context of Internet commerce, such as, through the use of encryption and digital signatures. See for example: Richard L Field, "The Electronic Future of Cash: Survey; 1996: Survey of the Year's Developments in Electronic Cash Law and the Law Affecting Electronic Banking in the United States, 46 *Am UL Rev* 967, April 1997, p 981; Raymond T Nimmer, Patricia Krauthouse, "Article: Electronic Commerce, New Paradigms in Information Law", 1995, 31 *Idaho Law Review*, 937. Additionally, the statutory requirement, derived from the Statute of Frauds 1677 (UK), that stipulates that certain contracts must be evidenced in writing and signed in order to be enforceable has been identified as a factor that brings about contractual uncertainty in the context of Internet commerce. For example, see John Robinson Thomas, "Note: Legal Responses to Commercial Transactions Employing Novel Communications Media", March 1992, 90 *Michigan Law Review* 1145 ; Raymond T Nimmer, Patricia Krauthouse, "Article: Electronic Commerce, New Paradigms in Information Law", 1995, 31 *Idaho Law Review*, 937; Marc E Szafran, "Note: A Neo-Institutional Paradigm for Contracts formed in Cyberspace: Judgment Day for the Statute of Frauds", 1996, 14 *Cardozo Arts & Entertainment Law Journal* 491 at pp 507-508; Central Computer and Telecommunications Agency, *Legal Issues and the Internet*, HMSO, London, 1996, Ch 8, pp 109-110, para 8.2.2. Some commentators have also suggested that contractual uncertainty exists in relation to when and how a contract transacted on the Internet is formed particularly in relation to when acceptance takes place. See for example: Henry H Perritt Jr, *Law and the Information Superhighway*, John Wiley & Sons, Inc, New York, 1996, Ch 9, p 382, sect 9.3; Graham JH Smith et al, *Internet Law and Regulation*, A Specially Commissioned Report, FT Law & Tax, London, 1996, Ch 8, p 100, para 8.2.4; Central Computer and Telecommunications Agency, *Legal Issues and the Internet*, HMSO, London, 1996, Ch 8, p 100, para 8.2.1; Paul Fasciano, "Note: Internet Electronic Mail: A last bastion for the mailbox rule", 25 *Hofstra Law Review*, 971 . Another area in which it has been suggested that contractual uncertainty exists, concerns the legal status of a business's marketing and promotional activities on the Internet, such as, whether such activity constitutes making an invitation to treat or making an "offer". See Joseph P Zammit and Felice B Galant, "Legal Considerations in Doing Business on the WWW", published in conjunction with the thirteenth annual Computer Law: Negotiating Complex Transactions Seminar on April 28 and 29 1997, http:/www.ljx.com/internet/zammit.html. Also, it has been suggested that the incorporation of standard terms by a business by referring to a hypertext link that sets out these terms, and requiring all customers to signify agreement with such terms by clicking on an icon or a button on which is enscribed the words "I agree" or "I accept" or "agreed" brings about contractual uncertainty. See Henry H Perritt Jr, *Law and the Information Superhighway*, John Wiley & Sons, Inc, New York, 1996, Ch 9, p 382, sect 9.3. Other aspects of Internet commerce that have been identified as bringing about contractual uncertainty include transacting with minors or parties with whom it is illegal or unauthorised to contract accepting on-line forms of payment, and transacting with a customer who purports to act on behalf of a principal or who falsely purports to be another party. See Henry H Perritt Jr, *Law and the Information Superhighway*, pp 384-385, sect 9.5;

management to contractual risks may be useful in ascertaining whether this is true in the Australian context. By applying the remaining steps of legal risk management to the contractual risks identified earlier in this thesis, those contractual risks for which there are appropriate risk management strategies can be eliminated leaving us with those contractual risks, which, by virtue of the fact that they cannot be managed, constitute a legal impediment to Internet commerce. Thirdly, it has been argued that the key legal challenges associated with Internet commerce relate to contractual risks such as the conclusion and enforcement of legal obligations[480] and, in particular, the risk that that an Internet transaction is unenforceable for failure to satisfy the Statute of Frauds writing requirement is "the principal perceived legal barrier to the development of electronic commerce on the Internet"[481]. The use of contract law in relation to Internet transactions is arguably more significant than in relation to offline transactions:

> …contract law has greater relevance in information transactions. The terms of the contract, especially those terms related to the cope of the granted rights, have greater importance in the information economy than in the goods economy[482].

It seems useful therefore to investigate in this thesis whether this is actually so. Accordingly, the following contractual risks will be examined in detail:

Henry H Perritt, Jr, "Legal and Technological Infrastructures for Electronic Payment Systems", 1996, 22 *Rutgers Computer & Technology Law Journal* 1, p 30.

480 Jonathon Kemberry, Senior Attorney at Arnheim Tite & Lewis, "Solving a legal conundrum on a world scale", 1998, http:.//www.global-ecom.net/inside.asp?insideid=55.

481 RJ Robertson, "Electronic Commerce on the Internet and the Statute of Frauds", *South Carolina Law Review*, Summer 1998, vol 48, p787 at p789.

482 Gail E Evans & Brian F Fitzgerald, "Information Transactions under UCC Article 2b: The Ascendancy of Freedom of Contract in the Digital Millenium?" *UNSW Law Journal*, Volume 21(2), http://www.law.unsw.edu.au/unswlj/ecommerce/evans.html at IA.

Table 58 LEGAL RISKS EXAMINED IN THIS THESIS
Risk that an Internet transaction is unenforceable for failure to satisfy the Statute of Frauds writing requirement;
Risk that that a business becomes contractually bound to terms unintentionally;
Risk that an acceptance communicated by a business does not give rise to a binding contract;
Risk that a customer is not contractually bound to standard terms purportedly incorporated by a business;
Risk that a business enters into a contract that is invalid because it was unauthorised;
Risk of incurring liability in relation to the acceptance of on-line payments.

4.6 Conclusion

In this chapter it was established that the first and second steps of the legal risk management framework developed in chapter 2 are effective when applied in practice. However, in relation to the first step (establishing the context), the research demonstrated the difficulties with applying the framework at a generic level, as it became clear that it was only possible to set out some general legal risk management objectives for business conducting Internet commerce.

In relation to the second step of the legal risk management framework it was established that several of the techniques advocated in risk management theory for identifying risk are equally useful for identifying legal risk. By applying these techniques a number of legal risks associated with Internet commerce were identified. It is also suggested that the range of risks identified was much wider than if just a

literature review were undertaken (which is traditionally the approach an academic writer would take to identifying legal risks to a business) or a review of the relevant case law or legislation (an approach that a legal adviser would typically take when advising on the legal risks facing a business).

The research further found that many of the legal risks identified are legal risks that equally face businesses conducting commerce off-line. The legal risks that differ from or are additional to the legal risks associated with off-line commerce can be attributed to three key characteristics of Internet commerce, that is: (i) Internet commerce operates in a digital and paperless environment, (ii) Internet commerce involves distance (non-face-to-face) commerce and (iii) Internet commerce can involve cross jurisdictional commerce.

Having established that the first and second step of the legal risk management framework can be applied in practice, the next chapter in this thesis considers the application in practice of the third (legal analysis step) and fourth step (evaluation and selection of legal risk management strategies).

CHAPTER 5 CYBER - DEALING II: RISK ANALYSIS AND RISK MANAGEMENT STRATEGIES

5.1 Introduction

In this chapter, the legal risk management framework developed in chapter 2 is further evaluated by applying the 3rd (risk analysis) and 4th (evaluation and selection of risk management strategies) steps to the legal risks associated with Internet commerce.

It is in applying the third and fourth steps to the legal risks associated with Internet commerce that the limitations of the legal risk management framework become apparent. For example, the legal risks selected for risk analysis are analysed *qualitatively* rather than quantitatively, there being insufficient data collected and made publicly available at present to undertake a quantitative analysis of legal risk. Also, the use of the legal risk management framework at a generic level proves to be problematic. In particular, it proves difficult to select descriptors for a scale to categorise the *consequence* of a legal risk in the absence of a specific business to refer to. In addition, only *qualitative* techniques can be used for evaluating and selecting appropriate legal risk management strategies as the use of quantitative techniques require specific reference to a business.

Nevertheless the research in this chapter establishes that the legal risk management framework developed in chapter 2 is effective when applied in practice. By analysing the six selected contractual risks associated with Internet commerce by reference to their consequence and likelihood it was possible to categorise each risk according to their level of risk. This provided an authoritative basis for prioritising

the six contractual risks, a useful outcome not achievable in respect of conventional legal advice, which typically lacks a methodology that enables legal risks to be evaluated consistently. Interestingly, the most serious of the contractual risks analysed here are the risk that a customer is not contractually bound to standard terms purportedly incorporate by a business and the risk that a business enters into a contract that is invalid because it was unauthorised.

In order not to break the flow of discussion, third and fourth steps of the legal risk management framework are discussed together in relation to each selected legal risk. Further, to avoid repetition, and again to facilitate the flow of discussion, a detailed examination of one legal risk management strategy is provided separately, namely, the use of encryption and digital signatures.

5.2 Legal risks *analysed* qualitatively

As noted in chapter 2, it will be more common for a given legal risk to be analysed qualitatively rather than quantitatively. Not surprisingly therefore the legal risks discussed in this chapter will be analysed *qualitatively*, as there is simply not enough data available that would enable a quantitative analysis to be undertaken. The analysis that follows involves undertaking a detailed examination of the factual circumstances and applicable law that gives rise to each of the legal risks identified in the chapter 2.

The approach taken here follows the approach set out in Australian Standard *AS/NZS 4360 - 1999, Risk Management* for undertaking qualitative risk analysis. That is, three qualitative scales will be used to analyse the selected legal risks: (a) a scale

for classifying the consequences of a risk eventuating; (b) a scale for classifying the likelihood of a risk eventuating and (c) a scale for classifying the overall level of risk.

Whilst it is relatively simple to devise a scale for use in this chapter in relation to (a) and (c), devising a scale for (b), that is, a scale that classifies qualitatively the *consequence* of risk eventuating, is problematic. The descriptors commonly used for devising a scale for (b), such as the model scales set out in *AS/NZS 4360 - 1999, Risk Management* classify the consequence of a risk eventuating by reference to a risk's effect on the viability of a business. For example, a risk classified as "negligible" is a risk that, if it eventuated, would have no financial effect on the business. It is not feasible to use descriptors in such a way when using risk management to provide a generic qualitative analysis, such as in this chapter, rather than a risk analysis for a specific business. Whether the consequence of a given risk affects the viability of a business depends on circumstances particular to the business such as its size, the number of investments it holds and its cash flow. It is therefore not possible to use descriptors that refer to the viability of a business when undertaking a generic analysis.

It is tempting to conclude therefore that there is little value in using risk management to analyse a legal risk at a generic level. It is argued here that the use of risk management to analyse legal risk at a generic level is as useful as, if not more useful than, the conventional manner in which lawyers provide legal advice on a given legal risk. Why is this so? The use of the risk management process in the context of legal risk requires legal risks to be analysed by reference to a scale of

descriptors. This results in the legal risks being analysed consistently. In turn, a consistent approach to analysing legal risk allows legal risks to be prioritised according to a systematic process rather than according to a more subjective "gut feel" or intuition, although admittedly some aspects of the risk management process still involve these elements[483]. Whilst legal advice provided in the conventional manner can follow a consistent approach, the risk management process *ensures* that legal risks (often quite disparate) are analysed consistently and systematically. Whether the provision of legal advice in the conventional manner results in a consistent approach to analysing legal risks requires a legal adviser to consciously consider whether he or she has employed a consistent approach when evaluating each legal risk. The risk management process through its simple use of scales automatically ensures that the approach taken to analyse each legal risk is consistent.

Returning to the issue of which set of descriptors to use in relation to the legal risks discussed in this chapter, it is proposed to use a set of descriptors that can best be described as relative descriptors, that is they provide a means by which the consequence of a given legal risk can be compared to the consequence of another legal risk. In other words, the descriptors can still be used to prioritise legal risks, but clearly these descriptors are not as useful to a particular business as the use of descriptors that are tailored to the business's financial circumstances.

The qualitative scale used for classifying the *consequence* of a legal risk in this chapter is as follows:

---

[483] The role of "gut feel" and intuition in relation to legal risk management is discussed at 5.12.3.

Table 59 SCALE FOR CLASSIFYING CONSEQUENCE OR IMPACT OF A LEGAL RISK EVENTUATING[484]	
Descriptor	Description
Extreme	The consequences would threaten the survival of not only the business's Internet commerce activities, but also the business, possibly causing major problems for clients, the administration of the business's Internet commerce activities or a large part of the public sector.
Very high	The consequences would threaten the survival or continued effective function of the business's Internet commerce activities or require the intervention of top level management.
Medium	The consequences would not threaten the business's Internet commerce activities but administration of the business's Internet commerce activities could be subject to significant review or changed ways of operating.
Low	The consequences would threaten the efficiency or effectiveness of the business's Internet commerce activities but can be dealt with internally.
Negligible	The consequences are of negligible consequence to the business.

The qualitative scale used for classifying the *likelihood* of a legal risk in this chapter is as follows:

Table 60 SCALE USED FOR CLASSIFYING LIKELIHOOD OR FREQUENCY OF LEGAL RISK[485]	
Descriptor	Description
Almost certain	The risk will eventuate in most circumstances.

[484] Adapted from Standards Australia/Standards New Zealand Joint Technical Committee on Risk Management, "A Basic Introduction to Managing Risk using the Australian and New Zealand Risk Management Standard - AS/NZS 4360: 1999", Master Draft as at 4/1/99 p. 25.

[485] Adapted from appendix D, *AS/NZS 4360- 1995, Risk Management*.

Likely	The risk will probably eventuate in most circumstances.
Moderate	The risk should eventuate at some time.
Unlikely	The risk could eventuate at some time.
Rare	The risk may eventuate only in exceptional circumstances.

Finally, the scale used for classifying the *level* of risk will be:

Table 61 SCALE FOR LEVEL OF RISK[486]

Descriptor	Description
Extreme risk	Must be managed by senior management with a detailed plan.
Severe risk	Detailed research and management planning required at senior level.
Moderate risk	Manage by specific monitoring or response procedures.
Low risk	Manage by routine procedures.

Combining the three scales used for classifying *consequence*, *likelihood* and *level* of risk results in the following matrix:

Table 62 MATRIX DEPICTING THE SCALES USED IN THIS THESIS

	CONSEQUENCES OF RISK EVENTUATING				
LIKELIHOOD OF RISK EVENTUATING	**Extreme**	**Very high**	**Medium**	**Low**	**Negligible**
Almost certain	Extreme risk	Extreme risk	Extreme risk	Severe risk	Severe risk
Likely	Extreme risk	Extreme risk	Severe risk	Severe risk	Moderate risk

[486] Adapted from Standards Australia/Standards New Zealand Joint Technical Committee on Risk Management, p 26.

Moderate	Extreme risk	Extreme risk	Severe risk	Moderate risk	Low risk
Unlikely	Extreme risk	Severe risk	Moderate risk	Low risk	Low risk
Rare	Severe risk	Severe risk	Moderate risk	Low risk	Low risk

The overall *level* of risk for each legal risk will be determined by reference to this matrix.

5.3 *Evaluation* and *selection* of risk management strategies using qualitative methods

In relation to the evaluation and selection of risk management strategies step (Step 4) of the risk management process, a number of risk management strategies will be put forward in relation to each legal risk. These risk management strategies will then be evaluated qualitatively. This is because it is only possible to use quantitative measurement techniques when there is a specific business that can be referred to. In any case, in relation to the risks associated with Internet commerce it is more likely that qualitative techniques will be used to evaluate risk management strategies. For example, an E-business Risk Management Professional states that he uses qualitative techniques when evaluating and selecting strategies for managing the risks associated with Internet commerce[487]. Thus, the risk management strategies put forward here will be evaluated and selected by reference to the following qualitative approaches:

---

[487] Response dated 20 January 2000 to a self-completion questionnaire enquiring how the participant uses management methodology in the context of legal risk. Participants' names have not been disclosed to honour a request of some participants to remain anonymous. All responses are available on file.

- Considering the effect that each strategy may have on a business's ability to fulfill its objectives, such objectives should include the objectives referred to in 2.4.1 at p37: (i) to reduce the liability to which the business is exposed; (ii) to achieve compliance with legislative and other regulatory frameworks; and (iii) to protect the business's legal rights and interests;
- Referring to the *degree* of *consequence* and *likelihood* of risk, as discussed at 2.4.4.4.1 at p102 in order to determine whether a business should retain or transfer a given legal risk;
- Considering whether the risk management strategy accords with the general principle that a business should not retain or accept a risk over which it has no control as discussed at 2.4.4.4.4 at p107.

5.4 Risk that an Internet transaction is unenforceable for failure to satisfy the Statute of Frauds writing requirement ("Statute of Frauds risk")

5.4.1 ANALYSIS OF THE CONSEQUENCE OF THE RISK EVENTUATING

The *consequence* of the Statute of Frauds risk, as concluded in the discussion that follows, is depicted in Figure 8:

Figure 8 EVALUATION OF THE CONSEQUENCE

Risk that an Internet transaction is unenforceable for failure to satisfy the writing requirement	**Consequence:** ***Low*** **(based on the assumption discussed below)**

The consequence of the Statute of Frauds risk is that a business cannot enforce an Internet transaction which is subject to, but does not comply with, the Statute of Frauds writing requirement.

What impact this will have on a business depends on whether customers usually pay for the goods or services upfront (obviating the need for enforcement), the value of the Internet transaction that is unenforceable and the extent to which the business incurred associated costs in the course of the transaction (such as shipping costs). This makes it difficult to provide a meaningful generic estimate of the consequence of this risk and demonstrates that attempting to use risk management methodology at a generic level rather than by reference to a specific business is problematic. Clearly, the higher the value of the Internet transaction and the more the business has expended on associated costs the greater the consequence will be if this risk eventuates. Thus, an assessment of this legal risk can only be made if certain assumptions about the value of the Internet transactions conducted by a business can be made. The assumption made here is that businesses conducting Internet commerce are able to bear the loss caused by a *single* Internet transaction[488] proving to be unenforceable (that is, the value of the transaction that was unenforceable). This arguably is a reasonable assumption to make- few businesses would transact Internet commerce in goods or services whose value was so great that the business could not

---

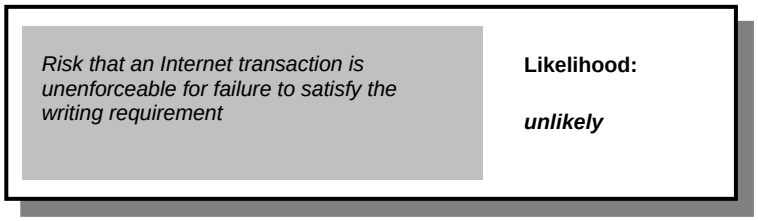
[488] Whilst it is tempting to argue that it is necessary to consider the scenario where hundreds and thousands of lower value Internet transactions are carried out risk management methodology dictates that this factor is taken into account when assessing the *likelihood* of this legal risk. It is therefore relevant here to consider the consequence in terms of the effect of a single Internet transaction proving to be unenforceable.

bear the loss of the value of a single Internet transaction. Assuming that a business could bear the loss associated with being unable to enforce a particular Internet transaction, the consequence of the risk eventuating is assessed as being *low*. That is, the consequence would threaten the efficiency or effectiveness of the business's Internet commerce activities but can be dealt with internally. Where such assumption is incorrect the assessment of the consequence of this legal risk may be different.

5.4.2 ANALYSIS OF THE LIKELIHOOD OF THE RISK EVENTUATING

The *likelihood* of this legal risk, as concluded in the discussion that follows, is depicted in Figure 9:

Figure 9 EVALUATION OF THE LIKELIHOOD



A number of factors will affect the likelihood of this legal risk eventuating. They are as follows:

- Whether Internet transactions are governed by the requirement that a contract, in order to be enforceable, must be evidenced in writing and signed by the party against whom a contract is sought to be enforced **(**the **"Statute of Frauds writing requirement")** (this requirement is explained in more detail below);

- Whether Internet transactions could satisfy the Statute of Frauds writing requirement;
- The extent to which the UN Convention on Contracts for the International Sale of Goods 1980 applies.

These factors require detailed examination in order to provide an overall analysis of the likelihood of risk.

5.4.2.1 Whether Internet transactions are governed by the Statute of Frauds writing requirement"

Not all Internet transactions are subject to the Statute of Frauds writing requirement. In fact, the contracts typically transacted on the Internet are not likely to fall within the categories of contract that are subject to the Statute of Frauds writing requirement. A contract need only satisfy the Statute of Frauds writing requirement where required to by legislation or where agreed to by the transacting parties. In Australia, the legislation that imposes the Statute of Frauds writing requirement in the contractual context is broadly derived from the Statute of Frauds 1677 (UK) (in particular, sections 4 and 17). Whether a particular contract is required by legislation to satisfy the Statute of Frauds writing requirement varies from jurisdiction to jurisdiction. For this reason, it is difficult to make general observations about the types of contracts to which the Statute of Frauds writing requirement applies, except to comment that the following types of contracts are, in most jurisdictions, subject to the Statute of Frauds writing requirement: (i) contracts that constitute special promises by executors, (ii) contracts of guarantee, (iii) contracts made in consideration of marriage, (iv) contracts for the sale of land or an interest in land, and

(v) contracts that are not to be performed within a year[489]. In addition, assignments of copyright and patents, hire purchase contracts, bills of exchange, promissory notes and contracts of marine insurance are subject to a prescribed Statute of Frauds writing requirement in order to be legally effective[490].

In addition, in the Northern Territory, Western Australia and Tasmania only, contracts that constitute a sale of goods *may*, if they exceed the stipulated amount, be subject to the Statute of Frauds writing requirement[491]. The Statute of Frauds writing requirement is imposed in these jurisdictions by their respective Sales of Goods Acts. It is important to note that evidencing a contract in writing that is signed is only one of several ways in which the relevant Sale of Goods provision can be satisfied. Thus, in the Northern Territory, Tasmania and Western Australia, the relevant provision of each respective Sale of Goods Act provides that the provision will also be satisfied by *acceptance and receipt of the goods*, or *the giving of something in earnest to bind the contract*, or by *part payment*[492]. The application of the Statute of Frauds writing requirement in relation to the sales of goods is further limited in that it applies only to sales of goods that exceed the following values: Tasmania $20, Western Australia $20 and Northern Territory $50[493].

---

489 JG Starke QC, NC Seddon, MP Ellinghaus, *Cheshire and Fifoot's Law of Contract*, 6th Australian Edition, Butterworths, Sydney 1992, Ch 5, pp 233-250, paras 508-533.

490 *Electronic Commerce: Building the Legal Framework*, Report of the Electronic Commerce Expert Group to the Attorney-General, 31 March 1998, http://law.gov.au/aghome/advisory/eceg/ecegreport.html, para 2.6.18.

491 The writing requirement for contracts for the sale of goods has been abolished in Queensland, South Australia, Australian Capital Territory, Victoria and New South Wales.

492 Sale of Goods Act 1895 (Tas), s 9, Sale of Goods Act 1895 (WA), s 4(1) and Sale of Goods Act 1972 (NT), s 9.

493 Sale of Goods Act 1895 (Tas), s 9, Sale of Goods Act 1895 (WA), s 4(1) and Sale of Goods Act

In the context of Internet commerce it is characteristic for a customer to pay upfront and for delivery to be effected soon after. It is submitted that these fall within one of the *alternative* means for satisfying the relevant Sale of Goods provisions, that is, the *acceptance and receipt of the goods*. "Acceptance" is defined in the relevant Sale of Goods provisions as 'any act in relation to the goods which recognises a pre-existing contract of sale, whether there be acceptance in performance of the contract or not'.[494] This definition means that 'any conduct on the part of the buyer which recognises that a prior contract has been made' will constitute an act of "acceptance"[495]. The upfront payment by a customer transacting on the Internet is clearly an act that recognises that a prior contract has been made, which in turn will constitute "acceptance" for the purposes of the relevant provisions. "Receipt" is taken to mean 'the actual delivery of the goods by the seller to the buyer or his or her agent' [496]. The delivery by a business of goods to a customer, pursuant to a transaction conducted on the Internet with the customer, will fall within the meaning of "receipt". Therefore, most Internet transactions that are subject to a Sales of Goods Act provision which imposes the Statute of Frauds writing requirement will not need to actually comply with the writing requirement because they can satisfy one of the alternative means for satisfying the relevant provision.

1972 (NT), s 9.

494 Sale of Goods Act 1895 (Tas), s 9(3), Sale of Goods Act 1895 (WA), s 4(3) and Sale of Goods Act 1972 (NT), s 9(3).

495 JG Starke QC, NC Seddon, MP Ellinghaus, *Cheshire and Fifoot's Law of Contract*, 6th Australian Edition, Butterworths, Sydney 1992, Ch 5, p 283, para 582.

496 JG Starke QC, NC Seddon, MP Ellinghaus, para 584.

In conclusion, the instances in which a business's Internet transactions are governed by the Statute of Frauds writing requirement and cannot be satisfied by reliance on the alternative means for satisfying the relevant Sale of Goods provisions are limited.

5.4.2.2 Whether Internet transactions could satisfy the Statute of Frauds writing requirement

It is important to note that in practice it is unlikely that businesses that engage in Internet transactions which are subject to the Statute of Frauds writing requirement will be in a position where they actually need to enforce a contract. As noted earlier, the usual way in which businesses conduct Internet commerce is to authenticate payment before delivery of the goods or services purchased by a customer. Because Internet commerce typically takes place in this way, the circumstances in which a business will need to enforce an Internet transaction will be limited. There may, however, be some situations, which are more likely to arise in relation to business-to-business Internet commerce, where a business may be prepared to fulfil its obligations before the contractual obligations of the other party has been fulfilled. In such circumstances, a business may find itself in a situation where it desires to enforce an Internet transaction, because the party with whom it has transacted has failed to fulfil its contractual obligations. The following discussion examines whether the Statute of Frauds writing requirement can be satisfied in relation to Internet commerce.

With a few exceptions, that are not, in general, relevant to Internet commerce[497], the Statute of Frauds writing requirement is satisfied where there is: (i) a *memorandum* upon which is *written* the material terms of the contract agreed to by the transacting parties (that is, it is not necessary that the contract itself be in writing) and (ii) the memorandum bears the signature of the party against whom the contract is sought to be enforced, commonly referred to as the party to be charged (from a business's perspective the memorandum must be signed by the customer with whom it contracts). Each of these elements will be considered separately. It is necessary, however to first consider briefly how messages, data and information are transmitted through the Internet.

5.4.2.2.1 How messages, data and information are transmitted through the Internet

In this thesis the term **"Internet communication"** is used broadly to refer to all messages, data or information that can be transmitted through the Internet. An Internet communication therefore includes e-mail messages, or data, or a message transmitted by way of a browser (such as when data inputted into a form on a business's web page is transmitted to the business by a customer by selecting the "send" button or icon).

It is also appropriate at this point to provide an elementary description of how an Internet communication is transmitted.

---

[497] For example, in relation to contracts for the sale of land or an interest in land, the writing requirement is only satisfied if the contract itself is in writing in South Australia, Western Australia, Victoria, Queensland and Tasmania. All other jurisdictions allow such contracts to be evidenced in writing. Such types of contracts are not presently conducted on the Internet.

Basically, there are several computer protocols known as the Internet Protocol Suite[498] that govern the interactions that take place that result in a computer connected to the Internet being able to transmit and receive Internet communications to or from another computer connected to the Internet. The most important protocol is the network protocol called the Transmission control protocol/Internet protocol (TCP/IP) which specifies the rules by which Internet communications are transmitted through the Internet, the routes which Internet communications will take to get to their destinations and the rules that govern the naming system for computers connected to the Internet[499]. Each time an Internet communication is transmitted through the Internet, the communication is broken down into smaller data packets called datagrams, each of which contain header information[500] that consists of information concerning the sender's computer, the recipient's computer and other information which enables the entire communication to be "reconstituted".

The Internet communication, now in the form of several packets of data, is then transmitted to the customer's server (that is the server of the organisation providing Internet access to the customer eg an Internet Service Provider or an internal server). The server directs the packets to the Internet through a gateway, a computer (which

---

498 "Internet Protocols and Software Tools", http://www.hcc.hawaii.edu/iss/unix/module2.html.

499 "WWWIntro- WWW Acronyms", 1996, http://www.slis.ua.edu/wwwintro/www.htm.

500 A header consists of various information including the source IP number (which identifies the computer that sent the communication), the destination IP number (which identifies the computer to which the communication is to be sent), the version of IP protocol used to create the datagram, the type of service required for the datagram, the length of the datagram and the datagram's identification number.

can be general purpose or dedicated) [501] that connects a network with one or more other networks[502]. The gateway's router identifies the destination of the packets and directs the packets to the intended recipient's computer. A datagram may pass through a series of independent networks connected by gateways whose routers choose which route the datagram should take depending on factors such as which connection is "closer" and the volume of traffic passing through a particular connection. Each datagram comprising an Internet communication may in fact take a different route to the others.

When the Internet communication reaches the server of the intended recipient's computer (once again this may be an internal server or an Internet Service Provider) the Internet communication is "reconstituted" by reassembling the data packets. The recipient's server then transmits the Internet communication to the recipient's computer, or in the case of e-mail directs the e-mail message to the recipient's account on the server to which the recipient's computer gains access when the recipient's e-mail application checks new mail.

Another layer of the TCP/IP protocol that "runs on top" of TCP/IP is what is often termed the service or application protocols which are used to enable the various Internet services (for example, e-mail, World Wide Web, File Transfer Protocol (FTP), netnews) available. Thus, computers use the Simple Mail Transport Protocol

---

501 Alan Silverstein, "Under the Hood of the World Wide Web", Paradesa Media, 1996-1997, http://www.learnthenet.com/english/html/70alan.htm.

502 Charles L Hedrick, "Introduction to the Internet Protocols- Routing", Rutger's University, 1987, http://oac3.hsc.uth.tmc.edu/staff/snewton/tcp-tutorial/sec6.html.

in relation to the transmission, receipt and display of e-mail[503], the network news transfer protocol in relation to transmission, receipt and display of netnews[504], and the hyper text transfer protocol (HTTP) in relation to the transmission, receipt and display of web pages. Most browsers can handle several protocols, providing access to various Internet services using the same application. For example, both Netscape and Internet Explorer enable users to send e-mail, transfer and display files, read and post net news and display web pages.

5.4.2.2.2 The first element of the Statute of Frauds writing requirement

Whether the first element of the Statute of Frauds writing requirement, that is, the existence of a memorandum upon which is written the material terms of the contract agreed to by the transacting parties **("memorandum in writing")**, can be satisfied in the context of Internet commerce requires an examination of the relevant case law and legislation.

No Australian case has directly considered whether Internet communications exchanged between a business whether by e-mail (eg. the e-mail of terms on which a business agrees to contract and a reply e-mail by a customer accepting those terms) or on the web (eg. the display on a business's web site of the terms on which the business agrees to transact and the selection by a customer of text, a button or an icon, which transmits the customer's acceptance of those terms) could constitute a memorandum for the purposes of the Statute of Frauds writing requirement.

---

503 Silverstein, http://www.learnthenet.com/english/html/70alan.htm.
504 Silverstein, "http://www.learnthenet.com/english/html/70alan.htm.

To determine whether an Internet transaction could satisfy the memorandum in writing element it is necessary to consider the following issues:

- Whether an Internet communication can constitute a memorandum;
- Whether the meaning of "writing" includes words that appear in "electronic form";
- Whether a memorandum is valid if it is comprised partially of text or selections that were selected by a customer from the business's web page and partially of text or formatting that is reconstituted by the business's Internet commerce software application after the contract was concluded;
- Whether a memorandum can be comprised of a grouping of Internet communications exchanged between a business and a customer.

Each of these issues is discussed in turn.

5.4.2.2.3 Can an Internet communication constitute a memorandum for the purposes of satisfying the Statute of Frauds writing requirement?

Generally, the courts have accepted a wide range of documents as constituting a "memorandum" for the purposes of the Statute of Frauds writing requirement. Thus, documents such as telegrams[505] and even a cheque in combination with a receipt[506] have been held to constitute a memorandum for the purposes of satisfying the Statute of Frauds writing requirement. However, the underlying assumption has been that the document upon which the material terms of a contract appears is in paper form. If this interpretation is correct, Internet communications exchanged between a business and

---

505 *Goodwin v Francis* (1870) LR 5 CP 295.

a customer could only satisfy the memorandum requirement if the business electronically stored all Internet communications between it and its customers that evidenced the terms on which the business has transacted and the business then printed out these communications in the event of a dispute. Assuming that the Internet communications could be linked to comprise a single memorandum (this possibility is discussed at 5.4.2.2.6 at p266), such an approach would satisfy the memorandum requirement, even though the printouts constituting the memorandum came into existence after the contract was formed, provided that the printed-out Internet communications came into existence before action is taken to enforce the contract[507].

There is, however, support for an interpretation of "memorandum" that includes a document in electronic form. Such support can be found in the Interpretation Acts of each jurisdiction[508]. It is clear that each jurisdiction specifies that, when interpreting

---

506 *Hawkins v Price* [1947] Ch 645.

507 See *Popiw v. Popiw* [1959] VR 197.

508 **Section 25 of the Acts Interpretation Act 1901 (Cth)** provides:
25. In any Act, unless the contrary intention appears:
"document" includes:
(a) any paper or other material on which there is writing;
(b) any paper or other material on which there are marks, figures, symbols or perforations having a meaning for persons qualified to interpret them; and
(c) any article or material from which sounds, images or writings are capable of being reproduced with or without the aid of any other article or device.
Section 21 of the Interpretation Act 1987 (NSW) provides:
document means any record of information and includes:
(a) anything on which there is writing, or
(b) anything on which there are marks, figures, symbols or perforations having a meaning for persons qualified to interpret them, or
(c) anything from which sounds, images or writings can be reproduced with or without the aid of anything else, or
(d) a map, plan, drawing or photograph.

Section 17 of the Interpretation Act 1967 (ACT) provides that in an Act, unless the contrary intention appears- "document" includes:

(a) any paper or other material on which there is writing:
(b) any paper or other material on which there are marks, figures, symbols or perforations having a meaning for persons qualified to interpret them; and
(c) any article or material from which sounds, images or writings are capable of being reproduced with or without the aid of any other article or device.

Section 38 of the Interpretation of Legislation Act 1984 (Vic) provides:

"Document" includes, in addition to a document in writing-

(a) any book, map, plan, graph or drawing;
(b) any photograph;
(c) any label, marking or other writing which identifies or describes anything of which it forms part, or to which it is attached by any means whatsoever;
(d) any disc, tape, sound track or other device in which sounds or other data (not being visual images) are embodied so as to be capable (with or without the aid of some other equipment) of being reproduced therefrom;
(e) any film (including microfilm), negative, tape or other device in which one or more visual images are embodied so as to be capable (with or without the aid of some other equipment) of being reproduced therefrom; and
(f) anything whatsoever on which is marked any words, figures, letters or symbols which are capable of carrying a definite meaning to persons conversant with them.

Section 5 of the Interpretation Act 1984 (WA) provides:

"document" includes any publication and any matter written, expressed or described upon any substance by means of letters, figures, or marks, or by more than one of these means which is intended to be used or may be used for the purpose of recording that matter.

Section 24(bb) of the Acts Interpretation Act 1931 (Tas) provides:

references to a document shall be construed as including references to-

(i) any paper or other material on which there is printing or writing or on which there are marks, symbols, or perforations having a meaning for persons qualified to interpret them; and
(ii) a disc, tape or other article from which sounds, images, writing, or messages are capable of being reproduced.

Section 36 of the Acts Interpretation Act 1954 (Qld) provides:

"document" includes-

(a) any paper or other material on which there is writing; and
(b) any paper or other material on which there are marks, figures, symbols or perforations having a meaning for a person qualified to interpret them; and
(c) any disc, tape or other article or any material from which sounds, images, writings or messages are capable of being produced or reproduced (with or without the aid of another article or device).

In the Northern Territory, **section 19 of the Interpretation Act (NT)**, provides that the word "document" includes:

(a) any of, or part of any of, the following things:
  (i) paper or other material on which there is writing;
  (ii) a map, plan, drawing or photograph;
  (iii) paper or other material on which there are marks, figures, symbols or perforations having a meaning for persons qualified to interpret them;
  (iv) an article or any material from which sounds, images or writings are capable of being reproduced with or without the aid of another article or device;
  (v) an article on which information has been stored or recorded, either mechanically or electronically;

legislation that refers to a "document", the meaning ascribed to the word "document" includes a document in electronic form. Although the Statute of Frauds writing requirement uses the term "memorandum" it is submitted that the word "document" can be used interchangeably with the word "memorandum" in this context. The courts have consistently assumed that a "memorandum" is a form of "document" and so too have the text writers[509]. Therefore, it is legitimate for the courts to look at the meaning ascribed to the word "document" in the relevant Interpretation Act to determine whether a document in electronic form constitutes a memorandum for the purposes of the Statute of Frauds writing requirement. On this basis it is concluded that a document in electronic form can constitute a memorandum for the purposes of the Statute of Frauds writing requirement.

It should further be noted that the Report of the Electronic Commerce Expert Group **("Electronic Commerce Expert Group Report")** recommended that a provision following Article 5 of the UNCITRAL Model Law on Electronic Commerce should be legislatively implemented in Australia[510]. Article 5 of the Model Law provides that information should not be denied legal effect solely on the grounds that it is in electronic form[511].

(vi) any other record or information;
(b) a copy, reproduction or duplicate of such a thing; and
(c) a part of such a copy, reproduction or duplicate.

509 See for example, DW Greig and JLR Davis, *The Law of Contract*, The Law Book Company Ltd, 1987, Sydney, Ch 12, p 696-697 and JG Starke QC, NC Seddon, MP Ellinghaus, *Cheshire & Fifoot's Law of Contract*, 6th Australian Edition, Butterworths, Sydney 1992, Ch 5 paras 534-538.

510 *Electronic Commerce: Building the Legal Framework.* See Recommendation 5.

511 Article 5 of the UNCITRAL Model Law on Electronic Commerce provides:
Article 5 Legal Recognition of data messages

The Commonwealth Electronic Transactions Act 1999 (Cth) incorporates this recommendation in section 8[512]. This legislative provision supports the assertion that a document in electronic form can constitute a memorandum for the purposes of the Statute of Frauds writing requirement, as the effect of Section 8 is to provide legal recognition of writing that appears in electronic form.

Similarly, clause 6(2) of the Victorian Electronic Commerce Framework Bill (Vic) has provisions that would support an interpretation that a document in electronic form can constitute a memorandum for the purposes of the Statute of Frauds writing requirement[513]. If it is accepted that writing on paper, setting out the material terms of the contract between the transacting parties, constitutes a memorandum, then it follows that, the effect of clause 6(2) is that if the writing is in electronic form, it too will constitute a memorandum.

In conclusion, in relation to Internet transactions governed by the Electronic Transactions Act 1999 (Cth) the requirement that the material terms of the contract be

---

Information shall not be denied legal effect, validity or enforceability solely on the grounds that it is in the form of a data message.

[512] Section 8 of the Commonwealth Electronic Transactions Act 1999 (Cth) provides:

8 Validity of electronic transactions

(1) For the purposes of a law of the Commonwealth, a transaction is not invalid merely because it took place wholly or partly by means of one or more electronic communications.

(2) The general rule in subsection (1) does not apply in relation to the validity of a transaction to the extent to which another, more specific provision of this Part deals with the validity of the transaction.

Exemptions

(3) The regulations may provide that subsection (1) does not apply to a specified transaction.

(4) The regulations may provide that subsection (1) does not apply to a specified law of the Commonwealth.

evidenced in a memorandum will be satisfied, even though what constitutes a memorandum is in fact in electronic form . Similarly, if the Electronic Commerce Framework Bill (Vic) is passed, then, in relation to transactions that are governed by Victorian law, and subject to the Statute of Frauds writing requirement, a business conducting Internet commerce could, it is argued, satisfy the requirement that the material terms of the contract be evidenced in a memorandum, even though what constitutes a memorandum is in fact in electronic form. The common law, in any case, does provide some support for the view that a document in electronic form can constitute a memorandum for the purposes of the Statute of Frauds writing requirement.

5.4.2.2.4 The meaning of "writing"

To determine whether a document in electronic form constitutes a memorandum in *writing* it is relevant to examine the meaning ascribed to the word "writing" in the Interpretation Acts. In the federal jurisdiction the word "writing" is defined in section 25 of the Acts Interpretation Act 1901 (Cth) as including 'any mode of representing or reproducing words, figures, drawings or symbols in a visible form'. In the Australian Capital Territory, the word "writing" is defined in section 17 of the Interpretation Act 1967 (ACT) as including 'any mode of representing or reproducing words, figures, drawings or symbols in a visible form'. In New South Wales, the

---

513 Clause 6(2) of the Victorian Electronic Commerce Framework Bill (Vic) provides:

…

(2) The effect of writing in electronic form is the same for the purposes of any law as that of writing in paper form if the electronic form is such as to permit retention of the writing for subsequent reference.

word “writing” is defined in section 21 of the Interpretation Act 1987 as including ‘printing, photography, photocopying, lithography, typewriting and any other mode of presenting or reproducing words in a visible form’. In South Australia, section 4 of the Acts Interpretation Act 1915 defines “writing” to include ‘any visible form in which words may be reproduced or presented’.

In Western Australia, section 5 of the Interpretation Act 1984 (WA) provides that ‘“writing” and expressions referring to writing include printing, photography, photocopying, lithography, typewriting and any other modes of representing or reproducing words in visible form.’ Section 36 of the Queensland Acts Interpretation Act 1954 (Qld) provides that writing ‘includes any mode of representing or reproducing words in a visible form’. In Tasmania, section 24(b) of the Acts Interpretation Act 1931 (Tas) provides that in any Act, ‘expressions referring to writing shall be construed as including references to any mode of representing or reproducing words, figures, or symbols in a visible form’.

In the Northern Territory, section 26 of the Interpretation Act (NT) provides that ‘In an Act, words, expressions and provisions referring to writing shall be construed as including references to any mode of representing or reproducing words, figures or symbols in a visible form whether or not an optical, electronic, mechanical or other means or process must be used before they can be perceived.’ Finally, in Victoria, section 38 of the Interpretation of Legislation Act 1984 (Vic) provides that “writing” includes ‘all modes of representing or reproducing words, figures or symbols in a visible form and expressions referring to writing shall be construed accordingly’.

Each of these definitions of the word "writing" indicate clearly that, where a document is required under legislation to be in writing, a document recorded in electronic form will satisfy this requirement. Furthermore, in respect of Commonwealth law, section 9 of the Electronic Transactions Act 1999 (Cth)[514]

---

[514] Section 9 of the Electronic Transactions Act 1999 (Cth) provides:

9 Writing Requirement to give information in writing

(1) If, under a law of the Commonwealth, a person is required to give information in writing, that requirement is taken to have been met if the person gives the information by means of an electronic communication, where:

(a) in all cases—at the time the information was given, it was reasonable to expect that the information would be readily accessible so as to be useable for subsequent reference; and

(b) if the information is required to be given to a Commonwealth entity, or to a person on behalf of a Commonwealth entity, and the entity requires that the information be given, in accordance with particular software requirements, by means of a particular kind of electronic communication—that last-mentioned requirement has been met; and

(c) if the information is required to be given to a Commonwealth entity, or to a person on behalf of a Commonwealth entity, and the entity requires that particular action be taken by way of verifying the receipt of the information—that last-mentioned requirement has been met.

Permission to give information in writing

(2) If, under a law of the Commonwealth, a person is permitted to give information in writing, the person may give the information by means of an electronic communication, where:

(a) in all cases—at the time the information was given, it was reasonable to expect that the information would be readily accessible so as to be useable for subsequent reference; and

(b) if the information is permitted to be given to a Commonwealth entity, or to a person on behalf of a Commonwealth entity, and the entity requires that the information be given, in accordance with particular software requirements, by means of a particular kind of electronic communication—that requirement has been met; and

(c) if the information is permitted to be given to a Commonwealth entity, or to a person on behalf of a Commonwealth entity, and the entity requires that particular action be taken by way of verifying the receipt of the information—that requirement has been met.

Certain other laws not affected

(3) This section does not affect the operation of any other law of the Commonwealth that makes provision requiring or permitting information to be given, in accordance with particular software requirements:

(a) on a particular kind of data storage device; or

(b) by means of a particular kind of electronic communication.

Giving information

(4) This section applies to a requirement or permission to give information, whether the expression *give*, *send* or *serve*, or any other expression, is used.

(5) For the purposes of this section, *giving information* includes, but is not limited to, the following:

(a) making an application;

(b) making or lodging a claim;

(c) giving, sending or serving a notification;

contains a provision modelled on Article 6 of the UNCITRAL Model Law on Electronic Commerce[515]. Section 9 makes it clear that, in relation to Internet transactions governed by Commonwealth law (broadly Internet transactions entered into by corporations, Internet transactions involving overseas or interstate trade, Internet transactions involving Commonwealth departments and entities and Internet transactions with individuals or businesses in the Territories if not all Internet transactions depending on constitutional interpretation of the extent of the Commonwealth government's telecommunications powers), the Statute of Frauds writing requirement could be met if the memorandum in writing existed in electronic form. Similarly, clause 6(1) of the Victorian Electronic Commerce Framework Bill (Vic), if enacted, would have the same effect in relation to Internet transactions governed by Victorian law[516].

(d) lodging a return;
(e) making a request;
(f) making a declaration;
(g) lodging or issuing a certificate;
(h) making, varying or cancelling an election;
(i) lodging an objection;
(j) giving a statement of reasons.

Note: Section 13 sets out exemptions from this section.

[515] Article 6 of the UNCITRAL Model Law on Electronic Commerce, provides:

Article 6 Writing

Where the law requires information to be in writing, that requirement is met by a data message if the information contained therein is accessible so as to be usable for subsequent reference.

[516] Clause 6 of the Victorian Electronic Commerce Framework Bill (Vic) provides:

6. Writing

(1) A person may use writing in electronic form for any purpose for which writing is required or permitted by law.

… [extracted above]

(3) This section—

(a) applies despite any provision to the contrary made by the particular law;
(b) without limiting paragraph (a), applies even if the particular law expressly or impliedly requires an original document if the electronic form is such as to permit reproduction of the document at any time as it existed when used for the relevant purpose;

5.4.2.2.5 Can a memorandum be comprised partially of text or selections that were entered by a customer into the business's web page and partially of text or formatting that is reproduced by the business's Internet commerce software application after the contract was concluded?

The fact that the terms "memorandum" and "writing" extend to documents and text that appear in electronic form does not necessarily mean that the Statute of Frauds writing requirement can be satisfied in relation to Internet commerce. This is because Internet transactions do not always involve the creation of a single memorandum (even in electronic form) which contains text that reflects the material terms on which the parties have agreed to transact.

For example, when Internet commerce is transacted by way of a business's web site it is typical for an Internet transaction to be effected through text or a selection typed in by a customer into a form on the business's web page. Only the text typed into the form (or the selections made by the customer) on the business's web page is then transmitted from the customer's browser to the business's server and then to the business's Internet commerce software application to enable the sale to be processed. The text or selection made by the customer, but not the text or formatting comprising the form, is either processed by a software application on the business's server (using a Common Gateway Interface (CGI)) or is even processed before the text reaches the business's server for example, if the business's web page uses Active X or Java. Often the text or selection typed in by the customer is directly inputted into the

---

(c) does not apply in relation to a particular transaction if the parties to that transaction otherwise agree or any of those parties reasonably requires a kind of writing other than writing in electronic form;
(d) does not apply to the extent to which its operation is excluded by section 8 in the case of a particular law.

business's database. In any case, it is not possible to point to a single memorandum on which the material terms of the contract entered into by the business and a customer are written. This suggests that where Internet commerce is conducted in this way the memorandum in writing element cannot be satisfied.

However, many Internet commerce software applications are programmed so that they can faithfully reproduce the web page from which the customer entered text or made selections. Combined with the text or selections made by the customer that were transmitted to the business it is theoretically possible to "reconstitute" a record of the material terms of the Internet transaction in writing[517]. Will the courts accept this as a memorandum in writing? It is argued here that there is precedent for the courts to do so. The courts have accepted that a memorandum in writing need not be contemporaneous with the contract that it is evidencing[518]. So, the fact that a "reconstituted" memorandum is created after an Internet transaction is concluded should not affect the validity of the memorandum. However, there is one factor that could affect the validity of a "reconstituted" memorandum. By way of background, the second element of the Statute of Frauds writing requirement requires the signature of the party to be charged. From a business's perspective this means that in order to

---

[517] For example, even the database application FileMaker Pro, aimed at the low end of the Internet commerce market, allows text sent to a business's server via a form to be displayed in the same way as the form appearing on the business's web page with the customer's selections or inputted text displayed.

[518] Provided a memorandum comes into existence before action is commenced to enforce a contract *(Popiw v Popiw* [1959] VR 197) a memorandum containing the material terms of the contract will be valid as a memorandum need not be contemporaneous with the formation of the contract. As noted by JG Starke QC, NC Seddon, MP Ellinghaus in *Cheshire and Fifoot's Law of Contract*, 6th Australian Edition, Butterworths, Sydney 1992, Ch 6, p 599, para 16.37 the memorandum is supposed to be evidence of a contract already made.

satisfy the Statute of Frauds writing requirement a memorandum evidencing an Internet transaction must be signed by the customer who was party to that transaction. Assuming that a memorandum in electronic form can be signed, the time at which the memorandum would be signed by a customer would be at the same time as when the customer is typing in or selecting an order in a form on the business's web page. A reconstituted memorandum therefore would technically involve altering or adding to the memorandum once the memorandum had been signed as it would comprise the text or selections made by the customer with the added text and formatting of the business's web page that had been generated by the business's Internet commerce software application. Interestingly, there is support in the case law for the argument that a "reconstituted" memorandum which contains additions or alterations after the signature of a customer is nonetheless valid. The courts have held that modifications to a memorandum after it has been signed can still operate as a "memorandum" that satisfies the Statute of Frauds writing requirement. In *Council of Auctioneers and Agent v SP Hilton & Co Pty Limited*, unreported judgment, CLD 13628 of 1984[519] the Supreme Court of New South Wales held that a memorandum will still be valid even if the text of it was altered after at least one of the signatures was placed on it:

> …where, as here, with the authority of the parties, words have been inserted or alterations made in the text of what purports to be such agreement, after one at least of the signatures was placed upon it, the principles applicable are in my view as follows: (1) The agreement is enforceable if the insertions or alterations accord with the terms agreed upon at the time of such earlier signature. (2) The agreement is enforceable if agreement had not been reached at the time of such earlier signature, and the insertions or alterations

[519] 12 December 1984, Supreme Court of New South Wales, Common Law Division, 1984 NSW Lexis 2290; BC8400124.

> accord with the agreement subsequently reached. (3) The agreement may be unenforceable if the document accurately sets forth the terms agreed upon at the time of signature, or at some time thereafter, and the alterations record a variation affected by a subsequent agreement. In the third of those propositions I have said no more than "may be unenforceable", as the question does not arise for decision here, and it may be that despite the decision in *New Hart Builders v Brindley* (supra) there could be cases in which some form of ratification would have effect[520].

It is therefore concluded that a "reconstituted" memorandum comprised of the text or selection entered in by a customer into a form on a business's web page and the text and the formatting of the form on the business's web page generated by the business's electronic commerce software application could satisfy the memorandum in writing element of the Statute of Frauds writing requirement. There could however be considerable evidentiary problems with establishing that the memorandum reproduced by the business's software application exactly replicated the form appearing on the business's web page and that the text inputted by the customer was not altered when transposed into the "reconstituted" memorandum.

5.4.2.2.6 Can a memorandum consist of a series of linked Internet communications?

In order to satisfy the memorandum in writing element in relation to some Internet transactions it may be necessary to link a number of Internet communications. For example, where an Internet transaction is effected by way of e-mail the material terms of the transaction agreed by the parties may be set out in number of e-mails transmitted between the transacting parties. Will the courts accept that a series of linked Internet communications constitutes a memorandum in writing? The courts

---

[520] *Council of Auctioneers and Agent v SP Hilton & Co Pty Limited*, unreported judgment, CLD 13628 of 1984,12 December 1984, Supreme Court of New South Wales, Common Law Division, 1984 NSW Lexis 2290; BC8400124.

have accepted that a series of paper documents can be linked to a comprise a single memorandum for the purpose of satisfying the Statute of Frauds writing requirement, provided that the documents can be connected either by an expressly or impliedly: *Harvey v Edwards Dunlop & Co Ltd* (1927) 39 CLR 302. The textbook writers have suggested that (paper) documents can be linked to satisfy the Statute of Frauds writing requirement in the following circumstances: (i) where there is a document signed by the party against whom the contract is sought to be enforced; and (ii) there is a sufficient reference, express or implied, in that document to either (a) a second document or (b) another transaction that was reduced into writing, provided that the documents, when read together, constitute a 'sufficiently complete' memorandum[521]. It is arguable therefore that the courts should accept that a series of linked Internet communications comprise a memorandum in writing, provided of course, that read together, the material terms of the contract are set out.

It is relevant to note that the Electronic Commerce Expert Group Report recommended that a provision following Article 10 of the UNCITRAL Model Law on Electronic Commerce be legislatively implemented in Australia. Article 10 of the Model Law provides that a legal obligation to retain records, information or documents is met if such information, documents or records is stored in electronic form provided that the information stored can be accessed for subsequent reference and the original or an accurate format is retained[522].

---

[521] Starke, Seddon, Ellinghaus, para 545.

[522] Article 10 of the UNCITRAL Model Law on Electronic Commerce provides:
Article 10. Retention of Data Messages

This recommendation was incorporated in Commonwealth law in the Electronic Transactions Act 1999 (Cth), section 11. Section 11 allows a person to produce a document that is in electronic form provided that there is a reliable assurance as to the integrity of the information in the message and that the information is readily accessible so as to be useable for subsequent reference[523]. This provides support to

---

(1) Where the law requires that certain documents, records or information can be retained, that requirement is met by retaining data messages, provided that the following conditions are satisfied:
(a) the information contained therein is accessible so as to be usable for subsequent reference; and
(b) the data message is retained in the format in which it was generated, sent or received, or in a format which can be demonstrated to represent accurately the information generated, sent or received; and
(c) such information, if any, is retained as enables the identification of the origin and destination of a data message and the date and time when it was sent or received.

(2) An obligation to retain documents, records or information in accordance with paragraph (1) does not extend to any information the sole purpose of which is to enable the message to be sent or received.

(3) A person may satisfy the requirement referred to in paragraph (1) by using the services of any other person, provided that the conditions set forth in subparagraphs (a), (b) and (c) of paragraph (1) are met.

[523] Section 11 of the Electronic Transactions Act 1999 (Cth) provides:
11 Production of document
Requirement to produce a document
(1) If, under a law of the Commonwealth, a person is required to produce a document that is in the form of paper, an article or other material, that requirement is taken to have been met if the person produces, by means of an electronic communication, an electronic form of the document, where:
(a) in all cases—having regard to all the relevant circumstances at the time of the communication, the method of generating the electronic form of the document provided a reliable means of assuring the maintenance of the integrity of the information contained in the document; and
(b) in all cases—at the time the communication was sent, it was reasonable to expect that the information contained in the electronic form of the document would be readily accessible so as to be useable for subsequent reference; and
(c) if the document is required to be produced to a Commonwealth entity, or to a person on behalf of a Commonwealth entity, and the entity requires that an electronic form of the document be produced, in accordance with particular software requirements, by means of a particular kind of electronic communication— that last-mentioned requirement has been met; and
(d) if the document is required to be produced to a Commonwealth entity, or to a person on behalf of a Commonwealth entity, and the entity requires that particular action be taken by

the view that, provided that the requirements set out in *Harvey v Edwards Dunlop & Co Ltd* are satisfied, Internet communications can be linked to comprise a single memorandum in relation to transactions governed by Commonwealth law. This is because section 11 effectively provides that the fact that a contract is evidenced only by way of an Internet communication that is in electronic form is not a basis for denying the validity or enforceability of a contract. In other words, if the law says that a series of linked paper documents can comprise a memorandum, then section 11

---

way of verifying the receipt of the document—that last-mentioned requirement has been met.

Permission to produce a document

(2) If, under a law of the Commonwealth, a person is permitted to produce a document that is in the form of paper, an article or other material, then, instead of producing the document in that form, the person may produce, by means of an electronic communication, an electronic form of the document, where:

(a) in all cases—having regard to all the relevant circumstances at the time of the communication, the method of generating the electronic form of the document provided a reliable means of assuring the maintenance of the integrity of the information contained in the document; and

(b) in all cases—at the time the communication was sent, it was reasonable to expect that the information contained in the electronic form of the document would be readily accessible so as to be useable for subsequent reference; and

(c) if the document is permitted to be produced to a Commonwealth entity, or to a person on behalf of a Commonwealth entity, and the entity requires that an electronic form of the document be produced, in accordance with particular software requirements, by means of a particular kind of electronic communication— that requirement has been met; and

(d) if the document is permitted to be produced to a Commonwealth entity, or to a person on behalf of a Commonwealth entity, and the Commonwealth entity requires that particular action be taken by way of verifying the receipt of the document—that requirement has been met.

Integrity of information

(3) For the purposes of this section, the integrity of information contained in a document is maintained if, and only if, the information has remained complete and unaltered, apart from:

(a) the addition of any endorsement; or

(b) any change which arises in the normal course of communication, storage or display.

Note: Section 13 sets out exemptions from this section.

Certain other laws not affected

(4) This section does not affect the operation of any other law of the Commonwealth that makes provision requiring or permitting electronic forms of documents to be produced, in accordance with particular software requirements:

(a) on a particular kind of data storage device; or

(b) by means of a particular kind of electronic communication.

provides that a series of linked documents in electronic form produced in place of a series of documents in paper form will suffice. There is, however, an alternative and narrower interpretation of section 11 which is that there must have been in existence at some point in time the document in paper form. The explanatory paper accompanying the Electronic Transactions Act 1999 (Cth) when it was in bill form envisages that a paper form of the document exists[524]. Under this interpretation, as Internet transactions can take place without any documentation at all being in paper form the effect of section 11 would be of limited use in supporting the argument that a series of linked Internet communications can comprise a memorandum, since the Internet communications would not ever have originally existed in a paper form. If this interpretation of section 11 is correct it may still be possible to put forward an argument that a series of linked Internet communications should be considered equivalent to a series of linked documents by reliance on section 8 of the Electronic Transactions Act 1999 (Cth), the effect of which has been discussed earlier in this chapter, but in short, makes clear that a transaction under a law of the Commonwealth will not be invalid simply because it was conducted by the use of electronic communications. However, section 8 is intended to apply only where a more specific section in Part 2 of the Act does not apply[525]. Thus, on the narrow interpretation of

---

524 See for example, Attorney- General's Department, "Explanatory Paper -Electronic Transactions Bill 1999", January 1999 at p 11 where it states, "This requirement is intended to ensure that the information in the document has remained complete and unaltered from when it was in the form of a paper document through its translation into the form of an electronic communication."

525 Subsection 11(2) provides that Section 8 will only apply where a more specific section in Part 2 of the Act does not apply. The Attorney- General's Department, "Explanatory Paper -Electronic Transactions Bill 1999", January 1999 at p 6 states: "Subclause (2) makes clear that this provision

section 11, it is uncertain that a series of linked Internet communications can comprise a memorandum.

Clause 6(2) of the Electronic Commerce Framework Bill (Vic)[526], if enacted, will have the effect that a series of linked Internet communications used in relation to an Internet transaction governed by Victorian law will constitute linked documents, provided that such communications can be retained for subsequent reference. It follows that, if such communications have the same effect as that of writing in paper form, provided they satisfy the requirements set out in *Harvey v Edwards Dunlop & Co Ltd*, they can constitute a memorandum for the purposes of the Statute of Frauds writing requirement.

Notwithstanding that an argument can be made out that the courts should accept that a series of linked Internet communications can constitute a memorandum in writing there is still an evidential problem of proving that an Internet communication has not been altered since it was created. This problem may well be met through date stamping the Internet communications combined with digital signatures.

5.4.2.2.7 Some conclusions about the first element of the writing requirement

In conclusion, whether an Internet transaction that is subject to the Statute of Frauds writing requirement can satisfy the requirement of a "memorandum in

---

is only intended to operate where another, more specific, provision in Part 2 of the Bill does not apply. That is, it will operate as a default provision, providing a general rule that will have effect when the specific provisions in Part 2 do not operate. This is to ensure that this provision does not conflict with, or override, any of the specific requirements contained in the other provisions in Part 2."

526 Clause 6(2) provides:

writing" depends on how the Internet transaction was conducted. In instances where the Internet transaction results in a single Internet communication that sets out the material terms of the agreement, albeit in electronic form, it is highly probable that the courts will be satisfied that the memorandum in writing requirement is met. Moreover, the Commonwealth Electronic Transactions Act 1999 (Cth) (according to the broader interpretation of section 11) and Victorian Electronic Commerce Framework Bill (under clause 6(2)), if enacted, legislatively provide that such an Internet communication constitutes a memorandum in writing in their respective jurisdictions.

However, some Internet transactions may not be able to satisfy the "memorandum in writing" element of the Statute of Frauds writing requirement. Some methods of conducting Internet commerce may be such that in order to satisfy the "memorandum" requirement of the Statute of Frauds writing requirement it is necessary to link a series of Internet communications. Also, some methods of conducting Internet commerce mean that a memorandum in writing could only exist if the law accepted that a memorandum could be comprised partially of text or a selection entered by a customer into a form on a business's web page and the text and formatting of the form generated by the business's electronic commerce software application. In both cases it is suggested that the case law supports an argument that

---

> The effect of writing in electronic form is the same for the purposes of any law as that of writing in paper form if the electronic form is such as to permit retention of the writing for subsequent reference.

the court should accept there exists a valid memorandum in writing but it is acknowledged that there are associated evidential difficulties.

5.4.2.2.8 The second element of the Statute of Frauds writing requirement

The second element of the Statute of Frauds writing requirement is that the memorandum must bear the signature of the party against whom the contract is sought to be enforced. Clearly it is not possible for a memorandum to be signed with a handwritten signature in the context of Internet commerce. This raises the question of whether alternative methods of "signing" will suffice. For example, will a typed signature satisfy the signature element of the Statute of Frauds writing requirement? Can an electronic "facsimile" signature such as a scanned in handwritten signature, or the more sophisticated biometric facsimile of a signature satisfy the signature element of the Statute of Frauds writing requirement? Also would a digital signature satisfy the signature element of the Statute of Frauds writing requirement? These methods are all techniques that could be used in place of a handwritten signature in the context of Internet commerce. Whether their use would satisfy the signature element of the Statute of Frauds writing requirement will be considered in turn.

5.4.2.2.9 Whether the typed name of a customer constitutes a signature

The word "signature" has not been defined in any of the Interpretation Acts of each State and Territory, although in New South Wales[527] and Queensland[528] "sign" includes the attaching or affixing of a seal and the making of a mark and in Western

---

[527] Section 21 of the Interpretation Act 1987 (NSW).
[528] Section 36 of the Acts Interpretation Act 1954 (Qld).

Australia "sign" includes the affixing or making of a seal, mark or thumbprint[529]. It is necessary therefore, to turn to the common law to ascertain what, apart from a handwritten signature, can constitute a signature.

In considering the common law on signatures it is relevant to draw a distinction between how the courts have treated the requirement of a signature in general and the how the courts have defined what constitutes a signature for the purpose of satisfying the Statute of Frauds writing requirement. In considering what constitutes a signature in general, the courts have taken a broad view of what constitutes a signature. For example, there is Australian authority for the view that a document will be considered to satisfy the requirement for a signature if there appears upon it a mark made by or by the authority of the signatory in instances where a statute merely requires that a document shall be signed: *R v Moore: ex parte Myers* (1884) 10 VLR 322 at 324. The High Court has further stated that a signature need not even be signed by the party whose signature is being affixed; In *O'Reilly v State Bank of Victoria Commissioners* (1983) 153 CLR 1 at 11 Gibbs, J pointed out that "as a general proposition at common law, a person sufficiently signs a document if it is signed in his name and with his authority by somebody else". Further, a rubber stamped or engraved signature, if authorised by the signatory, constitutes a signature: *Goodman v. J Eban Limited* 1954 1 QB 550 (which was approved in *Molodysky v Vema Australia Pty Ltd* (Supreme Court of NSW Equity Division, No. 4189 of 1988, 20 December 1988). In addition, the courts have held that the printed name of the signatory can constitute a

---

529 Section 5 of the Interpretation Act 1984 (WA).

signature. The High Court in *Neill v Hewens* (1953) 89 CLR 1 envisaged that a typed name of a party could constitute a signature, although on the facts of that case it was held that 'when in the course of the preparation of the document [the defendant's] name was typed in by the solicitor's clerk it could not at that point of time have operated as an equivalent of his signature'[530]. Likewise in *Torrac Investments Pty Ltd v Australian National Airline Commission* (1985) ANZ Conv R 82 at 5 the court assumed that a printed name that was sent by telex constituted a signature[531]. Also, a signature need not be located at the foot of a document, provided that the signature was intended to authenticate the whole of the document: *Caton v. Caton* (1876) LR 2 HC 127.

More specifically, in relation to the *signature element of the Statute of Frauds writing requirement*, it appears that the courts have assumed that in the absence of an actual handwritten signature, a signature must, at the very least, comprise *the name of the relevant party* and *an intention (that can be inferred) of the party to be bound by the document on which the party's name appear:*

> The need for the memorandum to be "signed" has been given an elastic interpretation by the courts, concentrating upon the presence of the defendant's name upon the document, and his accompanying conduct, as recognising the existence of the contract.
>
> The operation of this principle ("the authenticated signature fiction") is dependent upon two elements: the fact of the defendant's name on the

---

530 *Neill v Hewens* (1953) 89 CLR 1 at 13.

531 See discussion of JG Starke QC, NC Seddon, MP Ellinghaus, *Cheshire and Fifoot's Law of Contract*, 6th Australian Edition, Butterworths, Sydney 1992, Ch 5, p 256, para 541.

> document; and the existence of a basis for inferring the necessary intention on his part to be bound by the document containing his name so recorded.[532]

The "authenticated signature fiction" is a principle laid down by the courts which provides that the signature element of the Statute of Frauds writing requirement can be satisfied, without the actual handwritten signature of the party to be charged, by the printed or typed name of that party provided that the party expressly or impliedly indicates that he or she recognizes the writing as being an authenticated expression of the contract. This principle can be traced to early English cases such as *Shneider v Norris* (1814) 2 M & S 286; 105 ER 388; *Tourret v Cripps* (1879) 48 LJ Ch 567; *Evans v Hoare* (1892) 1 QB 593 and the more recent case of *Leeman v Stocks* (1951) Ch 941. In the Australian context, the principle was applied by the High Court in *Neill v Hewens* (1953) 89 CLR 1 and referred to in *Pirie v Saunders* (1961) 104 CLR 149. In *Neill v Hewens* (1953) 89 CLR 1 the High Court appeared to accept the proposition of Counsel for the Respondent that the "authenticated signature fiction" would apply when: (a) the writing constituting the "memorandum" contains the name of the party to be charged and (b) that the party to be charged has shown him or herself, or through a duly authorised agent, that the party recognises the writing (though not subscribed with the party's personal signature) as being the final or complete record of the contract, although on the facts of the case the principle did not apply[533]. In *Pirie v Saunders* (1961) 104 CLR 149 the High Court referred to the

---

[532] DW Greig and JLR Davis, *The Law of Contract*, The Law Book Company Ltd, 1987, Sydney, Ch 12, pp 713-714.

[533] *Neill v Hewens* (1953) 89 CLR 1 at p 14. The High Court held that the presence of the defendant Hewen's name typed in by a solicitor's clerk into a contract for the sale of land did not attract the

"authenticated signature fiction" but again on the facts of the case the principle was held not to apply[534]. The High Court cited and seemingly accepted the principle as enunciated by the Full Court of the Supreme Court of NSW, when the party's dispute came before the Full Court, "that if the name of the party to be charged (not being a signature in the ordinary sense of the word) is placed on the document said to constitute the written memorandum of the contract, it is to be treated as a signature for the purposes of the statute if such party expressly or impliedly indicates that he recognizes the writing as being an authenticated expression of the contract."[535]

It follows that a document containing the typed name of a customer, (such as an e-mail or a file created from the text inputted by a customer into a form appearing on a business's web page) will satisfy the signature element of the Statute of Frauds writing requirement provided that it can also be proved that the party whose name is typed intended that the document constitute an authenticated expression of the contract[536]. Thus, a typed name that has been entered by a customer into a form on a

---

operation of the "authenticated signature fiction" because it was clear on the evidence that the defendant had not intended the contract to constitute the final or complete expression of the contract between the parties without the defendant's actual signature.

534 In *Pirie v Saunders* (1961) 104 CLR 149 the High Court held that on the facts, a solicitor's note detailing terms on which the parties had agreed to contract did not constitute a memorandum as the note was simply a brief notation of instruction for the preparation of a draft lease for submission to the respondent's solicitor. The note did not indicate the existence of a binding contract: "..in other words, it may be said that the enumerated particulars do not appear as a note or memorandum of a subsisting contract as distinct from bare instructions for the preparation of a formal lease. Both the document and its contents are quite consistent with the hypothesis that the parties had not made any prior binding contract and that their rights and obligations were not to be effected until the execution of a memorandum of lease in the form which, after dicussion, it should finally take. That being so it in no way recognizes the existence of any binding contract and cannot therefore be regarded as a note or memorandum of any contract" at p 145.

535 *Pirie v Saunders* (1961) 104 CLR 149 at p 154.

536 See DW Greig and JLR Davis, Fifth Cumulative Supplement to the Law of Contract, The Law Book Company Limited, 1993 p 174 in relation to the commentary made at p 715 of *The Law of*

business's web site or in an e-mail from the customer to the business will constitute a signature for the purposes of the Statute of Frauds writing requirement, provided that it can be established that the customer intended the writing (whether in the e-mail or the form) to be a final record of the transaction. However, it is unlikely that the name of a sender of an e-mail in the "From:…" line in an e-mail header will constitute a signature for the purposes of the Statute of Frauds writing requirement. It is suggested here that the courts would be loath to find that the presence of a sender's typed name in an e-mail header by itself signifies that the sender intended the e-mail to constitute the final record of the transaction between the parties. Generally, the name of the sender is automatically inserted by the sender's e-mail application in order to comply with e-mail protocols/standards that require this information in order for an e-mail to be sent. In such circumstances it would surely be difficult to argue that the presence of the sender's name in the e-mail header expressly or impliedly signifies that the sender intends that the e-mail be the final and complete record of the transaction between the parties. Of course, whether the "authenticated signature fiction" will apply depends on the factual circumstances of each case. Thus, where a

---

Contract, The Law Book Company Ltd, Sydney, 1987: "However, ultimately the question of whether the typing of a name on a message or document constitutes a signature depends on the apparent intention of the parties, to be deduced from the circumstances as a whole."

In referring to signatures that appear on telexes or facsimiles the writers further comment at p 174, "It is necessary to examine the contents of the message and document which is transmitted and the purpose for its transmission against the background of the parties' dealings to establish if, in the circumstances, the act of authentication amounts to the sender's assent to the terms contained in the message or document."

See also the commentary at pp 713-714 where it is noted that two elements must be established in order to satisfy the signature element of the writing requirement: the name of the party and an intention (this can be inferred) of the party to be bound by the document on which the party's name appears.

sender expressly or impliedly indicates that the e-mail (though not subscribed with the party's personal signature) is the final or complete record of the contract between the parties, then the courts may well apply the "authenticated signature fiction" and find that the signature element of the Statute of Frauds writing requirement has been satisfied.

It is relevant to discuss here the effect of any legislative implementation of Article 7 of the UNCITRAL Model Law on Electronic Commerce. Article 7 provides that where an electronic method is used for signing a document which is reliable for the purpose for which the method was used, then such method employed will satisfy any legal requirement for a signature[537]. Arguably the effect of this provision is to provide legal status to a typed signature where the use of a typed signature is sufficient to identify a person and to indicate a person's approval of the contents of the Internet communication in question. The guide accompanying the UNCITRAL Model Law on Electronic Commerce envisages that in determining whether a particular method used in place of a signature is appropriate legal, technical and commercial factors may be taken into account including:

> …the sophistication of the equipment used by each of the parties; (2) the nature of their trade activity; (3) the frequency at which commercial

---

[537] *Article 7. Signature*
(1) Where the law requires a signature of a person, that requirement is met in relation to a data message if:
(a) a method is used to identify that person and to indicate that person's approval of the information contained in the data message; and
(b) that method is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement.
(2) paragraph (1) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for the absence of a signature.

> transactions take place between the parties; (4) the kind and size of the transaction; (5) the function of signature requirements in a given statutory and regulatory environment; (6) the capability of communication systems; (7) compliance with authentication procedures set forth by intermediaries; (8) the range of authentication procedures made available by any intermediary; (9) compliance with trade customs and practice; (10) the existence of insurance coverage mechanisms against unauthorized messages; (11) the importance and the value of the information contained in the data message; (12) the availability of alternative methods of identification and the cost of implementation; (13) the degree of acceptance or non-acceptance of the method of identification in the relevant industry or field both at the time the method was agreed upon and the time when the data message was communicated; and (14) any other relevant factor[538].

It is arguable that given other more secure, non-repudiable methods of identifying and signifying approval of the contents of an Internet communication, such as digital signatures and electronic signatures, are available, that the use of a typed signature in place of a signature would as a general rule qualify for the legal recognition accorded under Article 7 of the UNCITRAL Model Law on Electronic Commerce. Conversely, it is conceivable that there will be circumstances where it is considered appropriate to use typed signatures eg. when the value of the transaction is low and where digital signature or electronic signature technology is not available to both transacting parties.

Section 10 of the Electronic Transactions Act 1999 (Cth) is broadly based on Article 7 of the UNCITRAL Model Law on Electronic Commerce. Section 10 provides that, where a method is used to identify a person and to indicate the person's approval of the information communicated, it will satisfy the requirement for a signature, provided that the method used was as reliable as was appropriate for the

---

538 "Guide to the Enactment of the UNCITRAL Model Law on Electronic Commerce (1996", 1997, para 58, http://www.un.or.at/uncitral/texts/electcom/ml-ec.htm.

purposes for which the information was communicated. Although arguably the typed name of a person is intended to identify a person and indicate that person's approval of the information communicated, it is unlikely that, except where the value of the transaction is very low, a typed signature will satisfy the requirement that the method used is "appropriate" given how simple it would be to impersonate someone else if a typed name constituted in these circumstances a signature.

Section 5(1) of the Electronic Commerce Framework Bill (Vic) provides that a person may use an electronic signature for a purpose for which a signature is required or permitted by law. Section 5(2) further states that the effect of an electronic signature is the same for the purposes of any law as that of a paper-based signature. Section 3 defines an "electronic signature" as the result of a process by which a person authenticates a document in electronic form and acknowledges that the document is being signed. Given that an "electronic signature" is given such a broad definition it is arguable that a typed signature falls within the definition of electronic signature and therefore under section 5 has the same legal effect as a paper-based signature.

In conclusion, there exists common law precedent for supporting the argument that a typed signature can constitute a signature for the purposes of the Statute of Frauds writing requirement. Further, under the Electronic Transactions Act 1999 (Cth) and the Electronic Framework Bill (Vic), if enacted, it is arguable that, due to the legal status afforded to electronic signatures by this legislation, and due to the broad language used in the legislation to define electronic signatures or methods of

electronically signing a document, typed signatures will fall within the categories of electronic signatures accorded legal recognition as signatures. In the Commonwealth jurisdiction, it should be noted there is an additional requirement that use of a typed signature is "appropriate", as required under section 10, which will have the effect of limiting the circumstances in which a typed signature will be given legal status as a signature.

5.4.2.2.10 Whether the use by a customer of an electronic "facsimile" signature constitutes a signature

In relation to whether an electronic "facsimile" signature constitutes a signature for the purposes of the Statute of Frauds writing requirement it is relevant to briefly describe how electronic "facsimile" signatures can be created and transmitted through the Internet. The term electronic "facsimile" signature is used to describe an electronic signature which also has the visual appearance of a paper-based signature.

In its least sophisticated form an electronic "facsimile" signature would comprise an image of a handwritten signature that has been scanned in from a paper based version of the handwritten signature.

A more sophisticated "facsimile" signature is a digitised handwritten signature created using biometrics. It is convenient, by way of illustration, to describe the PenOp software. PenOp, owned by PenOp Inc, is software that operates as a plug-in, or component, that can add functionality to several applications, such as Adobe Acrobat, Netscape Navigator and Microsoft Word. Basically, PenOp creates an electronic "facsimile" of a signature by digitising a party's signature whilst it is being written on a digital tablet or a touch screen. Whilst a signature is being written,

PenOp digitises and records various information about the signature (such as the date and time the signature was written, the identity of the signatory and several biometric measurements concerning how the signature was signed such as stroke direction, speed and acceleration) to create what is termed a "Biometric Token", that is attached to the electronic document which a party wishes to "sign". Additionally, an image of the signature forms part of the Biometric Token so that the party's "facsimile" signature can be viewed. Also incorporated into the Biometric Token is a compressed form of the contents of the electronic document which the party wishes to "sign" **("hash value")**[539] that is created by applying a mathematical algorithm. A hash value of the data that comprises the Biometric Token is also created and it and the Biometric Token are encrypted to create a "signature". Other parties can determine whether a "signature" has been altered or "cut and pasted" into a document or whether a document has been altered by analysing the signature using PenOp software. The image of a party's "facsimile" signature can also be viewed with the aid of a viewer that is being distributed free of charge by PenOp.

At present, the only Australian jurisdiction that provides for legal recognition of an electronic "facsimile" of a signature is the Commonwealth jurisdiction. Section 10 of the Commonwealth Electronic Transactions Act 1999 (Cth) provides legal recognition of electronic (including digital) signatures provided that the technique used to achieve an electronic "facsimile" signature is appropriate for the purposes for which it was used and is reliable as appropriate in the circumstances. The Victorian

---

[539] Also called a "hash result", "message digest" or "checksum".

Electronic Commerce Framework Bill, section 5 also accords legal validity to electronic signatures. The Victorian Bill defines an electronic signature as the result of a process applied by a person to a document in electronic form by which the person authenticates the document and acknowledges that the document is being signed.

The definition of electronic signature employed by the Commonwealth Electronic Transactions Act 1999 (Cth) and the Victorian Electronic Commerce Framework Bill is arguably broad enough to apply to what in this thesis is termed an electronic "facsimile" signature, even one that is less sophisticated than the model used in Pen Op, such as the use of a scanned handwritten signature, although the Commonwealth Electronic Transactions Act 1999 (Cth) requires that an electronic signature's use must be appropriate to the purposes for which it was used and as reliable as is necessary given the circumstances. It is clear, in relation to Internet transactions governed by Commonwealth law that an electronic "facsimile" signature constitutes a signature subject to the "appropriateness" requirements discussed earlier at 5.4.2.2.10. Similarly, if the Victorian Electronic Commerce Framework Bill is enacted, it will be clear in relation to Internet transactions governed by Victorian law that an electronic "facsimile" signature constitutes a signature.

Without a legislative provision of the type employed by the Commonwealth Electronic Transactions Act 1999 (Cth) and the Victorian Electronic Commerce Framework Bill, it will be necessary to look at the common law to determine whether an electronic "facsimile" signature constitutes a signature for the purposes of the

Statute of Frauds writing requirement. There is some support in the case law for the view that an electronic "facsimile" signature constitutes a signature for the purposes of the Statute of Frauds writing requirement. In the unreported Supreme Court of NSW judgment of *Molodysky v Vema Australia Pty Ltd* (Supreme Court of NSW Equity Division, No. 4189 of 1988, 20 December 1988) Justice Cohen held that a facsimile of a contract for the sale of land upon which the signature of the defendant had been written constituted a document signed by the defendant:

> The question of whether a facsimile bearing a person's signature constitutes a document signed by that person is not easy to resolve. Where a statute requires a signature to be placed on a document it is sufficient if the person authorises the placing on the appropriate document of a signature by mechanical means such as a rubber stamp or engraving. *Goodman v J. Eban Limited* 1954 1 QB 550. Lord Evershed MR said at 557 that "the essential requirement of signing is the affixing in some way, whether by writing with a pen or pencil or by otherwise impressing upon the document, one's name or 'signature' so as personally to authenticate the document." A facsimile copy of the document is one which is sent by telephonic means and reproduced at the receiving end by what can be in general terms but somewhat inaccurately described as a photographic process. When a person sends a signature with the intention that it should be produced by facsimile then that person is authorising the placing on the facsimile copy of a copy of his signature with the intention that it be regarded as his signature. This of course does not apply in every case of a signature on a facsimile document but only if it is intention of the person concerned that what appears on the final copy is to be regarded as that person's signature for the purpose of authenticating the document.[540]

It is submitted that an electronic "facsimile" signature is analogous to a signature appearing on a faxed document and that the legal principles governing signatures appearing on faxed documents will equally apply to electronic "facsimile" signatures. Like an electronic "facsimile" signature, what appears on a facsimile is an electronic

---

[540] *Molodysky v Vema Australia Pty Ltd*, Supreme Court of NSW, Equity Division, No. 4189 of 1988, 20 December 1988, pp 28-29.

but visual representation of a handwritten signature. On this reasoning it follows that if a customer uses an electronic "facsimile" signature in an Internet communication to a business, such signature constitutes a signature for the purposes of the Statute of Frauds writing requirement provided that it was the intention of the customer that the electronic "facsimile" signature be regarded as a signature for the purpose of authenticating the Internet communication. Thus it would appear that, according to the common law, at least in NSW, an electronic "facsimile" signature could satisfy the signature element of the Statute of Frauds writing requirement.

In conclusion, there is some support in the common law for the argument that an electronic "facsimile" signature constitutes a signature for the purposes of the Statute of Frauds writing requirement. Further, under the the Electronic Transaction 1999 (Cth) and, if the Electronic Commerce Framework Bill (Vic) is enacted, it is arguable that, due to the legal status afforded to electronic signatures by this legislation, and due to the broad language used in the legislation to define electronic signatures, or methods of electronically signing a document, electronic "facsimile" signatures fall within the categories of electronic signatures accorded legal recognition as signatures, although in the Commonwealth jurisdiction this depends on whether the use of an electronic "facsimile" signature is "appropriate" as required under section 10.

5.4.2.2.11 Whether digital signatures constitute signatures for the purposes of the Statute of Frauds writing requirement

A description of digital signatures and how they work is given at 5.10.4 at p402.

Presently the only legislation in Australia that accords digital signatures the legal status of paper-based signatures is the Electronic Transactions Act 1999 (Cth). Both the Electronic Transactions Act 1999 (Cth) and the Electronic Commerce Framework Bill (Vic) have provisions that equate digital signatures with signatures[541]. Therefore, under the Electronic Transactions Act 1999 (Cth), the use of digital signatures will satisfy the signature element of the Statute of Frauds writing requirement, in relation to Internet transactions governed by Commonwealth law. If the Electronic Commerce Framework Bill (Vic) is enacted, the use of digital signatures will satisfy the signature element of the Statute of Frauds writing requirement, in relation to Internet transactions governed by Victorian law.

In the absence of legislation that expressly accords digital signatures the same legal significance as paper-based signatures it is relevant to consider the common law position on signatures. No Australian case law has directly considered the legal status of a digital signature and whether a digital signature could satisfy the signature element of the Statute of Frauds writing requirement. It was noted earlier, however, at 5.4.2.2.9 at p273 that the courts have broadly interpreted what constitutes a signature and it seems reasonable to speculate that the courts may be willing to extend the definition of signature to encompass digital signatures. The fact that digital signatures can fulfil several of the functions of paper-based signatures (such as authentication, non-repudiation, content integrity, identification) adds further support to an argument

---

[541] Section 10, Electronic Transactions Act 1999 (Cth), Clause 5, Electronic Commerce Framework Bill (Vic).

that the courts should accord digital signatures the same legal significance as paper-based signatures. However, it is suggested here that it is unlikely that the courts, in the absence of digital signature legislation, would accept that a digital signature constitutes a signature *for the purposes of the Statute of Frauds writing requirement*, notwithstanding that digital signatures can fulfil the same functions performed by signatures. This is because the common law expresses the requirements for a signature for the purposes of the Statute of Frauds writing requirement in terms of "form" rather than "function". Significantly, as noted earlier, the courts have assumed that in the absence of an actual handwritten signature, a signature that satisfies the signature element of the Statute of Frauds writing requirement should, at the very least, comprise the *name* of the relevant party[542]. This requirement can be distinguished from other statements made in the courts concerning the broader issue of what constitutes a signature generally where, unlike signatures used for the purposes of the Statute of Frauds writing requirement, there appears to be no requirement that a signature represent a party's name (for example, a signature in general can be comprised of a mark).

It follows that the use of digital signatures alone cannot be equated at common law with signatures that satisfy the Statute of Frauds writing requirement as digital

---

[542] See for example the commentary of DW Greig and JLR Davis, *The Law of Contract*, The Law Book Company Ltd, 1987, Sydney, Ch 12, pp 713-714 who state:

"The need for the memorandum to be "signed" has been given an elastic interpretation by the courts, concentrating upon the presence of the defendant's name upon the document, and his accompanying conduct, as recognising the existence of the contract.

The operation of this principle ("the authenticated signature fiction") is dependent upon two elements: the fact of the defendant's name on the document; and the existence of a basis for

signatures do not represent the signing party's name (for a detailed discussion of digital signatures and how they work see 5.10.4 at p402). If, however, digital signatures were used in combination with the typed name of the party it is arguable that according to common law principles such circumstances would constitute a signature for the purposes of the Statute of Frauds writing requirement. For example, if a customer's name and other order details was entered into a form on a business's web page which, when transmitted to the business, also "attached" the customer's digital signature, this would arguably constitute a signature for the purposes of the Statute of Frauds writing requirement, provided that it could be inferred that the customer intended to be bound by the contents of the web page form. Since it was earlier concluded that a typed name alone could constitute a signature for the purposes of satisfying the Statute of Frauds writing requirement it seems superfluous to require a customer to use a digital signature in order to satisfy the Statute of Frauds writing requirement.

It is also possible that the digital certificate provided by a customer in order to enable a business to verify the customer's digital signature, in combination with the customer's digital signature, would satisfy the "name" element as presumably the customer's digital certificate would refer to the customer's name. Given that the document comprising the digital signature is separate from the document comprising the digital certificate it seems unlikely that the courts would accept an argument that

---

inferring the necessary intention on his part to be bound by the document containing his name so recorded."

the two together constituted a signature for the purposes of the Statute of Frauds writing requirement. For the courts to accept such a proposition would be like accepting that, in relation to paper-based signatures, a document containing a party's name should, when read with a second document, satisfy the signature element of the Statute of Frauds writing requirement in relation to the second document because the first document refers to the name of the signing party and the first document can be linked in some way to the second document. It is therefore concluded that it is unlikely that the courts will find that digital signatures constitute signatures for the purposes of the Statute of Frauds writing requirement[543].

This conclusion is at odds with some writers who consider that digital signatures can constitute signatures under common law[544]. This difference in opinion can be attributed to several factors. First, many of those writers are commenting on US law which differs from the Australian situation in that the US Uniform Commercial Code, unlike the common law in Australia, provides that a mark can constitute a signature for the purposes of the US equivalent of the Statute of Frauds writing requirement,

---

543 Note that some authors have argued to the contrary. See for example Adrian McCullagh, Peter Little, William Caelli, "Electronic Signatures: Understand the Past to Develop the Future", *UNSW Law Journal*, 1998, Volume 21(2), at 46-461 who argue that "This indirect access to the name of the signatory should satisfy the Statute of Frauds provided the integrity of the electronic certificate is assured. The central issue for the purposes of the Statute of Frauds must b the act of affixing the mark with an intention to be bound together with some method of identifying the person so bound. It should not matter that the identification process is not directly from the document itself but is achieved through some indirect secure method."

544 See for example Professor Alan Tyree in *PINS and Signatures*, http://www.law.usyd.edu.au/~alant/inchoate.html expresses the view that a digital signature will satisfy the elements of a signature under the common law. Similarly, Leif Gamertsfelder in "Electronic Bills of Exchange: Will the current law recognise them?", *UNSW Law Journal*, 1998, Vol 21(2), 566 at 571 asserts that "only a technologically averse court could decide otherwise [than to conclude that digital signatures constitute signatures under common law.]

thus opening the way for an interpretation that a digital signature constitutes a signature[545]. Secondly, in some instances those writers who have concluded that digital signatures will constitute signatures under common law in the Australian context have failed to acknowledge the distinction between the requirements for signatures used for the Statute of Frauds writing requirement and for signatures in general[546]. These writers have typically approached the issue by examining the purpose or object of signatures (such as authentication, content integrity, non-repudiation, ceremony and identity) and concluding that since digital signatures can achieve or satisfy these elements that they too should be recognised as signatures under common law. Whilst it is not disputed that digital signatures share can replicate many of the features of paper-based signatures, it does not follow that digital signatures will constitute signatures under common law. As argued above, a distinction must be drawn between a signature used for the purpose of the Statute of Frauds writing requirement and a signature used more generally. To reiterate, a signature, other than an actual handwritten signature, which is used for the purpose of the Statute of Frauds writing requirement is subject to the *additional* requirement that it must comprise the *name* of the signing party, a requirement that has been overlooked by those writers who have concluded that digital signatures can constitute signatures under common law. Also, there are in fact some practical differences between digital signatures and paper-based signatures which stand in the way of

---

545 See for example, UCC 1-2-1(39) (1992).

546 See for example, Adrian McCullagh, Peter Little, William Caelli, "Electronic Signatures: Understand the Past to Develop the Future", *UNSW Law Journal*, 1998, Volume 21(2), p 452.

concluding that, because a digital signature can fulfil many of the functions of paper-based signatures, it should logically follow that a digital signature should have the same legal significance as a signature under common law. For example, a paper-based signature can be verified as long as the document on which the signature appears is still in existence. Digital signatures in contrast, in the same way that many computer files made 10 years ago can no longer be read using present technology, are unlikely to be verifiable for more than a limited amount of time given the pace of change in relation to the technology used to create, use and verify digital signatures[547]. Also, from an evidential viewpoint, in the event that the veracity of a paper-based signature is disputed the science of ascertaining and proving that a signature is fraudulent is relatively easy to explain and generally understood by laypeople such as judges and juries. In contrast, the science of ascertaining and proving a fraudulent digital signature is detected is not so simple or easily comprehensible:

> Digital signatures are fiendishly complex, involving arcane number theory, the workings of computer operating systems, communications protocols, certificate chain processing, certificate policies, and so on. There are very few people on this planet (if any) who completely understand every process involved in generating and verifying a digital signature. The potential for confused lawyers, judges and juries is extreme[548].

---

547 David Fillingham, "A Comparison of Digital and Handwritten Signatures", Paper for MIT 6.805/STS085: Ethics and Law on the Electronic Frontier, Fall 1997, http://www-swiss.ai.mit.edu/6805/student-papers/fall97-papers/fillingham-sig.html.

548 David Fillingham, "A Comparison of Digital and Handwritten Signatures", Paper for MIT 6.805/STS085: Ethics and Law on the Electronic Frontier, Fall 1997, http://www-swiss.ai.mit.edu/6805/student-papers/fall97-papers/fillingham-sig.html.

It is for these reasons that it is argued that it is unlikely that a court will find that a digital signature constitutes a signature for the purpose of the Statute of Frauds writing requirement.

In conclusion, under the Electronic Transaction Act 1999 (Cth) digital signatures used in transactions governed by Commonwealth law will be accorded the same legal status as paper-based signatures. If the Electronic Framework Bill (Vic) is enacted, digital signatures used in transactions governed by Victorian law will also be accorded the same legal status as paper-based signatures. It is doubtful whether digital signatures constitute signatures for the purpose of the Statute of Frauds writing requirement at common law.

5.4.2.3 Law reform proposal of Australian Securities Investment Commission

It is interesting to note that the Australian Securities Investment Commission in a *Response* submitted to the *Report of the Parliamentary Joint Committee Inquiry into Global Electronic Capital Raising and Share Trading* entitled *Issues Paper-Virtually no Liability: Securities Markets in an Electronic Age*, recommended that the "signature" requirements be removed from [the Statute of Frauds] legislation, and replaced with an "authentication" provision[549]. To date, this recommendation has not been taken up in any Australian jurisdiction. As noted earlier in this chapter, the Commonwealth has passed legislation and the Victorian government has put forward

---

[549] Australian Securities Commission, *Issues Paper-Virtually no Liability: Securities Markets in an Electronic Age* 1997, p 23, para 4.1, http://www.asic.gov.au.

a bill that accords functional equivalence to electronic signatures rather than eliminate the signature requirements from the Statute of Frauds legislation.

5.4.2.4 The extent to which the UN Convention on Contracts for the International Sale of Goods 1980 applies

It is relevant to note also the effect of the United Nations Convention on Contracts for the International Sale of Goods 1980 **("CISG Convention")** whose provisions have been adopted as law in each State and Territory[550]. Under Australian law, the provisions of the CISG Convention operate in relation to *the sales of goods* by Australian businesses to customers in countries who have adopted the Vienna Convention. Article 11 of the CISG Convention effectively overrides the Statute of Frauds writing requirement. Article 11 of the Vienna Convention provides:

> A contract of sale need not be concluded in or evidenced by writing and is not subject to any other requirement as to form. It may be proved by any means, including witnesses.

The operation of Article 11 (and for that matter the entire CISG Convention) is limited in that it does not apply to consumer sales, that is sales of goods bought for personal, family or household use unless the seller, at anytime before or at the conclusion of the contract, neither knew nor ought to have known that the goods were brought for personal family or household use[551]. Nor does the CISG Convention

---

[550] See, for example, ACT: Sale of Goods (Vienna Convention) Act 1987; NSW: Sale of Goods (Vienna Convention) Act 1986; Vic: Sale of Goods (Vienna Convention) Act 1987; WA: Sale of Goods (Vienna Convention) Act 1986; Qld: Sale of Goods (Vienna Convention) Act 1986; Tas: Sale of Goods (Vienna Convention) Act 1987; SA: Sale of Goods (Vienna Convention) Act 1986; NT: Sale of Goods (Vienna Convention) Act 1987.

[551] Article 2(a) of the United Nations Convention on Contracts for the International Sale of Goods.

apply to sale of goods by auction[552], sale of goods by authority of law[553], sale of securities or money[554], sale of ships, vessels, hovercraft, aircraft, and electricity[555], sale of goods to be produced or manufactured where the party ordering the goods undertakes to supply a substantial part of the materials, or where the main obligation of the supplier consists in supplying labour or other services[556]. Also, provision (Article 96) is made in the Vienna Convention for countries who have adopted the Vienna Convention to exclude the operation of Article 11 by making a declaration to that effect. To date, no Australian State or Territory has made such a declaration. Also, the operation of the Vienna Convention can be expressly excluded by the parties whose transaction is governed by the Vienna Convention.

Thus, where an Australian business conducts Internet commerce with an overseas party whose country has adopted the Vienna Convention, and where such business constitutes a non-consumer sale, the Statute of Frauds writing requirement will not apply unless the Vienna Convention has been expressly excluded by the parties or by the country of the customer with whom the business is transacting (pursuant to Article 96).

5.4.2.5 Conclusions about the likelihood of risk

In conclusion, the instances in which a business's Internet transactions are subject to the Statute of Frauds writing requirement and cannot satisfy one of the alternative

---

552 Article 2(b) of the United Nations Convention on Contracts for the International Sale of Goods.
553 Article 2(c) of the United Nations Convention on Contracts for the International Sale of Goods.
554 Article 2(d) of the United Nations Convention on Contracts for the International Sale of Goods.
555 Article 2(e)-(f) of the United Nations Convention on Contracts for the International Sale of Goods.

means for satisfying the relevant Sale of Goods provisions will be limited. It should be also noted that where an Australian business conducts Internet commerce with an overseas party whose country has adopted the Vienna Convention, and where such business constitutes a non-consumer sale, the Statute of Frauds writing requirement will not generally apply. Further, in relation to those Internet transactions that are subject to the Statute of Frauds writing requirement, but do not fall within one of the alternative means for satisfying the relevant Sale of Goods provisions, it is argued that it is open to the courts to draw upon analogous case law to conclude that an Internet transaction can nevertheless satisfy the two elements of the Statute of Frauds writing requirement, that there be a memorandum on which is written the material terms of the contract and that the memorandum is signed. In addition, the Commonwealth Electronic Transactions Act 1999 (Cth) and the Victorian Electronic Commerce Framework Bill (Vic), if enacted, largely facilitate the courts making such an interpretation in relation to transactions governed by Commonwealth and Victorian law as both the Commonwealth Electronic Transactions Act 1999 (Cth) and the Victorian Electronic Commerce Framework Bill (Vic) effectively provide that a document that is in electronic form will have the same legal effect as a paper-based document and that a document signed electronically will have the same legal effect as a paper-based signature.

There will, nevertheless, be Internet transactions for which it is necessary to make various arguments based on analogous case law, such as that a memorandum can be

---

[556] Article 3 of the United Nations Convention on Contracts for the International Sale of Goods.

comprised partially of text or selections that were selected by a customer from the business's web page and partially of text or formatting that is reconstituted by the business's Internet commerce software application after the contract; or that a memorandum can be comprised of a series of linked Internet communications; or that a typed signature constitutes a signature for the purposes of the Statute of Frauds writing requirement; or that a "facsimile" signature should constitute a signature for the purposes of the Statute of Frauds writing requirement. These propositions have yet to be tested in the courts.

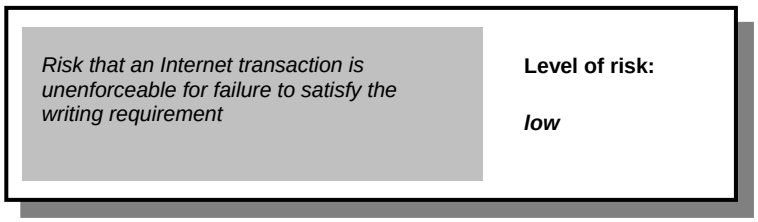
Moreover, it should be noted that, in practice, businesses conducting Internet commerce (at least those businesses conducting Internet commerce with consumers) tend to perform their obligations under an Internet transaction only after payment from the customer has been authenticated. In these circumstances a business is unlikely to be in a position where it seeks to enforce an Internet transaction. This seemingly obviates the need to consider whether the Statute of Frauds writing requirement can be satisfied in the context of Internet commerce. Business-to-business Internet transactions, however, may be different. Overall it is estimated that, given the limited circumstances in which a business conducting Internet commerce will be subject to the Statute of Frauds writing requirement, the likelihood of this risk eventuating for most businesses conducting Internet commerce is *unlikely*.

5.4.3 LEVEL OF RISK

The *level* of this legal risk, as concluded in the discussion that follows, is depicted in

Figure 10:

Figure 10 EVALUATION OF LEVEL OF RISK



The discussion at 5.4.1 at p243 led to the conclusion that the *consequence* of the Statute of Frauds risk was *low*. This assessment was based on the assumption set out and justified earlier that the consequence of such risk would threaten the efficiency or effectiveness of a business's Internet commerce but that the consequence could be dealt with internally.

The *likelihood* of this risk eventuating was assessed at 5.4.2 (starting at p 245) as being *unlikely* for several reasons including that the instances in which a business's Internet transactions would be subject to the Statute of Frauds writing requirement could often be satisfied under one of the alternative means for satisfying the relevant Sale of Goods provisions. Also, in relation to those Internet transactions that are subject to the Statute of Frauds writing requirement, but do not fall within one of the alternative means for satisfying the relevant Sale of Goods provisions, it is open to the courts to draw upon analogous case law to conclude that an Internet transaction

can nevertheless satisfy the two elements of the Statute of Frauds writing requirement.

As the *consequence* of this risk eventuating is assumed to be *low*, and the *likelihood* is *unlikely*, the level of this risk is *low*.

The evaluation of this legal risk is depicted in table form Table 63 at p426.

5.4.4 SOME RISK MANAGEMENT STRATEGIES

Before evaluating what risk management strategies are appropriate a discussion of what risk management strategies are available is necessary. Several *risk control* and *risk financing* strategies exist for managing this legal risk:

5.4.4.1 Risk control strategies

One *risk control* strategy is to record all communications transmitted by customers to the business relating to the terms on which the business has transacted with the customer, whether the Internet communications constitute text inputted by the customer into a form on the business's web page which is subsequently transmitted to the business, or e-mails from the customer to the business containing purchase order information. It is important that the business ensures that the records it keeps whether they constitute "linked" documents or a single document, contain the material terms of the contract. At the very least the following information should be included: the identity of the parties to the contact, the subject matter and the terms on which the parties have agreed to transact. In order to satisfy the Statute of Frauds writing requirement, not only the material terms of a contract must be specified in writing but also the signature of the party against whom a contract is sought to be enforced (from

a business's perspective the signature of the customer) is necessary. Accordingly, if a business's record management system is such that these elements are not recorded in one document (for example, the businesses records the text typed in by a customer into a form on the business's web page that includes the typed name of the customer which is then transmitted to the business, but the terms on which the parties have agreed to transact appear separately on the business's web page) then the business should also have in place a system that "links" the various elements of the Statute of Frauds writing requirement in order to ensure the courts will accept that an argument that the Statute of Frauds writing requirement is satisfied by virtue of several "linked" documents. Finally, it is important to note here that unless time stamping and other mechanisms are used to ensure integrity of the electronic records kept by the business it will be difficult from an evidential point of view for a business to prove that the Statute of Frauds writing requirement was satisfied. Guidance as to the standard the business should adopt in relation to storing and recording communications can be found from Section 12 of the Electronic Transactions Act 1999 (Cth) which sets out the standards for record retention that must be followed in order that an Internet communication can satisfy a requirement under a Commonwealth law to retain information. In addition, Article 10 of the UNCITRAL Model Law on Electronic Commerce specifies a standard that should be adopted where such records are required under law to be kept[557].

---

[557] *Electronic Commerce: Building the Legal Framework*, Report of the Electronic Commerce Expert Group to the Attorney-General, 31 March 1998, http://law.gov.au/aghome/advisory/eceg/ecegreport.html. See Recommendation 8.

If the business chooses to satisfy the signature element of the Statute of Frauds writing requirement by requiring customers to type in their name, a *risk control* strategy is for the business to make it clear at the time the customer is prompted to type in the customer's name that the typed name constitutes a signature.

In relation business-to-business transactions, particularly where there is an ongoing business relationship, an appropriate *risk control* strategy in respect of the signature element of the Statute of Frauds writing requirement may be for the business to require a customer to use electronic "facsimile" signatures such as PenOp to satisfy the signature element of the Statute of Frauds writing requirement. The use of electronic "facsimile" signatures is more appropriate in business-to-business transactions where a customer has an on-going relationship with the business as opposed to a one-off business-to-consumer Internet transaction given that to use electronic signatures both the customer and the business must invest in additional software and hardware.

Another *risk control* strategy in relation to the signature element of the Statute of Frauds writing requirement, is for a business to require its customers to use a digital signature. Given the additional cost to the customer (and for that matter to a business) involved with using digital signatures such risk management strategy is more appropriate for use in business-to-business Internet commerce where the value of the Internet transaction is high and the business has an ongoing trading relationship with its customer. Moreover, until digital signature legislation has been implemented in Australia that equates the legal effect of digital signatures with paper-based

signatures it is not recommended that a business use digital signatures to satisfy the signature element of the Statute of Frauds writing requirement as it is unlikely that at common law a digital signature constitutes a signature for the purposes of the Statute of Frauds writing requirement. A more detailed discussion of digital signatures and their use as a risk management strategy is discussed at 5.10 at p397.

If a business conducts Internet commerce with an overseas party whose country has adopted the Vienna Convention, the Statute of Frauds writing requirement will not apply unless the Vienna Convention has been expressly excluded or where the business transacts with consumers. It would nevertheless be prudent if, as a *risk control* strategy, the business stated in its terms of agreement that the transaction is subject to the Vienna Convention.

5.4.4.2 Risk financing strategies

A general *risk financing* strategy is risk retention. Internet transactions that are subject to the Statute of Frauds writing requirement are not rendered invalid if they do not satisfy the Statute of Frauds writing requirement. Rather, an affected Internet transaction is rendered unenforceable if the Statute of Frauds writing requirement is not complied with. For Internet transactions whose purchase price is low it may be cost effective for a business to elect to retain the risk that an Internet transaction it has entered into will be unenforceable in the event of a dispute (for example, by paying for losses as and when they arise or setting aside funds on an annual or regular basis to cover any losses arising from a risk that eventuates). Where the value of the transaction is high the appropriateness of the risk management strategy of retention

depends on whether the business could afford to retain any losses and this depends on the individual business's risk criteria.

Another *risk financing* strategy based on risk retention is to rely on the doctrines of part performance, estoppel and restitution. Each of these doctrines provides mechanisms for enforcing obligations in the absence of an enforceable contract. The principles governing the application of these doctrines are no different in the context of Internet commerce. Accordingly, it is not proposed to examine these doctrines in any detail. It is sufficient to comment that these doctrines have been used successfully to enforce obligations agreed to by transacting parties in circumstances where the Statute of Frauds writing requirement has not been satisfied. A business that conducts Internet commerce could therefore elect to take no additional steps to comply with the Statute of Frauds writing requirement in relation to Internet transactions that are affected by the Statute of Frauds writing requirement and instead choose to rely on the doctrines of estoppel, part performance or restitution should the situation arise that the business wishes to enforce the Internet transaction. Given that few Internet transactions will be affected by the Statute of Frauds writing requirement, it is arguably a reasonable risk management strategy to do nothing and take a risk that, if a dispute arises and it is necessary to take action to enforce an Internet transaction, the doctrines of estoppel, restitution and part performance can be relied on to render the Internet transaction enforceable.

5.4.5 EVALUATION OF RISK MANAGEMENT STRATEGIES

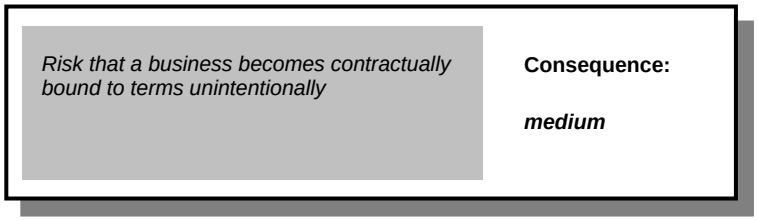
According to the risk management principles discussed at 2.4.4.4.1 at p102, because the *degree* of *consequence* and *likelihood* of this legal risk is *low* this risk should be managed through the risk financing strategy of risk retention. To retain this legal risk is also consistent with another guiding principle discussed at 2.4.4.4.4 at p107, which is that a business should only retain risks over which it has control. Moreover, given that the overall *level* of this risk is *low* and that there are no simple or cheap risk control or risk financing strategies it is suggested this legal risk falls into the category of risks which a business should regard as acceptable and therefore, in addition to retaining this legal risk, no risk treatment/risk minimisation at all is necessary. Should a business wish to treat this legal risk, no one risk management strategy stands out as the most suitable to implement. Rather, what risk management strategy to adopt will depend on factors particular to a business, such as the financial resources of the business and the value of the goods or services transacted online. Compared to the general legal risk criteria of a business conducting Internet commerce, this option arguably does not meet one of the legal risk objectives, that of protecting a business's legal rights and interests. In circumstances where the consequence of this risk is analysed as higher than the descriptor used here, then the business should treat or minimise this legal risk through implementation of one or more of the risk management strategies put forward above. The risk management strategies put forward and the recommended risk management strategies are set out in table form in Table 64 at p429.

5.5 Risk that a business becomes contractually bound to terms unintentionally

5.5.1 ANALYSIS OF THE CONSEQUENCE OF THE RISK EVENTUATING

The *consequence* of this legal risk, as concluded in the discussion that follows, is depicted in Figure 11:

Figure 11 EVALUATION OF THE CONSEQUENCE



The loss that a business would incur if this risk eventuated would be the cost associated with being contractually bound to an Internet transaction on terms that the business cannot or would rather not fulfil. In such circumstances, if the business failed to fulfil its contractual obligations the business would be liable for breach of contract. Under contract law, the measure of damages payable to a plaintiff for breach of contract is the amount of money necessary to place the innocent party (plaintiff) in the position he or she would have occupied if the contract had been performed[558]. Thus, where a business is selling products or services to a consumer through the Internet the amount of damages would, at the very least, be the cost to the consumer of obtaining the products or services purchased from the business elsewhere. Where a business is engaged in business-to-business Internet commerce the amount of

[558] *Robinson v Harman* (1848) 154 ER 363 per Parke B.

damages payable could be considerable as there is greater scope for a plaintiff to establish that, not only should the plaintiff should be compensated for having to obtain the business's services or products elsewhere, but that the plaintiff should be compensated for any losses incurred by the plaintiff resulting from the business's breach of contract, such as the plaintiff's inability to meet a deadline for a contract with a third party that relied on the defendant business meeting its contractual obligations.

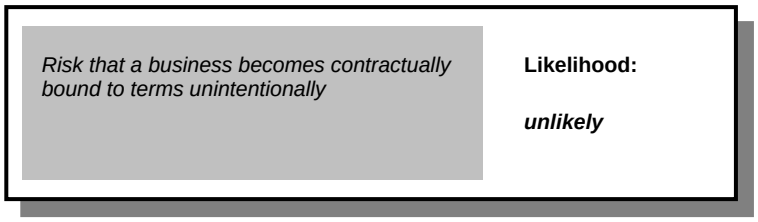
If, on the other hand a business performed its contractual obligations, the consequences if this risk eventuated would be that the business could incur loss, if to perform the contractual obligation was not profitable or resulted in reduced profits.

Providing a generic analysis of the consequence of this risk is difficult. It is suggested that the consequences discussed are unlikely to threaten the business's Internet commerce activities but would cause the business's Internet commerce activities to be subject to significant review or changed ways of operating. On a conservative analysis of the consequence of this risk, this risk constitutes a *medium* risk.

5.5.2 ANALYSIS OF THE LIKELIHOOD OF THE RISK EVENTUATING

The *likelihood* of this legal risk, as concluded in the discussion that follows, is depicted in Figure 12:

Figure 12 EVALUATION OF THE LIKELIHOOD



The risk that a business becomes contractually bound to terms unintentionally arises in five contexts in relation to Internet commerce:

- Where a business's marketing and promotional activities (whether through the web or by e-mail) constitutes making an "offer" rather than an "invitation to treat";
- Where a business's purported withdrawal of an "offer" to a customer is precluded because the business's "offer" has been accepted by a customer;
- Where during the course of negotiating the terms of an Internet transaction a "battle of the forms" situation arises such that a customer's terms override the business's;
- Where the terms of the contract negotiated between a business and a customer are altered by erroneous transmission;
- Where the business's computer software used for conducting Internet commerce is erroneously programmed or malfunctions so it makes or accepts offers in circumstances unauthorised by the business.

In order to determine the likelihood of risk it is necessary to consider these scenarios in some detail.

5.5.2.1 Where a business's marketing and promotional activities on the Internet constitute making an "offer" rather than an "invitation to treat"

A business risks being contractually bound to terms which it cannot or would prefer not to fulfil if it fails to take into account the legal distinction drawn between making "offers" and "invitations to treat" when undertaking its marketing and promotional activities on the Internet.

An "offer", in legal terms, is a proposal of the terms on which a business seeks to transact which, if accepted by a customer, will become *contractually binding* on the business. If a customer accepts an "offer" that is made on the Internet by a business (eg on a business's web site, through e-mail or on a bulletin board) the business will be contractually bound to the terms of that "offer". A business may therefore find that it is contractually bound to terms to which it would prefer not to be bound. For example, a business may find itself contractually bound to meet orders that, due to overwhelming demand, it cannot meet. Alternatively, where an "offer" is made on a business's web site, and the business fails to update its web site, the business may find itself contractually bound to sell a product or service at the out of date purchase price specified on the web site.

In contrast, the term "invitation to treat" refers to a proposal, which if responded to by a customer, is not contractually binding. Rather, an "invitation to treat" is an offer

to negotiate, or an offer to receive offers[559]. Thus, where a customer orders a business's goods or services in response to a business's "invitation to treat", the business is entitled to accept or reject the order.

Whether a business's marketing and promotional activities on the Internet constitute making an "offer" or an "invitation to treat" is determined by examining the objective intention of the business's conduct[560]. Thus, a business will be considered to have made an "offer" if a reasonable person would believe that an "offer" was being made. Such "offer" will be contractually binding on a business if a customer responds to it with a genuine belief that the business has made an "offer".

It is likely that the courts will apply the principles regulating analogous off-line activities when determining whether a business's marketing and promotional activities on the Internet constitute making an "offer" or an "invitation to treat". Thus, if a business's efforts at soliciting commerce on the Internet is analogous to the issue of circulars and general advertisements (*Spencer v Harding* (1870) LR 5 CP 561; *Re Mount Tomah Blue Metals Ltd* (in liq) [1963] ALR 346) or a display of a business's goods in a store (*Pharmaceutical Society of Great Britain v. Boots Cash Chemists (Southern) Ltd* [1953] 1 QB 401), it is probable that such activity will constitute making "invitations to treat".

It should be noted, however, that it does not ensue that every brochure and catalogue, or a display of goods constitutes making an "invitation to treat". It is still

---

559 *Carlill v. Carbolic Smoke Ball Co*, [1893] 2 QB 484.

560 JG Starke QC, NC Seddon, MP Ellinghaus, *Cheshire and Fifoot's Law of Contract*, 6th Australian Edition, Butterworths, Sydney 1992, Ch 1, p 54, para 109.

relevant to examine the objective intention of a business's conduct. Thus, in the classic case of *Carlill v Carbolic Smoke Ball Co* [1893] 1 QB 256 it was held that whilst, in general, brochures and advertisements constitute "invitations to treat" they could constitute "offers" if to a "reasonable man" they signified an intention to be contractually bound should a customer respond to them by purchasing the goods (or services) advertised.

Thus, a business's activities on the Internet, whether they be by means of a web page, or by e-mail, will constitute making an "offer" if those activities would appear to a reasonable person to signify an intention to be contractually bound if a customer responds. Accordingly, text in a business's web page or e-mail that states, for example, that the first two thousand sales of a business's goods or services will enjoy a discount of 25% will probably constitute an offer. On the other hand, the fact that a business's web page or e-mail uses the word 'offer' does not necessarily mean that the business is making an "offer" as the use of the word 'offer' is not conclusive[561].

Under the United Nations Convention on Contracts for the International Sale of Goods 1980 **("CISG Convention")**, whose provisions have been adopted as law in each State and Territory[562], there is a presumption under Article 14(2) that when a business solicits commerce from unspecified customers such activity is considered to constitute an invitation to treat. Thus, in relation to Internet transactions governed by

---

561 Starke, Seddon, Ellinghaus, para 109.

562 See, for example, ACT: Sale of Goods (Vienna Convention) Act 1987; NSW: Sale of Goods (Vienna Convention) Act 1986; Vic: Sale of Goods (Vienna Convention) Act 1987; WA: Sale of Goods (Vienna Convention) Act 1986; Qld: Sale of Goods (Vienna Convention) Act 1986; Tas: Sale of Goods (Vienna Convention) Act 1987; SA: Sale of Goods (Vienna Convention) Act 1986;

the CISG Convention (basically transactions with customers in countries who have adopted the Vienna Convention) a business's activities on the Internet are likely to be presumed to be invitations to treat.

It is difficult to definitively state here what the likelihood of this scenario eventuating is. It is concluded here that this scenario could eventuate at some time and this corresponds with the descriptor *unlikely*.

5.5.2.2 Where a business's purported withdrawal of an "offer" to a customer is precluded because the business's "offer" has been accepted by a customer

Where a business's marketing and promotional activities (whether by means of e-mail or a web site) constitute the making of an "offer" in legal terms, a business is entitled at law to withdraw its "offer" at any time up until acceptance of the "offer" by a customer. Depending on whether the postal rule applies to acceptances made on the Internet, however, a business may find that it is precluded from withdrawing its "offer" because the "offer" has been accepted by a customer, even when the customer's acceptance has not actually been received by the business (eg. the customer e-mailed an acceptance, but due to a delay occurring during transmission the acceptance of a business's "offer" was not actually received by the business at the time the business sought to withdraw its "offer").

The general principle governing the calculation of the time at which an acceptance takes place is that acceptance takes place when it is *actually* received by party that makes the "offer". Where acceptance is made by post, however, the general rule is

---

NT: Sale of Goods (Vienna Convention) Act 1987.

replaced with the postal rule. The postal rule provides that acceptance will be deemed to have taken place at the time the acceptance is posted. How the courts will characterise the communication of an acceptance through the Internet will determine a business's exposure to the risk that it cannot withdraw an "offer" it has made to a customer even though the customer's acceptance has not actually been received. If the postal rule applies to acceptances communicated through the Internet a business would be precluded from withdrawing its "offer" once a customer had communicated acceptance of the business's "offer" even if the acceptance had been lost during transmission[563]. Later in this chapter at 5.6.2 (at p335), the arguments for and against the application of the postal rule to acceptances made through the Internet are considered. It is relevant here to note that the conclusion drawn in the later discussion is that it is unlikely that the postal rule applies to acceptances made through the Internet.

5.5.2.3 Effect of Article 15 of the UNCITRAL Model Law on Electronic Commerce and Commonwealth and proposed Victorian legislation

It should be noted that Article 15 of the UNCITRAL Model Law on Electronic Commerce lays down some rules for determining when an Internet communication is deemed to be received[564]. It follows that in jurisdictions where Article 15 of the

---

563 Under the postal rule the posting of an acceptance constitutes an effective acceptance even if the message never arrives: *Household Fire & Carriage Accident Insurance Co Ltd v. Grant* (1879) 4 Ex D 216*; Georgoulis v Mandelinic* [1984] 1 NSWLR 612 at 616.

564 *Article 15. Time and place of dispatch and receipt of data messages*
(1) Unless otherwise agreed between the originator and the addressee, the dispatch of a data message occurs when it enters an information system outside the control of the originator or of the person who sent the data message on behalf of the originator.

Model Law on Electronic Commerce has been legislatively implemented, the time at which an acceptance communicated through the Internet is received would be determined by reference to the rules set out in Article 15. The point at time an Internet communication is deemed to be received depends on whether a business has a 'designated information system for the purpose of receiving data messages'. In instances where a business has such a system, an Internet communication is deemed to be received at the time when it enters the designated information system[565]. If an Internet communication is sent to the information system of a business which is not the designated information system, receipt of an Internet communication is deemed to have taken place when the Internet communication is retrieved by the business[566]. Where a business doesn't have a designated information system, receipt is deemed to

---

(2) Unless otherwise agreed between the originator and the addressee, the time of receipt of a data message is determined as follows:
  (a) if the addressee has designated an information system for the purpose of receiving data messages, receipt occurs:
    (i) at the time when the data message enters the designated information system; or
    (ii) if the data message is sent to an information system of the addressee that is not the designated information system at the time when the data message is retrieved by the addressee;
  (b) if the addressee has not designated an information system, receipt occurs when the data message enters an information system of the addressee.
(3) Paragraph (2) applies notwithstanding that the place where the information system is located may be different from the place where the data message is deemed to be received under paragraph (4).
(4) Unless otherwise agreed between the originator and the addressee, a data message is deemed to be dispatched at the place where the originator has its place of business, and is deemed to be received at the place where the addressee has its place of business. For the purposes of this paragraph:
  (a) if the originator or the addressee has more than one place of business, the place of business is that which has the closest relationship to the underlying transaction or, where there is no underlying transaction, the principal place of business;
  (b) if the originator or the addressee does not have a place of business, reference is to be made to its habitual residence.
(5) The provisions of this article do not apply to the following: [...].

[565] Article 15 (a)(iii) UNCITRAL Model Law on Electronic Commerce.

take place when the Internet communication enters the information system of the business[567].

The UNCITRAL Model Law on Electronic Commerce has not been legislatively incorporated into Australian law. The Electronic Commerce Expert Group rejected the approach taken in Article 15 of the UNCITRAL Model Law. Rather, the Electronic Commerce Expert Group Report states that any legislative attempt to specify when an Internet communication is deemed to be received should be based on "the recipient's ability to retrieve the information and, as a fall back position, upon the information coming to the attention of the recipient"[568]. In addition, the report also notes that if transacting parties are located in different time zones, a situation may arise where an Internet communication is deemed to be received by a party before the time it was sent. The Electronic Commerce Expert Group concluded that all time should be referenced to Universal Time/Greenwich Mean Time although the resulting Electronic Transactions Act 1999 (Cth) does not adopt this recommendation.

The time and place of receipt and, in addition, for dispatch, of an Internet communication governed by Commonwealth law is now regulated by section 14 of

---

566 Article 15 (a)(ii) UNCITRAL Model Law on Electronic Commerce.

567 Article 15 (b) UNCITRAL Model Law on Electronic Commerce. The accompanying Guide to the Enactment of the UNCITRAL Model Law on Electronic Commerce 1996 at para 2.14.4 provides that an Internet communication "enters" an information system at the time when it becomes available for processing within that information system.

568 *Electronic Commerce: Building the Legal Framework*, Report of the Electronic Commerce Expert Group to the Attorney-General, 31 March 1998, http://law.gov.au/aghome/advisory/eceg/ecegreport.html. See Recommendation 14.

the Electronic Transactions Act 1999 (Cth)[569]. In relation to an acceptance communicated through the Internet, section 14 provides that acceptance would not be

---

[569] Section 14 of the Electronic Transactions Act 1999 (Cth) provides:
14 Time and place of dispatch and receipt of electronic communications
Time of dispatch
(1) For the purposes of a law of the Commonwealth, if an electronic communication enters a single information system outside the control of the sender, then, unless otherwise agreed between the sender and the recipient of the electronic communication, the dispatch of the electronic communication occurs when it enters that information system.
(2) For the purposes of a law of the Commonwealth, if an electronic communication enters successively 2 or more information systems outside the control of the sender, then, unless otherwise agreed between the sender and the recipient of the electronic communication, the dispatch of the electronic communication occurs when it enters the first of those information systems.
Time of receipt
(3) For the purposes of a law of the Commonwealth, if the recipient of an electronic communication has designated an information system for the purpose of receiving electronic communications, then, unless otherwise agreed between the sender and the recipient of the electronic communication, the time of receipt of the electronic communication is the time when the electronic communication enters that information system.
(4) For the purposes of a law of the Commonwealth, if the recipient of an electronic communication has not designated an information system for the purpose of receiving electronic communications, then, unless otherwise agreed between the sender and the recipient of the electronic communication, the time of receipt of the electronic communication is the time when the electronic communication comes to the attention of the recipient.
Place of dispatch and receipt
(5) For the purposes of a law of the Commonwealth, unless otherwise agreed between the sender and the recipient of an electronic communication:
(a) the electronic communication is taken to have been dispatched at the place where the sender has its place of business; and
(b) the electronic communication is taken to have been received at the place where the recipient has its place of business.
(6) For the purposes of the application of subsection (5) to an electronic communication:
(a) if the sender or recipient has more than one place of business, and one of those places has a closer relationship to the underlying transaction—it is to be assumed that that place of business is the sender's or recipient's only place of business; and
(b) if the sender or recipient has more than one place of business, but paragraph (a) does not apply—it is to be assumed that the sender's or recipient's principal place of business is the sender's or recipient's only place of business; and
(c) if the sender or recipient does not have a place of business—it is to be assumed that the sender's or recipient's place of business is the place where the sender or recipient ordinarily resides.
Exemptions
(7) The regulations may provide that this section does not apply to a specified electronic communication.
(8) The regulations may provide that this section does not apply to a specified law of the Commonwealth.

deemed to have taken place until acceptance was actually received by the business's computer system (that is, the Internet communication containing the acceptance had actually entered the computer system of the business that was used or designated for the purpose of receiving Internet communications) or that the Internet communication came to the attention of the business. Thus, the risk that a business's purported withdrawal of an "offer" to a customer is precluded because the business's "offer" had been "accepted" (but not actually received by the business) could not arise.

In contrast, clause 7(3) of the Electronic Commerce Framework Bill (Vic), which introduces presumptions in relation to the time of sending and receipt of an Internet communication, takes an approach more like Article 15 of the UNCITRAL Model Law on Electronic Commerce, although no distinction is made between circumstances where a party has designated an information system to receive Internet communications and where a party has not designated a particular information system[570]. Should the Electronic Commerce Framework Bill (Vic) be passed, it is unlikely that, in relation to Internet transactions governed by Victorian law, this risk would eventuate, as acceptance would not be deemed to have taken place until it had entered a computer system under the control of the business (that is, the Internet

---

[570] Clause 7(3) of the Electronic Commerce Framework Bill (Vic) provides:

(3) A document being delivered electronically to a person or body—

(a) must be taken to have been sent when the electronic communication by which the document is sent leaves an information system under the control of the sender; and

(b) must be taken to have been received when the electronic communication by which the document is received enters an information system under the control of the recipient—

unless the contrary is proved or it is otherwise agreed between the sender and the recipient.

communication containing the acceptance had actually entered the computer system of the business).

To conclude, if a business's marketing and promotional activities on the Internet cannot be construed as making an offer this fact situation will never arise. However, as noted earlier, it is possible that a business's marketing and promotional activities on the Internet could constitute the making of an "offer". It is suggested here that the postal rule does not apply to Internet communications. Therefore a scenario where a withdrawal of an "offer" to a customer is precluded because the business's "offer" has been accepted by a customer is not likely to arise. Further, in relation to transactions governed by the Commonwealth Electronic Transactions Act 1999 (Cth) and the Commerce Framework Bill (Vic), if enacted, the effect will be that the postal rule will certainly not apply to transactions governed by such legislation. It is concluded therefore that the likelihood of this fact situation eventuating is *rare*, that is the scenario would eventuate only in exceptional circumstances.

5.5.2.4 Where during the course of negotiating the terms of an Internet transaction a "battle of the forms" situation arises such that a customer's terms override those of the business

The term "battle of the forms" refers to a situation that occurs when an offer to do business made by one party, on terms often printed on a form provided by that party, is purportedly accepted by the other party subject to qualifications, also often manifested in a form, but whose effect in law is to reject the first party's offer and to replace the first party's offer with a counter-offer. In effect, the relationship between the parties is reversed so that the second party becomes the party who is offering to

do business, which the first party can elect to accept or reject[571]. A situation can occur, in such circumstances, where the parties believe that a contract has been formed whereas according to law there is no contract; rather the existence of two offers. Where however, the parties have proceeded to do business with each other even though their exchanges indicate conflicting views of the terms of the contract, the courts have inferred that acceptance was made by conduct[572] and accordingly the terms of that contract reflect the terms put forward in the last counter-offer: *Butler Machine Tool Co Ltd v Ex-Cell-O Corp (England Ltd)* [1979] 1 WLR 401. The courts have held, however, that the rule that an acceptance that does not reflect an offer constitutes a counter-offer does not apply where the purported acceptance reflects simply a paraphrase of the terms made in the offer[573].

It should be noted that where a business contracts with an overseas customer whose country has adopted the United Nations Convention on Contracts for the International Sale of Goods, the opportunities for a "battle of the forms to arise" are limited in relation to contracts for the sale of goods. Article 19 of CISG, which all States and Territories have adopted[574], and which applies to all non-consumer sales of *goods* by Australian businesses to customers whose country has adopted the CISG, provides that an acceptance that modifies the terms of an offer of a customer will not constitute a counter-offer, provided that the qualifications of the second party do not materially alter the offer. Under the CISG, terms that alter the terms of an offer

---

[571] See for example, *Hyde v Wrench* (1840) 3 Beav 334.
[572] See for example, *Brogden v Metropolitan Railway Co* (1877) 2 App Cas 666.
[573] *Cavallari v Premier Refrigeration Co Pty Ltd* (1952) 85 CLR 20.

materially include terms relating to the 'price, payment, quality and quantity of the goods, place and time of delivery, extent of one party's liability to the other or the settlement of disputes'[575]. The rule set out in Article 19 is subject to the right of the first party to object to such an acceptance[576]. Where no objection is made by the first party the terms of the contract include the terms set out in the first party's offer and the modifications contained in the acceptance[577].

In conclusion, a 'battle of the forms' type situation is conceivable in the context of Internet commerce in relation to business-to-business Internet transactions. Internet transactions between businesses are more likely to involve negotiations as to terms than Internet transactions between a business and consumers, which are commonly conducted solely on the terms of the business. This scenario is therefore categorised as *unlikely* that is, it could eventuate at some time.

5.5.2.5 Where the terms of the contract negotiated between the business and a customer are altered by erroneous transmission

It is possible that during the course of negotiations conducted through the Internet that one party makes an "offer" to another and the terms made in the "offer" are altered due to erroneous transmission. For example, an "offer" made by a business by means of e-mail to a customer may be altered due to an erroneous transmission of the e-mail (this could occur due to malfunction in the e-mail software or due to breakdown of transmission on the Internet). A situation could arise where an altered

---

574 Article 2 of the United Nations Convention on Contracts for the International Sale of Goods.
575 Article 19(3), United Nations Convention on Contracts for the International Sale of Goods**.**
576 Article 19(2), United Nations Convention on Contracts for the International Sale of Goods.

message received by a customer is nevertheless comprehensible as an "offer" and is consequently accepted by the customer in the belief that it represents the business's "offer". This raises the question: would a business in such circumstances be contractually bound to the altered terms? Should such circumstances arise, the situation could be characterised by the courts as a mutual mistake. That is, the courts would find that each party was mistaken about the other's intention, with neither realising that the other was mistaken[578]. In determining whether a contract has been formed in such circumstances, the courts will apply an objective test, by enquiring whether a reasonable observer would have concluded that the party against whom the contract is sought to be enforced had intended to enter into the Internet transaction on those terms claimed by the party seeking to enforce the contract. It is likely that in such circumstances the courts would find that there is no contract because there is no acceptance of what is offered.

In conclusion, this risk will only ever arise where a business conducts negotiations with its customers as to the terms on which it is prepared to transact. Many Internet transactions are conducted solely on terms specified by the business such as in instances where a business displays or provides a hypertext link to its terms on a web page or where a business e-mails its customer the terms on which it is prepared to transact, on the basis that failure to agree to such terms will result in the business refusing to transact with the customer. In addition, the erroneously altered

---

577 Article 19(2), United Nations Convention on Contracts for the International Sale of Goods.

578 JG Starke QC, NC Seddon, MP Ellinghaus, *Cheshire and Fifoot's Law of Contract*, 6th Australian Edition, Butterworths, Sydney 1992, Ch 6, p 313, para 645.

communication needs to have been altered in such as way as to appear to be making an intelligible "offer" to the receiving party. This fact situation seems unlikely to commonly arise and therefore is categorised as *rare*. That is, the fact situation would eventuate only in exceptional circumstances.

5.5.2.6 Where a business's computer software used for conducting Internet commerce is erroneously programmed or malfunctions so it makes or accepts offers in circumstances unauthorised by the business.

Typically, the computer software used by businesses to conduct Internet commerce is pre-programmed to make or accept offers when certain circumstances occur such as when a customer has completed an on-line order form and provided payment details that have been authorised by the customer's card provider. If the computer software is incorrectly or erroneously programmed to make or accept offers in circumstances that have been unauthorised by the business, then the business faces the risk of being contractually bound to an Internet transaction to which it was not intended. It is possible that a business will be held contractually bound to any such Internet transactions that were entered into, notwithstanding the fact that the transaction was not authorised by the business, on the basis of agency principles. The New Zealand Law Commission Report on Electronic commerce suggested that an offer or acceptance made by a business's computer software is likely to be considered to constitute an offer made or accepted by an electronic agent of the business, which will be contractually binding on the business, provided that the offer or acceptance could be regarded as falling within the actual or ostensible authority of the

business[579]. There is however no legal authority (either statutory or case law) in Australia that expressly supports this proposition. The case law on theft or larceny involving cash that has been withdrawn from automatic teller machines (ATMs) is perhaps the closest the courts have come to considering whether an offer made or accepted by a computer software program is contractually binding on a business. In such cases the courts have chosen not to apply agency principles to transactions that involve a person effecting a bank withdrawal by way of an ATM. In *Kennison v Daire* (1986) 160 CLR 129 the High Court held that the fact that an ATM's computer software was programmed, when the ATM was offline, to allow withdrawal of cash by a party who did not have a current account with the bank did not amount to the bank consenting to such withdrawal. The High Court held at p 132 that:

> The fact that the Bank programmed the machine in a way that facilitated the commission of a fraud by a person holding a card did not mean that the Bank consented to the withdrawal of money by a person who had no account with the Bank. It is not suggested that any person, having the authority of the Bank to consent to the particular transaction, did so. The machine could not give the bank's consent in fact and there is no principle of law that require it to be treated as though it were a person with authority to decide and consent.[580]

Several subsequent cases have followed *Kennison v Daire*. Thus, it was held in *R v Evenett* (1987) 24 A Crim R 330 that the National Australia Bank had not consented to the defendant withdrawing funds from an ATM exceeding the amount in the defendant's account. The ATM was at the time "offline" and was programmed to allow the defendant in such circumstances to withdraw funds exceeding the amount

---

[579] Law Commission, "Electronic Commerce Part One- A guide for the Legal and Business Community", NZLC R50, October 1998, Wellington, New Zealand, pp 22-23, para 58.

in his account. The ATM was programmed to allow withdrawals up to $500 when it was "offline" regardless of the balance in account from which the withdrawal was being made. In *Ilich v The Queen* (1987) 162 CLR 110 Brennan J stated that the principle set out in *Kennison v Daire* was also applicable in a prosecution for theft under the Criminal Code.

So does the legal principle set out in the ATM cases apply to an offer made or accepted by a computer software program during the course of an Internet transaction a business? If it does a business will not be contractually bound if its computer software is erroneously programmed or malfunctions so it makes or accepts offers in circumstances unauthorised by the business. It seems reasonable to assume that the courts will be influenced by the ATM cases when deciding a case involving an offer or acceptance made by a computer software program. However, there are some arguments against following the approach taken in the ATM cases. The ATM cases involved criminal offences of either larceny or theft where the defendant intentionally set out to defraud a bank through the bank's ATM. It is submitted that an underlying policy factor in the ATM cases is the reluctance by the courts to allow a defendant to rely on a "technical" defence that the ATM authorised or consented on behalf of the bank to a withdrawal in circumstances where the defendant knew he was not entitled to such a withdrawal. In contrast, a customer transacting with a business on the Internet may not necessarily be aware that there is a programming error or malfunction which results in an offer or acceptance being made by the business's

---

[580] *Kennison v Daire* (1986) 160 CLR 129 at p 132.

computer software which is not intended by the business. Therefore there is an argument, at least where a customer did not have the intention to defraud the business by taking advantage of a known programming error of the business's computer software, that the principle set out in *Kennison v Daire* should not apply in such circumstances and that agency principles may well apply.

Also, it seems that the courts have not totally excluded the concept that a machine operated by computer software can act as an agent of the business that owns it. In *R v Baxter* 84 ALR 537, the Queensland Court of Criminal Appeal held that a party could be found guilty of making a false representation to the Commonwealth or a Commonwealth public authority in circumstances where the representation was not made directly to a person employed by the Commonwealth (or Commonwealth public authority) but to an ATM. In this case the appellant deposited forged cheques in several Commonwealth Bank accounts and withdrew money from these accounts by way of an ATM. The appellant was charged and convicted of several offences including making a false representation to a Commonwealth public authority. The false representation arose from the appellant using his plastic card and PIN in an ATM of the bank to obtain money to which he was not entitled. The Queensland Court of Criminal Appeal upheld this conviction rejecting the argument that a representation could not be made to a machine, namely an ATM, although the court did not expressly state that agency principles applied. However, by finding that the defendant did make a false representation to the Commonwealth Bank through the appellant's use of the bank's ATM surely this decision implies that agency principles

can and do apply to a transaction involving a machine operated by computer software.

It is therefore arguably premature to state conclusively that the principle in *Kennison v Daire* will govern offers or acceptances made by a business's computer software in the course of an Internet transaction. In other words there may well be circumstances where agency principles apply so as to make a business contractually bound to offers or acceptances made by the computer software of the business during the course of an Internet transaction. It is therefore necessary to consider what is the likelihood that a business's computer software is erroneously programmed or malfunctions so it makes or accepts offers in circumstances unauthorised by the business. It is difficult to definitively state what is the likelihood that a business's computer software used for conducting Internet commerce is erroneously programmed or malfunctions so it makes or accepts offers in circumstances unauthorised by the business. It seems reasonable to conclude that this fact situation would eventuate only in exceptional circumstances and therefore it should be categorised as *rare*.

5.5.3 SOME CONCLUSIONS ABOUT THE LIKELIHOOD OF RISK

Of the scenarios discussed above that could give rise to the risk that a business becomes contractually bound to terms unintentionally, two were categorised as *unlikely*: Where a business's marketing and promotional activities (whether through the web or by e-mail) constitutes making an "offer" rather than an "invitation to treat"; where during the course of negotiating the terms of an Internet transaction a

"battle of the forms" situation arises such that a customer's terms override those of the business.

The other three scenarios were categorised as *rare*: Where the terms of the contract negotiated between a business and a customer are altered by erroneous transmission; where the business's computer software used for conducting Internet commerce is erroneously programmed or malfunctions so it makes or accepts offers in circumstances unauthorised by the business; where a business's purported withdrawal of an "offer" to a customer is precluded because the business's "offer" has been accepted by a customer.

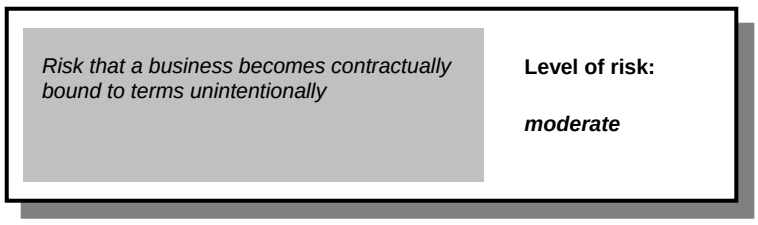
Taking a conservative approach the most appropriate descriptor for this legal risk is *unlikely*.

5.5.4 LEVEL OF RISK

The *level* of this legal risk, as concluded in the discussion that follows, is depicted in

Figure 13:

Figure 13 EVALUATION OF LEVEL OF RISK



As discussed at 5.5.1 (at p305) the *consequence* of the risk that a business becomes contractually bound to terms unintentionally depends on whether the business chooses to perform a contract it would rather not fulfil or to pay damages for breach of contract. On a conservative analysis of the consequence of this risk, this risk constitutes a *medium* risk.

The *likelihood* of this risk eventuating was assessed at 5.5.3 (at p325) as being *unlikely*.

As the consequence of this risk is *medium* and the likelihood of risk is *unlikely* the level of risk is *moderate*.

The evaluation of this legal risk is depicted in table form in Table 63 at p426.

5.5.5 SOME RISK MANAGEMENT STRATEGIES

The following risk management strategies could be used to manage this legal risk:

5.5.5.1 Where a business's marketing and promotional activities on the Internet constitute making an "offer" rather than an "invitation to treat"

The risk faced by a businesses of making "offers" instead of "invitations to treat", and as a result being bound to contractual terms which it cannot or would prefer not to fulfil, is a risk which a business can avoid quite simply by adopting the *risk control* technique of scrutinising its marketing and promotional activities on the Internet and ensuring that they cannot reasonably be understood as making "offers" unless it is so intended by the business.

5.5.5.2 Where a business's purported withdrawal of an "offer" to a customer is precluded because the business's "offer" has been accepted by a customer

A *risk control* strategy is the incorporation by a business of a contractual term that is based on Article 15(a)(ii) of the UNCITRAL Model Law on Electronic Commerce, such that acceptance of a business's "offer" is deemed to take place when the Internet communication accepting the business's offer is retrieved by the business (regardless of whether the business has a designated information system). This would minimise the risk that a business is precluded from withdrawing an offer notwithstanding that the business has not actually received communication of acceptance of its offer.

An alternative *risk control* strategy is for the business to include as a term of any transaction it enters into with its customers a term that reproduces or replicates a strategy used in relation to contracts effected through Electronic Data Interchange, in particular clause 10.2 of the Tradegate ECA Model EDI Trading Agreement. This clause effectively specifies that a transaction entered into by a business and a customer is governed by the instantaneous rule.

Electronic Data Interchange **("EDI")** is a procedure by which the computers of transacting parties can exchange standardised data. A common EDI use is inventory replacement whereby orders for stock are automatically generated by a business's computer to the computer of the business's supplier (often via a third party) according to the number of sales of the relevant stock made by the business. To ensure that the data exchanged through EDI is "readable" by the receiving computer, the data must be structured into a standardised form.

Parties intending to transact through EDI may choose to enter into a trading partner agreement. A trading partner agreement usually sets out the obligations of

each party and clarifies any legal uncertainties, including contractual uncertainties, that may be associated with contracting through EDI. Several model trading partner agreements have been developed by national and international bodies. Those provisions of the model trading partner agreements that clarify the contractual uncertainties associated with EDI may be suitable for adoption as risk management strategies by businesses conducting Internet commerce. For example, clause 10.2 of the Tradegate ECA Model EDI Trading Agreement (Short Form Agreement) provides that acceptance takes place when an EDI message constituting an offer is made available to the information system of the receiver:

> Unless otherwise agreed, a contract made by EDI will be considered to be concluded at the time and the place where the EDI message constituting the acceptance of an offer is made available to the information system of the receiver.

A clause such as this, that in effect applies the instantaneous communication rule to acceptances, if incorporated by a business conducting Internet commerce in its transactions with its customers, would minimise the risk that a business is precluded from withdrawing an offer notwithstanding that the business has not actually received communication of acceptance of its offer from the customer. This is because acceptance of a business's "offer" would be deemed to take place when a customer's acceptance of the business's offer is made available to the information system of the business and not when the acceptance is sent by a customer. Such term could be incorporated by a business e-mailing this term (and any other term that the business wishes to incorporate) to the customer with whom the business is transacting, or, if the business is conducting commerce on the web, the term could be displayed on the

business's web page. The principles governing incorporation of standard terms, discussed later in this chapter, would also need to be considered in order to ensure that such term is contractually binding on a customer.

It should be noted that whilst a risk management strategy may be to incorporate some provisions of EDI model trading partner agreements, the use of trading partner agreements themselves to incorporate these provisions are not, in general, suitable in the context of Internet commerce. The concept of trading partner agreements, which are signed off-line before parties begin transacting with each other, are not appropriate in the context of Internet commerce where a business is likely to seek to conduct commerce with customers with whom it does not necessarily have an ongoing trading relationship. Also, if trading partner agreements are required to be signed off-line this would introduce an element of delay and a business would risk losing potential customers by imposing a requirement to enter into a trading partner agreement in order to conduct Internet commerce with the business.

5.5.5.3 Where during the course of negotiating the terms of an Internet transaction a "battle of the forms" situation arises such that the customer's terms override the those of the business

A *risk control* strategy for a business affected by this risk is to refuse to transact with a customer except under the business's terms. For example, communication with a customer before the customer has signified acceptance of a business's terms (eg by clicking on a button or icon with the words "accept" on the business's web page containing the business's terms of business) could be avoided before an order can be made by a customer. This would eliminate the possibility of pre-existing "offers"

being made by a customer, giving rise to a battle of the forms situation. Alternatively, a customer can be prevented from completing an order (eg typing in or selecting order details from an order form on a web page that is then transmitted to the business) until the customer has signified acceptance of the business's terms (eg by clicking on a button to signify acceptance of the terms displayed on the business's web page), the rejection of which result in the customer being prevented from further progressing with the transaction.

In relation to business-to-business Internet commerce, where variations of terms are more likely to be sought by customers and acceded to by a business, a prudent *risk control* strategy is for the business to ensure that a mechanism is put in place such that if terms upon which the parties agree to transact can and are varied by a customer that subsequent to any variation accepted, a follow-up communication is transmitted to the customer confirming the varied term and reiterating all other terms on which the business is prepared to transact.

5.5.5.4 Where the terms of the contract negotiated between the business and a customer are altered by erroneous transmission

A *risk control* strategy is to require all customers' communications with the business to be "signed" with a digital signature. Digital signatures will be explained and discussed in more detail later in this chapter at 5.10 at p397. It is relevant here to note that their use provides a means for detecting whether an Internet communication received by a party differs from that which was transmitted by the party sending the Internet communication.

Another *risk control strategy* is for the business to incorporate as a contractual term with its customers a term that reproduces or at least replicate the effect of Article 13(5) of the UNCITRAL Model Law on Electronic Commerce. Article 13(5) of the UNCITRAL Model Law on Electronic Commerce specifically precludes reliance on an Internet communication received by a party where that party knew or should have known that the Internet communication was erroneous:

> Where a data message is that of the originator or is deemed to be that of the originator, or the addressee is entitled to act on that assumption, then, as between the originator and the addressee, the addressee is entitled to regard the data message as received as being what the originator intended to send, and to act on that assumption. The addressee is not so entitled when it knew or should have known, had it exercised reasonable care or used any agreed procedure, that the transmission resulted in any error in the data message as received.[581]

If a business incorporated terms in its transactions with its customers that had the same effect as Article 13(5) it would minimise the risk of the business being contractually bound to a term that was altered during transmission.

5.5.5.5 Where the business's computer software used for conducting Internet commerce is erroneously programmed or malfunctions so it makes or accepts offers in circumstances unauthorised by the business.

A *risk transfer* strategy is to outsource the production of the software used to conduct Internet commerce to a third party software developer or to purchase an off the shelf Internet commerce software package. Whilst this does not remove the risk that a business will be contractually bound to an Internet transaction on terms to

---

581 *UNCITRAL Model Law on Electronic Commerce*, Excerpt from the Report of the United Nations Commission on International Trade law on the work of its twenty-ninth session (28 May-14 June 1996) General Assembly, Fifty-first Session, Supplement No. 17 (A/51/17), http://www.un.or.at/uncitral/texts/electcom/ml-ec.htm#top.

which it did not intend to be bound by, the business may be able to recover the losses it has incurred as a consequence of wrongly programmed software from the third party developer, if the business ensures that a term of the software development or acquisition agreement provides for the recovery of losses incurred by the business as a consequence of an error or malfunction in the Internet commerce software. Furthermore, the business will need to ensure that it does not contract out its rights to sue for negligence in the event that the software is wrongly programmed.

Again the frequency of such risk arising can be minimised through using the *risk control* strategy of incorporating as a contractual term with all customers a term that reproduces or at least replicate the effect of Article 13(5) of the UNCITRAL Model Law on Electronic Commerce. As noted earlier, Article 13(5) precludes reliance by a party on an Internet communication received by the party which the party knew or ought to have known was erroneous.

5.5.6 EVALUATION OF RISK MANAGEMENT STRATEGIES

As discussed at 2.4.4.4.1 at p 102, one method for selecting which risk management strategy to implement is to examine the *degree* of *consequence* and *likelihood* of a given risk. As the consequence of this risk is *medium*, and the likelihood of this risk is *unlikely*, this risk is the type of risk that a business should retain and manage. To retain this legal risk is also consistent with another guiding principle discussed at 2.4.4.4.4 at p107, which is that a business should only retain risks over which it has control. In addition to retaining this legal risk, the business should consider implementing one or more of the strategies put forward in order to

minimise this legal risk. Compared to the general risk criteria of a business, employing some or all of the risk management strategies put forward will achieve the objective of reducing the liability to which the business is exposed as a consequence of conducting Internet commerce. So which risk management strategies should the business implement? Based on an assessment that implementation is not expensive and that implementation will significantly minimise this legal risk, a business should adopt all except two of the risk management strategies discussed. The two risk management strategies excepted are the use of digital signatures and the outsourcing of the production of the software used to conduct Internet commerce to a third party. It is not, however, suggested that these two risk management strategies are not cost effective. Rather, given that the implementation of these two strategies will involve a cost to the business, it will be necessary for a business to weigh the cost of implementing these two options against the benefits of implementing these strategies before deciding whether to adopt these risk management strategies. Depending on the circumstances of a particular business, it may or may not be appropriate to implement these two options.

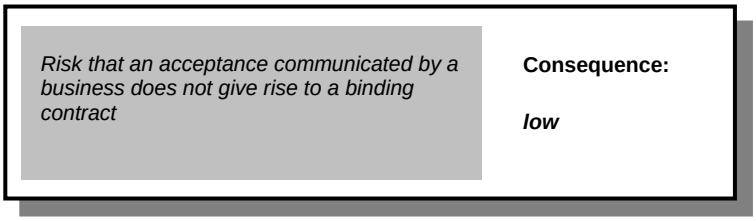
The risk management strategies put forward and the recommended risk management strategies are set out in table form in Table 64 at p429.

5.6 Risk that an acceptance communicated by a business does not give rise to a binding contract

5.6.1 ANALYSIS OF THE CONSEQUENCE OF THE RISK EVENTUATING

The *consequence* of this legal risk, as concluded in the discussion that follows, is depicted in Figure 14:

Figure 14 EVALUATION OF THE CONSEQUENCE

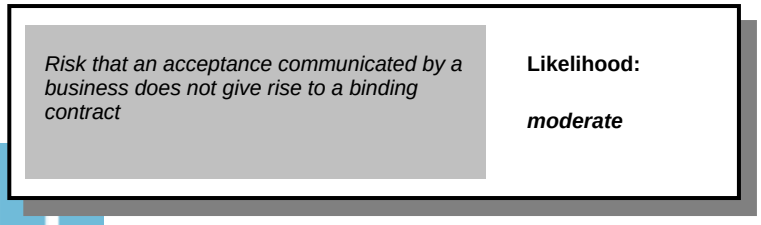


The loss that a business could incur should this risk eventuate is the cost to a business associated with losing a "sale" or "contract" as a consequence of a customer having withdrawn an "offer" made to the business. It is difficult to generalise here, as the value of a lost sale or contract will differ according to the product or service provided by a business. Again, this illustrates that legal risk management is more easily applied in relation to a specific business. Assuming that the loss of a sale will not have a more serious effect on a business than threatening the efficiency or effectiveness of the business's Internet commerce activities, this risk is categorised as having a *low* consequence.

5.6.2 ANALYSIS OF THE LIKELIHOOD OF THE RISK EVENTUATING

The *likelihood* of this legal risk, as concluded in the discussion that follows, is depicted in Figure 15:

Figure 15 EVALUATION OF THE LIKELIHOOD



It is accepted law in Australia that an "offer" can be withdrawn at any time up until it has been accepted. Earlier in this chapter at 5.5.2.1 p308 it was noted that a customer who seeks to transact with a business in response to a business's marketing and promotional activities on the Internet may, in some circumstances, be construed as making an "offer" in response to an "invitation to treat" of the business. In circumstances where a customer ordering a business's goods or services constitutes making an "offer", the customer is entitled to withdraw the "offer" at any time prior to acceptance of the "offer" by the business.

In the context of Internet commerce, if a customer sought to withdraw an "offer" it had made to a business, the customer would most likely communicate the withdrawal of the "offer" by e-mail to the business. Provided that the withdrawal of "offer" was communicated prior to acceptance of the "offer" by the business, such communication would relieve the "customer" from any obligation to go through with the purchase of a business's goods or services through the Internet.

Acceptances made by a business in the context of Internet commerce are likely to be effected either through conduct (for example, a business will accept a customer's "offer" by delivering the goods or services ordered by the customer) or through communicating acceptance to the customer through the Internet (such as by e-mail, or where the customer has ordered the business's goods or services from the business's

web site, a web page generated by the customer clicking on a button or hypertext to signify the customer's "offer" to transact with the business). Communicating through the Internet is not always perfect and it is not unusual for an Internet communication (whether by means of e-mail or on the web) to be delayed or even lost, even when the route the communication has taken is relatively uncomplicated:

> Assume that the gap between deemed despatch and deemed receipt is as narrow as possible. This could be because neither the offeree nor the offeror uses remote servers or intermediaries or because despatch is deemed to take place only at the departure of the message from the offeree's Internet access provider's server and receipt is deemed to be at the remote server of the offeror. It is still the case that there is as yet no guarantee when or if an e-mail will arrive. There is no certainty over the route of the e-mail or even that all of the e-mail will take the same route over the packet-switched network.[582] .

A situation could therefore arise where a business communicates its acceptance of a customer's "offer" through the Internet (either by e-mail or, through the business's web site) but, because its acceptance was delayed through transmission, the acceptance was not actually received by the customer prior to the transmission by the customer of a withdrawal of "offer". Whether a customer is nevertheless contractually bound to the Internet transaction depends on whether the postal rule governs acceptances made through the Internet.

The postal rule provides that where an acceptance is made by post, acceptance is effected at the time the acceptance is posted. If acceptances communicated through the Internet are governed by the postal rule, a business's acceptance of a customer's "offer" would be effective at the time the acceptance was communicated. The fact

---

582 Graham JH Smith et al, *Internet Law and Regulation,* A Specially Commissioned Report, FT Law

that the acceptance was delayed or not received by the customer would be irrelevant and a customer would be precluded from withdrawing the customer's "offer". The postal rule, however, does not usually apply when an acceptance is communicated through an instantaneous form of communication: *Brinkibon Ltd v. Stahag Stahl Und Stahlwarenhandelsgesellschaft Mbh* [1983] 2 AC 34[583]. In such instances, the acceptance is effected only when it has been received. Acceptances governed by the instantaneous rule include acceptances communicated by telex[584] and facsimile[585]. If the instantaneous communication rule were to apply in relation to Internet commerce, an acceptance communicated by a business by means of the business's web page would take place when it was displayed by the customer's web browser.

Presently only the Commonwealth has provided legislative guidance as to whether an acceptance communicated on the Internet is governed by the postal rule or the instantaneous communications rule and there is no case law that has directly considered this issue. As will be discussed in more detail below, s 14 of the Electronic Transactions Act 1999 (Cth) provides that the postal rule does not apply to Internet transactions governed by Commonwealth law. In relation to all other Internet transactions it is necessary to consider how the courts are likely to treat acceptances communicated through the Internet. Several arguments have been made in the

---

& Tax, London, 1996, Ch 8, p 99, para 8.2.2.

583 *Entores Ltd v Miles Far East Corp* [1955] 2 QB 327; *Brinkibon Ltd v Stahag Stahl Und Stahlwarenhandelsgesellschaft Mbh* [1983] 2 AC 34; *Express Airways v. Port Augusta Air Services* [1980] Qd R 543.

584 *Brinkibon Ltd v. Stahag Stahl Und Stahlwarenhandelsgesellschaft Mbh* [1983] 2 AC 34

literature for the postal rule to apply to acceptances communicated through the Internet, or at least to acceptances communicated by means of e-mail[586]. This view is based on the argument that an acceptance communicated through the Internet is more analogous to an acceptance made by letter than an acceptance communicated by means of an instantaneous form of communication, and therefore it is more appropriate for the postal rule to apply[587] at least in circumstances where the recipient has access to e-mail through an Internet service provider[588]. In other words, the argument is that e-mail is not instantaneous:

> Despite common belief, the process [of transmission of an e-mail] does not take place in a substantially instantaneous manner. Rather, it will typically take minutes, hours, or in some cases, days. Perhaps what creates confusion is the true substantial instantaneousness of intrasystem messages, which do not involve the Internet, or the occasional transmission of an Internet e-mail message in a substantially instantaneous manner. Or perhaps the cause of confusion is the substantially instantaneous nature of message transmission as the message passes through the wires themselves. But often overlooked are the "stops" that the message makes along the way, at the various servers and nodes that process it, breaking it up into pieces and reassembling it, or

---

585 *Reese Bros v Hamon-Sobelco* (1988) 5 BPR [97325], Court of Appeal (NSW) and *Wogen Resources Ltd v Just Australia China Holdings Ltd and Anor*, 22 November 1994, Supreme Court of Victoria, Commercial Division

586 See for example, Paul Fasciano, "Note: Internet Electronic Mail: A Last Bastion for the Mailbox Rule", 25 Hoftstra Law Review 971 and Heather Rowe, "Electronic Commerce: Legal Implications of consumer oriented electronic commerce" *Computer Law and Security Report*, vol 14 no 4 1998 232 at 236. See also Law Commission, "Electronic Commerce Part One- A guide for the Legal and Business Community", NZLC R50, October 1998, Wellington, New Zealand, p 28 para 71 in which it was advocated that the postal rule apply to acceptances made by e-mail where the e-mail is sent through an Internet Service Provider who receives the e-mail on behalf of the recipient but that the instantaneous rule apply where the recipient has a direct and immediate access to e-mail.

587 JG Starke QC, NC Seddon, MP Ellinghaus, *Cheshire and Fifoot's Law of Contract*, 6th Australian Edition, Butterworths, Sydney 1992, Ch 1, pp 82-83, para 140.

588 Interestingly, the Law Commission in, "Electronic Commerce Part One- A guide for the Legal and Business Community", NZLC R50, October 1998, Wellington, New Zealand, p 28 para 71 advocated that the instantaneous rule apply where the recipient has a direct and immediate access to e-mail but where the recipient has access to e-mail through an Internet service provider than the postal rule should apply because "…those using an ISP may only communicate as quickly as their telephone access, service provider and personal inclination dictate."

> redirecting it to a less congested portion of the Internet, or holding it until other messages are received, for a simultaneous, periodic dispatch. Further, one of the stops may be inoperative, causing the message to be delayed or never received at all[589].

The alternative view is that Internet communications, including e-mail should be subject to the laws governing instantaneous forms of communication. Notwithstanding the opposing view expressed, particularly in relation to e-mail, it is submitted that the instantaneous communication rule is the correct rule to apply in relation to acceptances communicated on the Internet. The reasons for this view are two pronged. Firstly, Internet communications are more like other forms of instantaneous communication (eg telexes and facsimiles) than communications conveyed by post. For example, the similarities between acceptances communicated on the Internet and acceptances communicated by means of facsimile machine are much greater than the similarities between acceptances communicated on the Internet and acceptances communicated by way of post (Both forms of communication are electronic and delivery is usually instantaneous although there are circumstances where delivery can be delayed due to technical problems or because the equipment for receiving a communication was not turned on or checked by the recipient.) However, it is acknowledged that this argument is harder to sustain in relation to Internet communications that take the form of e-mail where the recipient access e-mail through a third party Internet Service Provider, that is where the recipient does not have direct and continuous access to e-mail.

---

589 Fasciano, p 1001.

Secondly, even if technically some Internet communications, namely e-mails sent under certain circumstances, are not in nature instantaneous there are policy reasons for making all Internet communications subject to the instantaneous rule. The argument put forward by commentators in favour of the postal rule has only been raised in relation to e-mail. There has been no suggestion that the postal rule should apply to other forms of Internet communication such as a form on a business's web page. If the courts were to find that acceptances communicated by e-mail were subject to the postal rule but acceptances communicated through the web were subject to the instantaneous communication rule, an inconsistent outcome would arise. This would be particularly so if the New Zealand Law Commission approach were taken whereby e-mails received where the recipient had a direct and immediate access to e-mail would be governed by the instantaneous rule but e-mails where the recipient accessed e-mail through an Internet service provider would be governed by the postal rule. If such an approach reflected the law in Australia a situation could arise where:

- an acceptance communicated by a business on-line *through a web page* to a customer would take effect *only if actually received by a customer* and;
- an acceptance communicated by the business in the form of an *e-mail* to a customer who had *continuous and direct access* would take effect *only if actually received by a customer* ; **but**

- an acceptance communicated to a customer in the form of an *e-mail* where the *customer's access involved going through a third party Internet Service Provider* would take effect as soon as the business sent the message.

For reasons of consistency the instantaneous rule should be applied to all forms of Internet communication.

Furthermore, as indicated by Lord Wilberforce in *Brinkibon* and by Justice Cohen in the NSW Supreme Court case *NM Superannuation Pty Ltd v Baker* [1927] 7 ACSR 105 the instantaneous communication rule can accommodate instances where an acceptance has not been accessed by a recipient because, for example, the computer which accesses Internet communications was not switched on and logged into receive Internet communications. Lord Wilberforce in *Brinkibon* recognised that such instances could arise in the context of communications made by telex where actual delivery time was not instantaneous. He considered that the time at which acceptance takes place in such instances would depend on the intentions of the parties, by reference to business practices and in some cases a judgment as to where the risks should lie:

> The senders and recipients may not be the principals to the contemplated contract. They may be servants or agents with limited authority. The message may not reach, or be intended to reach, the designated recipient immediately: messages may be sent out of office hours, or at night, with the intention, or upon the assumption, that they will be read at a later time. There may be some error or default at the recipient's end which prevents receipt at the time contemplated and believed in by the sender. The message may have been sent and/or received through machines operated by third persons. And many other variations may occur. No universal rule can cover all such cases: they must be resolved by reference to the intentions of the parties, by sound

> business practice and in some cases by a judgment where the risks should lie.[590]

In *NM Superannuation Pty Ltd* which was concerned with the time at which a notice transmitted by means of facsimile machine was received, Justice Cohen took the view that although ordinarily receipt of a communication transmitted by facsimile will be taken to be at the time the communication was received by the recipient's facsimile machine, there may however be circumstances, such as where no person was able to receive the communication at the time the recipient's facsimile machine received the communication where this assumption will be displaced:

> In my opinion it is reasonable to assume that if a fax machine has been kept switched on then it is available for the purpose of receiving letters or other communications on it. That amounts to receipt by the trustee in that it had made and kept available the means of documents being received by it. In any case there is no reason why I should assume that the trustee through its employees or agents was not in its office at 5.22 pm on 30 June 1989 or on any other day in the ordinary course of its business. I cannot take judicial notice that people are not normally at work between 5 pm and 5.30 pm and there is no evidence which would suggest that the trustee through its representatives was not present at that time. It may well be in appropriate circumstances that evidence could be given that notwithstanding that a facsimile machine is left in operation there was nobody in the office to receive the messages until the following day but that is not the case here[591].

Accordingly, it is concluded that in the event of a dispute as to the time at which a customer received a business's acceptance the instantaneous rule should govern acceptances communicated through the Internet.

As for when an instantaneous communication is deemed to be received it is likely that the courts will be guided by Lord Wilberforce in *Brinkibon* and Justice Cohen in *NM Superannuation* and hold that, as with telexes and facsimiles, acceptance will

---

590 *Brinkibon Ltd v. Stahag Stahl Und Stahlwarenhandelsgesellschaft Mbh* [1983] 2 AC 34 at 42.

generally be deemed to have taken place at the time when the business's acceptance was received by the customer's equipment that receives Internet communications (for example, in relation to acceptances made by way of e-mail, the customer's e-mail server and in relation to web communications, the customer's web browser. Where an acceptance is communicated by e-mail and the customer's e-mail server is operated by a 3rd party such as an Internet Service Provider then acceptance would most likely take place at the time the customer's e-mail software application actually receives the e-mail). Only where a customer can bring evidence to prove that it was not possible, at the time the acceptance was received, for the customer to access the communication containing the business's acceptance, will a court consider deeming that acceptance took place at a later time.

5.6.2.1 Effect of Commonwealth Electronic Transactions Act 1999 and proposed Victorian legislation

As discussed at 5.5.2.3 at p312, section 14 of the Electronic Transactions Act 1999 (Cth) provides that the time of receipt of an Internet communication is, where the business has designated an information system for the purpose of receiving Internet communications, the time when the Internet communication enters that information system, unless otherwise agreed between the sender and the recipient of the Internet communication. Where the business has not designated an information system for the purpose of receiving Internet communications then, unless otherwise agreed between the sender and the recipient of the electronic communication, the time of receipt of

---

591 *NM Superannuation Pty Ltd v Baker* [1992] 7 ACSR 105 at 114-115.

the electronic communication is the time when the electronic communication comes to the attention of the recipient.

As discussed also at 5.5.2.3 at p312, clause 7(3) of the Electronic Commerce Framework Bill (Vic) which provides a presumption acceptance is deemed to have taken place when the Internet communication containing the acceptance it has entered a computer system under the control of the business (that is, the Internet communication containing the acceptance had actually entered the computer system of the business).

Thus, the postal rule does not apply to Internet transactions governed by Commonwealth law. Further, if the Electronic Commerce Framework Bill (Vic) is enacted, the postal rule will not apply to Internet transactions governed by Victorian law.

5.6.2.2 Effect of Article 18(2), United Nations Convention on Contracts for the International Sale of Goods 1980

It is relevant to note also the effect of the United Nations Convention on Contracts for the International Sale of Goods 1980 **("CISG Convention")** whose provisions have been adopted as law in each State and Territory[592]. As noted earlier at 5.4.2.4 at p294, under Australian law, the provisions of the CISG Convention operate in relation to *the sales of goods* by Australian businesses to customers in countries who have adopted the Vienna Convention. Article 18(2) of the CISG Convention

---

[592] See, for example, ACT: Sale of Goods (Vienna Convention) Act 1987; NSW: Sale of Goods (Vienna Convention) Act 1986; Vic: Sale of Goods (Vienna Convention) Act 1987; WA: Sale of Goods (Vienna Convention) Act 1986; Qld: Sale of Goods (Vienna Convention) Act 1986; Tas:

effectively provides that acceptance is received at the time it reaches the receiving party. In other words the postal rule does not apply to transactions governed by the CISG unless otherwise agreed by the transacting parties or there is usage or customer to that effect[593]. Article 24 also confirms that the postal rule does not apply in relation to acceptances governed by the CISG, providing that an acceptance is received when it is made orally to the recipient, at the time it was made, or when it is delivered *by any other means* to the recipient's place of business or mailing address or in the event of neither being present, the recipient's habitual residence.

5.6.2.3 Some conclusions about the likelihood of risk

As it is argued here that the receipt of acceptances communicated through the Internet are not governed by the postal rule, but rather the rule governing receipt of instantaneous communications, the likelihood of this risk eventuating is real. In fact, in relation to consumer Internet transactions that involve delivery by mail (as a period of delay between order and delivery exists), it is quite likely that a business will receive from customers a withdrawal of an offer to purchase the business's services or products. Whilst the likelihood that an Internet communication will be delayed cannot be predicted, it seems reasonable to assume that at some time a business would be faced with a situation where it accepted a customer's offer but is advised by the customer that the offer was withdrawn prior to the customer receiving the business's acceptance. This, in turn, could give rise to a situation where a business

---

Sale of Goods (Vienna Convention) Act 1987; SA: Sale of Goods (Vienna Convention) Act 1986; NT: Sale of Goods (Vienna Convention) Act 1987.

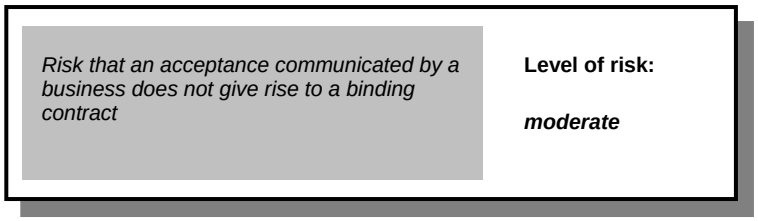
effects delivery of the goods or services ordered through the Internet by a customer to later find that the customer claims that the order was cancelled. Accordingly, this risk is categorised as *moderate*, that is, the risk should eventuate at some time.

5.6.3 LEVEL OF RISK

The *level* of this legal risk, as concluded in the discussion that follows, is depicted in

Figure 16:

Figure 16 EVALUATION OF LEVEL OF RISK



As noted at 5.6.1 (at p334) the consequence of the risk that an acceptance communicated by a business does not give rise to a binding contract will depend on the value of the Internet transaction. Without reference to a specific business it is possible only to suggest that the *consequence* of this risk eventuating is *low* on the basis that the consequences could threaten the efficiency or effectiveness of the business's Internet commerce activities but can be dealt with internally. The

---

593 Law Commission, "Electronic Commerce Part One- A guide for the Legal and Business

discussion at 5.6.2 (at p 335) of the *likelihood* of this risk eventuating concluded that this risk should eventuate at some time and therefore the risk was categorised as *moderate*. As this risk has been categorised as *low* in *consequence* and *moderate* in *likelihood* the level of risk is *moderate*.

The evaluation of this legal risk is depicted in table form in Table 63 at p426.

5.6.4 SOME RISK MANAGEMENT STRATEGIES

A *risk control* strategy for a business would be to implement a system such that the customer is required to confirm an order before the goods or services ordered by the customer are delivered. If such a system were in place this would reduce instances of the situation arising where a customer claims that an order was cancelled (that is, the customer's "offer" was withdrawn) but receipt of the cancellation is not actually received by the business until after delivery of the goods or services purchased from the business has been effected.

5.6.5 EVALUATION OF RISK MANAGEMENT STRATEGIES

According to the risk management principles discussed at 2.4.4.4.1 at p102 because the consequence of this risk is *low* and the likelihood of risk is *moderate*, this risk is the type of risk that should be retained and managed by the business. To retain this legal risk is not, however, consistent with another guiding principle discussed at 2.4.4.4.4 at p107, which is that a business should only retain risks over which it has control. Here, the business has no control over any delays that may occur in relation to acceptances it transmits to a customer through the Internet. In reality, however, a

---

Community", NZLC R50, October 1998, Wellington, New Zealand, p 28 para 72.

business will probably have no choice but to retain this legal risk as it seems unlikely that this legal risk could be transferred, such as by way of insurance. Given that the risk *level* is *moderate*, it would be prudent for the business to implement the risk management strategy put forward to minimise this risk. Implementing this risk management strategy could involve considerable cost to a business if the business's Internet commerce software has to be reconfigured or even rewritten or modified to incorporate this option. Accordingly, it may or may not be cost effective for a particular business to implement this risk management strategy. Compared to the general risk criteria for a business conducting Internet commerce, the implementation of a risk management strategy would achieve the objective of protecting a business's legal rights and interests.

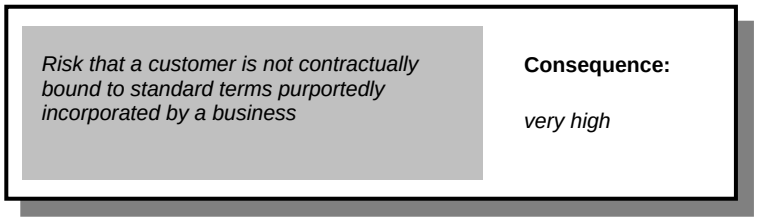
The risk management strategies put forward and the recommended risk management strategies are set out in table form in Table 64 at p429.

5.7 Risk that a customer is not contractually bound to standard terms purportedly incorporated by a business

5.7.1 ANALYSIS OF THE CONSEQUENCE OF THE RISK EVENTUATING

The *consequence* of this legal risk, as concluded in the discussion that follows, is depicted in Figure 17:

Figure 17 EVALUATION OF THE CONSEQUENCE



The consequence to a business should this risk eventuate is the cost to the business of having to transact with a customer without being able to rely on the terms which the business had sought to incorporate. What this cost will be, of course, depends on the terms that the business sought unsuccessfully to incorporate. Accordingly, it is difficult to provide a meaningful analysis of the consequence of this risk at a generic level. Taking a conservative view, given that terms that are typically sought to be incorporated by businesses are terms limiting liability, the impact of a business not succeeding at law in incorporating its standard terms in an Internet transaction is *very high*. That is, the consequences would threaten the survival or continued effective function of the business's Internet commerce activities or require the intervention of top level management.

5.7.2 ANALYSIS OF THE LIKELIHOOD OF THE RISK EVENTUATING

The *likelihood* of this legal risk, as concluded in the discussion that follows, is depicted in Figure 18:

Figure 18 EVALUATION OF THE LIKELIHOOD

Risk that a customer is not contractually bound to standard terms purportedly incorporated by a business	**Likelihood:** ***unlikely***

A business that conducts Internet commerce may wish to make use of standard terms in its transactions with its customers. This is typically the case in relation to business-to-consumer Internet transactions. A business may seek to incorporate its standard terms by including them in an order form that is e-mailed to its customers and which requests customers to signify acceptance of the terms by return e-mail, or by displaying terms on the business's web page which requires customers to click on a button, icon or hypertext to signify acceptance of those terms before the customer is allowed to proceed with purchasing the business's goods or services. It has been suggested that the incorporation of standard terms by a business by referring to a hypertext link that sets out these terms, and requiring all customers to signify agreement with such terms by clicking on an icon or a button on which is enscribed the words "I agree" or "I accept" or "agreed" brings about legal risk. For example,

> It may be plausible for the user of the computer system to deny knowledge of the screen message (many people ignore some messages that appear on their computer screens) and to deny that simply proceeding to the next series of screens constituted any intentional acceptance of any offer. [594]

[594] Henry H Perritt Jr, *Law and the Information Superhighway*, John Wiley & Sons, Inc, New York, 1996, Ch 9, p 382, sect 9.3.

In general, a business can incorporate standard terms in two ways: (i) where a customer has signed the document on which the terms are written; or (ii) by inferring incorporation of the terms through receipt by a customer of a notice of the terms where the transaction is of the kind that ordinarily is entered into without a signed document[595]. If, in the context of Internet commerce, a business purports to incorporate standard terms that do not cannot satisfy either method of incorporating terms, the business risks repudiation by a customer of the terms purportedly incorporated by the business.

Each method of incorporation will be examined in the context of Internet commerce in order that an analysis of the likelihood of this risk can be made.

5.7.2.1 Incorporation of terms by way of signature

A business that conducts Internet commerce can incorporate standard terms in an Internet transaction by requiring its customers to sign an e-mail that contains the standard terms or to sign a form in a web page on which the terms are displayed. As discussed earlier in this chapter at 5.4.2.2.9 and 5.4.2.2.10, whilst it is not possible for a customer to affix a handwritten signature in relation to Internet transactions, the typed name of a customer or an electronic "facsimile" signature probably constitutes a signature under common law for the purposes of the Statute of Frauds writing requirement. Furthermore, as was discussed at 5.4.2.2.9 and 5.4.2.2.10, an electronic "facsimile" signature and, even in some circumstances, a typed signature will be given the same legal effect as a paper-based signature under the Electronic

595 Starke, Seddon, Ellinghaus, para 424.

Transactions Act 1999 (Cth) (the Commonwealth legislation requires that the use of a typed signature be as reliable as was appropriate for the purposes for which the information was communicated. See 5.4.2.2.9) and the Electronic Commerce Framework Bill (Vic), if enacted. Assuming that the typed name of a customer or an electronic "facsimile" signature, likewise, constitutes a signature for the purposes of incorporation of terms by signature, a business could, if it so wished, incorporate standard terms in a contract between it and a customer by displaying its standard terms on its web page, or e-mailing the terms to a customer, accompanied by text which requests customers to either type in their name or affix an electronic "facsimile" signature to signify acceptance of those terms, noting that each of these acts will bear the same significance as if a handwritten signature had been affixed. In addition, under the Electronic Transactions Act 1999 (Cth) and the Electronic Commerce Framework Bill (Vic), if passed, a business can incorporate standard terms by requiring a party to affix a digital signature, as the use of a digital signature will be given the same legal effect as a paper-based signature. As discussed at 5.4.2.2.11, digital signatures are unlikely to constitute signatures under common law. Therefore a business cannot incorporate terms by requiring a digital signature in relation to an Internet transaction that is not governed by electronic commerce legislation.

5.7.2.2 Incorporation of terms by way of notice

The alternative way in which standard terms can be incorporated in an Internet transaction is by inferring acceptance of the business's terms, through the receipt by a

customer of notice of the business's standard terms, on the basis that such a transaction falls within the category of contracts that are ordinarily entered into without a signed document. Terms are typically incorporated without a customer's signature by the issue of a ticket or notice to the customer on which a business's terms (usually excluding liability in the event of a breach by the business) are printed. In the context of Internet commerce, the practice of incorporating a business's standard terms without obtaining the signature of a customer is commonly used in relation to the provision of software, where the licences detailing the terms of use for the software imposed by a business are referred to as web wrap or on-line shrinkwrap licences. In general, the courts have held that standard terms can only be incorporated in the absence of a signature, if a reasonable person would have expected to find contractual terms on the ticket or notice on which the terms are displayed: *Parker v. South Eastern Railway Co.* (1877) 2 CPD 416; *Causer v. Brown* [1952] VLR 1. In addition, reasonable notice of the terms must have been given: *Oceanic Sun Line Special Shipping Co Inc v Fay* (1988) 165 CLR 197. Furthermore, where a business seeks to incorporate standard terms in circumstances where a customer has made an "offer" to transact with the business, it is necessary to construe the business's purported incorporation of standard terms as a counter-offer in order for the terms to be effectively incorporated: *MacRobertson Miller Airline Services v Commissioner of State Taxation* (WA) (1975) 133 CLR 125; *Oceanic Sun Line Special Shipping Co Inc v Fay* (1988) 165 CLR 197.

In order for a business to successfully incorporate terms into an Internet transaction without a customer's signature the business would therefore need to display the terms which it seeks to incorporate (whether by means of e-mail or on the business's web page) where it is reasonable to expect such terms. In addition, in order to satisfy the requirement of reasonable notice, the customer's attention should be drawn to the terms, for example, by using bold text, or a graphic that draws attention to the terms. A common example of this approach taken by businesses that conduct Internet commerce is the use of "click through" licences whereby the customer is required to click through a number of forms or screens to signify acceptance of the terms on which the parties agree to transact before an order or delivery of the goods of services online is allowed to proceed.

5.7.2.3 Some conclusions about the likelihood of risk

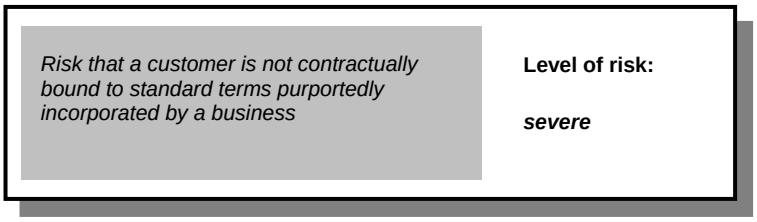
In relation to Internet commerce, particularly business-to-consumer Internet transactions, the most common method of incorporating standard terms in Internet transactions is by way of notice. A business typically displays the terms to which the customer has agreed on a web page and requires the customer to click on a button to signify acceptance of those terms. Some methods of incorporating terms by notice may not at law be effective, as in the case of a business displaying the terms in circumstances where it is not reasonable to expect such terms or because the business has not drawn the customer's attention to the terms. Many methods used by businesses, however, will satisfy the requirements for incorporation by notice.

Accordingly, the likelihood of risk is categorised as *unlikely*. That is the risk could eventuate at some time.

5.7.3 LEVEL OF RISK

The *level* of this legal risk, as concluded in the discussion that follows, is depicted in Figure 19:

Figure 19 EVALUATION OF LEVEL OF RISK



The consequence of the risk that a customer is not contractually bound to standard terms purportedly incorporated by a business will depend on the terms the business sought unsuccessfully to incorporate. The discussion at 5.7.1 at p349 concluded that the *consequence* of this risk is *very high* given that the types of terms a business typically seeks to incorporate are terms that limit the business's liability. The *likelihood* of this risk is assessed as being unlikely given that the method typically employed to incorporate terms (a business will display the terms on which it wishes to transact and then require the customer to click on a button to signify acceptance) will, in most cases, incorporate such terms at law. As this risk has been categorised as

very high in *consequence* and *unlikely* in *likelihood* the risk level is *severe*. The evaluation of this legal risk is depicted in table form in Table 63 at p426.

5.7.4 SOME RISK MANAGEMENT STRATEGIES

The *risk control* strategies for managing this risk revolve around ensuring that the business's standard terms are incorporated at law either by signature or by way of notice.

If a business seeks to incorporate standard terms by way of signature, a *risk control* strategy is to seek to incorporate terms by way of typed signature (although it should be noted in relation to Internet transaction governed by section 10 of the Commonwealth Electronic Transactions Act 1999 the use of a typed signature to incorporate terms by signature in relation to transactions governed by the Commonwealth legislation may not satisfy the additional requirement that such use be as reliable as appropriate in the circumstances) or electronic signature rather than by digital signature. Except for Internet transactions governed by Commonwealth law , and until digital signatures are legislatively or judicially accorded the status of signatures in other Australian jurisdictions, it is not recommended that a business seek to incorporate terms using digital signatures. A more detailed discussion of how digital signatures work and the disadvantages of using them is made at 5.10 at p397.

Another *risk control* strategy in relation to terms which a business seeks to incorporate by way of signature, is to ensure that the customer is made aware of the significance of typing in the customer's name or using an electronic "facsimile" signature. (For example, the business displays on its web page containing the terms a

conspicuous notice which states “By typing in your name [or by affixing your electronic signature], you have signified that you agree to the terms displayed on this page”).

A *risk control* strategy for the business in relation to terms it seeks to incorporate by notice, is for the business to ensure that the display of the terms sought to be incorporated appears in circumstances in which it is reasonable to expect such terms. (For example, such terms could be displayed on the same page that the order form is displayed on a web page). In addition, attention must be drawn to the terms. (For example, the business should draw attention to the terms on its web site with the use of a prominent button or icon or hypertextlink to the terms).

5.7.5 EVALUATION OF RISK MANAGEMENT STRATEGIES

As with the other legal risks, it is relevant to consider the *degree* of *consequence* and *likelihood* of risk in determining which risk management strategy to implement. The consequences of this risk are *very high* and the likelihood *unlikely*. According to risk management principles, as discussed at 2.4.4.4.1 at p102, this type of risk should be transferred by way of insurance.

It is not known whether a business can insure against this type of risk. Certainly, the consequence of this risk does not fall within the types of loss typically covered by insurance, such as physical damage, legal liability or errors and omissions. Nor is this risk likely to be covered by the “specialist” insurance policies that are aimed specifically at businesses that conduct Internet commerce. Such Internet insurance policies typically cover liability for loss of money or electronic funds (resulting from

theft of a customer's credit card data) arising out of use of a business' web site, personal injury liability caused by electronic communication of information or a person's unauthorised access to the business's web site, and provide insurance for assets such as computer equipment, data and media in respect of direct physical loss from vandalism, losses from computer viruses, business interruption and communications being overwhelmed or interrupted from a covered cause of loss[596].

If insurance cannot be obtained, or it is not cost effective for the business to obtain insurance against this risk, then the business must retain and manage the risk. Certainly retaining the risk is consistent with another guiding principle discussed at 2.4.4.4.4 at p107, which is that a business should only retain risks over which it has control. In such circumstances, the business must implement risk management strategies to minimise its exposure to this risk given that the risk level is *severe*. In fact it is suggested that given the level of risk, this risk requires detailed research and management planning at senior level. Compared to the general risk criteria for a business conducting intent commerce, either approach (that is, to transfer the risk by way of insurance or to retain the risk and implement risk management strategies to minimise the risk) will conform with the objective of protecting a business's legal rights and interests.

So which risk management strategies should a business implement? Due to the legal uncertainty concerning whether a typed signature constitutes a signature at law

---

[596] See for example the Internet Security Liability insurance policy offered by the US insurance company, Hamilton Dorsey Alston Co at http://www.webriskins.com/isl_cov.htm.

in all jurisdictions (that is the uncertainty raised in relation to Internet transactions governed by section 10 of the Commonwealth Electronic Transactions Act (Cth)), and to the additional transactional costs involved with incorporating terms by using digital signature technology, a business that wishes to incorporate standard terms should do so by way of notice. Accordingly, the risk management strategy that should be implemented is for the business to ensure that the display of the terms sought to be incorporated appears in circumstances in which it is reasonable to expect such terms and that the customer's attention must be drawn to the terms. The cost of implementing this strategy is not likely to outweigh the risk reduction benefit of this option.

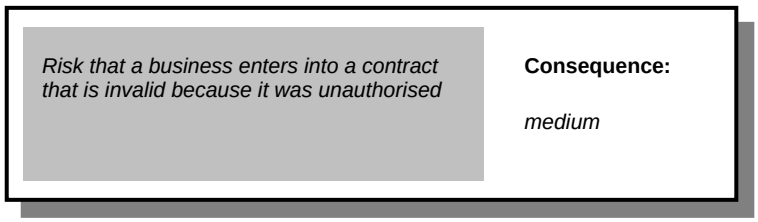
The risk management strategies put forward and the recommended risk management strategies are set out in table form in Table 64 at p429.

5.8 Risk that a business enters into a contract that is invalid because it was unauthorised

5.8.1 ANALYSIS OF THE CONSEQUENCE OF THE RISK EVENTUATING

The *consequence* of this legal risk, as concluded in the discussion that follows, is depicted in Figure 20:

Figure 20 EVALUATION OF THE CONSEQUENCE



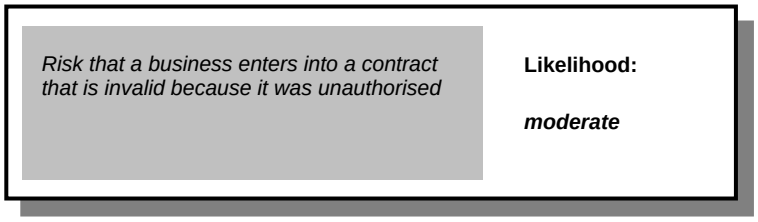
The consequence of this risk eventuating is that an Internet transaction entered into under these circumstances is invalid at law. Any Internet transaction subsequently repudiated by the party with whom a business is transacting or believed it was transacting, will not be enforceable. In addition, the business may be liable for statutory non-compliance if the Internet transactions conducted by the business are prohibited by law. In such circumstances, the consequence will not only be that the Internet transaction entered into is invalid but the business may be liable under criminal law for breaching the law. Although it is difficult to categorise the consequences of this risk with precision without reference to a specific business this risk has been categorised as *medium* in consequence. That is, the consequences would not threaten the business's Internet commerce activities but administration of the business's Internet commerce activities could be subject to significant review of or changed ways of operating. This assessment is based on the premise that this legal risk, if it eventuated, would also give rise to liability for statutory non-compliance. Where this is not the case, such as where an Internet transaction is unauthorised because it was entered into by an agent on behalf of a principal without authority, this risk is assessed as low in consequence which is consistent with the assessment of other legal risks, the consequences of which are that any Internet transaction entered into is unenforceable. Conversely, where the consequence of this legal risk involves liability for statutory non-compliance and the penalty for non-compliance is serious such as a substantial fine or a prison sentence for employees, manager or directors of

the business, this legal risk would be categorised as very high or extreme in consequence.

5.8.2 ANALYSIS OF THE LIKELIHOOD OF THE RISK EVENTUATING

The *likelihood* of this legal risk, as concluded in the discussion that follows, is depicted in Figure 21:

Figure 21 EVALUATION OF THE LIKELIHOOD



A business faces the risk of entering into an unauthorised Internet transaction in two contexts: (i) where the party with whom the business is transacting is unauthorised to enter into the transaction due to laws prohibiting or otherwise regulating the type of goods or services offered by a business to that party. For example, where certain goods can only be sold to persons over a certain age or cannot legally be sold in certain jurisdictions[597]; (ii) where the party with whom the business is transacting is purportedly acting for a principal but lacks actual, ostensible, or implied actual authority to do so. For example, a customer may falsely claim to act on

behalf of another party and induce the business to transact with the business on that basis.

5.8.2.1 *Effect of Article 13(3)(b) of the UNCITRAL Model Law on Electronic Commerce and the Commonwealth Electronic Transactions Act 1999 (Cth) where the party with whom the business is transacting is purportedly acting for a principal but lacks actual, ostensible, or implied actual authority to do so*

It is relevant in this discussion to consider Article 13(3)(b) of the UNCITRAL Model Law on Electronic Commerce in relation to where the party with whom the business is transacting is purportedly acting for a principal but lacks actual, ostensible, or implied actual authority to do so. Article 13(3)(b) entitles a party to regard an Internet communication (for example an on-line payment) to have been made by a principal where such communication results from the conduct of a party whose relationship with the principal or any agent of the principal enables that person to gain access to a method used by the principal to identify Internet communications as its own[598].

---

[597] Graham JH Smith et al, *Internet Law and Regulation*, A Specially Commissioned Report, FT Law & Tax, London, 1996, Ch 8, p 103, para 8.2.8.

[598] *Article 13. Attribution of data messages*

(1) A data message is that of the originator if it was sent by the originator itself.

(2) As between the originator and the addressee, a data message is deemed to be that of the originator if it was sent:

(a) by a person who had the authority to act on behalf of the originator in respect of that data message; or

(b) by an information system programmed by or on behalf of the originator to operate automatically.

(3) As between the originator and the addressee, an addressee is entitled to regard a data message as being that of the originator, and to act on that assumption, if:

(a) in order to ascertain whether the data message was that of the originator, the addressee properly applied a procedure previously agreed to by the originator for that purpose; or

(b) the data message as received by the addressee resulted from the actions of a person whose relationship with the originator or with any agent of the originator enabled that person to gain access to a method used by the originator to identify data messages as its own.

The Guide to the Model Law[599] states that Article 13 is not to intended to displace any rules of agency, and therefore whether a party had actual, implied or ostensible authority is left to be determined by the relevant governing law[600]:

> The purpose of article 13 is not to assign responsibility. It deals rather with attribution of data messages by establishing a presumption that under certain circumstances a data message would be considered as a message of the originator, and goes on to qualify that presumption in case the addressee knew or ought to have known that the data message was not that of the originator[601].

The Electronic Commerce Expert Group expressed reluctance to legislatively implement Article 13 of the Model Law. The Electronic Commerce Expert Group Report observed that the effect of Article 13(2)(b) was to expand on existing agency law principles by "binding an orginator to messages sent by information systems

---

(4) Paragraph (3) does not apply:
  (a) as of the time when the addressee has both received notice from the originator that the data message is not that of the originator, and had reasonable time to act accordingly; or
  (b) in a case within paragraph (3) (b), at any time when the addressee knew or should have known, had it exercised reasonable care or used any agreed procedure, that the data message was not that of the originator.

(5) Where a data message is that of the originator or is deemed to be that of the originator, or the addressee is entitled to act on that assumption, then, as between the originator and the addressee, the addressee is entitled to regard the data message as received as being what the originator intended to send, and to act on that assumption. The addressee is not so entitled when it knew or should have known, had it exercised reasonable care or used any agreed procedure, that the transmission resulted in any error in the data message as received.

(6) The addressee is entitled to regard each data message received as a separate data message and to act on that assumption, except to the extent that it duplicates another data message and the addressee knew or should have known, had it exercised reasonable care or used any agreed procedure, that the data message was a duplicate.

599 United Nations Commission on International Trade Law, "Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce (1996)", http://www.un.or.at/uncitral/texts/electcom/ml-ec.htm, paras 83.

600 United Nations Commission on International Trade Law, "Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce (1996)", http://www.un.or.at/uncitral/texts/electcom/ml-ec.htm, para 84.

601 United Nations Commission on International Trade Law, "Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce (1996)", http://www.un.or.at/uncitral/texts/electcom/ml-ec.htm, para 83-92.

programmed by or on behalf of the originator"[602]. This was seen by the Expert Group as too broad because, "it appears to make the originator responsible even if the programming or the data on which the program operates is altered by a third party or a computer virus"[603]. In addition, the Expert Group preferred an approach by which an assumption as to attribution of an Internet communication could be made only where authentication procedures used by the purported sender met a specified standard, rather than as proposed by Article 13(3)(a) where the authentication procedures used by the purported sender had been previously agreed to by the purported sender. The reason for this was, "a presumption of attribution for any and all authentication procedures cannot be justified when the security and reliability of such systems varies so markedly as to prevent a factual basis for such a presumption"[604]. The Electronic Commerce Expert Group considered that to implement legislation regulating attribution in relation to Internet transactions would result in the creation of rules that could place recipients of Internet communications in a better position than recipients of manually signed paper-based communications and to do so was contrary to the basic premise that electronic commerce legislation should neither prefer nor disadvantage electronic commerce compared with off-line commerce[605]. Instead the Electronic Commerce Expert Group concluded that a legislative provision should be enacted that allows parties to agree between themselves as to how issues of attribution are to be resolved and that any legislation

---

602 *Electronic Commerce: Building the Legal Framework*, para 4.5.65.
603 *Electronic Commerce: Building the Legal Framework*, para 4.5.65.
604 *Electronic Commerce: Building the Legal Framework*, para 4.5.66.

governing attribution of Internet communications should be restricted to restating the common law (such as general agency principles)[606]. This, however, would be subject to a requirement that such agreed rules of attribution are fair and reasonable to impose in all the circumstances[607]. The Electronic Commerce Expert Group considers relevant to the question of fairness and reasonableness the following factors:

> The reliability and security of any procedures which are used by the originator and addressee to authenticate the originator of the data message or to ensure that the content of the messages received is the same as that which was sent; and the reliability and security of the access device used by the originator to operate such procedures[608].

Thus, in line with the view that any legislative provision as to attribution should simply reflect the common law, the Electronic Commerce Expert Group recommended that where parties have not determined the issue of attribution by agreement, that legislation should provide that an Internet communication that is purportedly sent by a party should only bind that party if in fact the Internet communication was sent by that party or with their authority. This places the onus on the receiving party to prove that an Internet communication was sent by sent by the purported sender or with that party's authority[609].

The recommendations of the Expert Group were implemented in section 15 of the Electronic Transactions Act 1999 (Cth). Section 15 effectively restates but does not

---

605 *Electronic Commerce: Building the Legal Framework*, paras 4.5.76-4.5.78.
606 *Electronic Commerce: Building the Legal Framework*, para 4.5.78.
607 *Electronic Commerce: Building the Legal Framework*, para 4.5.79.
608 *Electronic Commerce: Building the Legal Framework*. See para (vii) of the Executive Summary and Recommendation 12.

purport to codify the common law position in relation to the attribution of Internet communications regulated by Commonwealth law[610]. Thus a party, who is subject to Commonwealth law, will only be bound by an Internet communication if in fact the Internet communication was sent by that person or with their authority. Furthermore, the laws of agency, including the doctrines of apparent and actual authority, are not affected[611].

The Victorian Electronic Commerce Framework Bill (Vic) does not deal with the issue of attribution of Internet communications, and therefore, like other jurisdictions that lack electronic commerce legislation (and the Commonwealth position), is governed by the common law.

5.8.2.2 Some conclusions about the likelihood of risk

---

609 *Electronic Commerce: Building the Legal Framework*. See Recommendation 12.

610 Attorney- General's Department, "Explanatory Paper -Electronic Transactions Bill 1999", January 1999 at p 15-16. Section 15 of the Electronic Transactions Act 1999 (Cth) provides:

15 Attribution of electronic communications

(1) For the purposes of a law of the Commonwealth, unless otherwise agreed between the purported sender and the recipient of an electronic communication, the purported sender of the electronic communication is bound by that communication only if the communication was sent by the purported sender or with the authority of the purported sender.

(2) Subsection (1) is not intended to affect the operation of a law (whether written or unwritten) that makes provision for:

(a) conduct engaged in by a person within the scope of the person's actual or apparent authority to be attributed to another person; or

(b) a person to be bound by conduct engaged in by another person within the scope of the other person's actual or apparent authority.

Exemptions

(3) The regulations may provide that this section does not apply to a specified electronic communication.

(4) The regulations may provide that this section does not apply to a specified law of the Commonwealth.

611 Attorney- General's Department, "Explanatory Paper -Electronic Transactions Bill 1999", January 1999 at p 15-16.

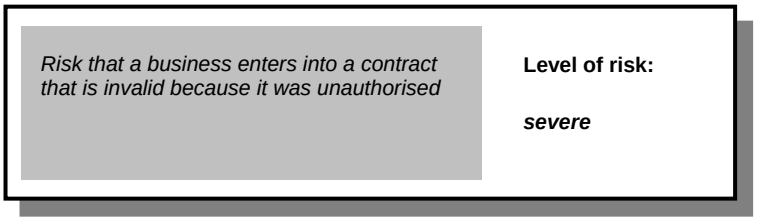
Unlike the other legal risks discussed in this chapter, assessing the likelihood of this risk on a generic basis is difficult here because factors particular to a specific business, such as the type of product or service offered, and the countries/ jurisdictions where such products or services are offered will obviously affect the likelihood of this risk eventuating. Based on a conservative analysis, this risk is categorised as a *moderate* risk. That is, the risk should eventuate at some time. Clearly, where a business is selling services or products, the sale of which is illegal in some jurisdictions, there is a greater likelihood of the risk eventuating than if the services or the products the business is selling are not illegal.

5.8.3 LEVEL OF RISK

The *level* of this legal risk, as concluded in the discussion that follows, is depicted in

Figure 22:

Figure 22 EVALUATION OF LEVEL OF RISK



The *consequence* of the risk that a business enters into a contract that is invalid was assessed as being *medium* at 5.8.1 at p360 because the consequences would

threaten a business's Internet commerce activities but could be dealt with internally. The *likelihood* of this risk depends on the products or services a business is offering through the Internet and the countries/jurisdictions to which the business's product or services are offered. A conservative assessment of the *likelihood* of this risk is that this legal risk should eventuate at some time, that is, the likelihood is *moderate*. As this risk has been categorised as *medium* in *consequence* and *moderate* in *likelihood* the level of this risk is *severe*. The evaluation of this legal risk is depicted in table form in Table 63 at p426.

5.8.4 SOME RISK MANAGEMENT STRATEGIES

In relation to where a customer is prohibited at law from entering into a transaction with the business, a *risk control* strategy that a business could implement is to require its customers to use digital signatures which are certified as to a customer's age, country of residence, authority to contract or whatever factor it is necessary for the business to confirm in order that the particular Internet transaction entered into is authorised. How digital signatures can be used to effect this and the disadvantages associated with using digital signatures are discussed later in this chapter at 5.10 at p397.

In relation to Internet transactions which are prohibited in certain jurisdictions, a *risk control* strategy is for the business to block transactions with customers whose Internet service provider domain falls within one of those jurisdictions and, in the case of the sale of tangible goods, to block transactions whose delivery address falls within a jurisdiction that prohibits such transactions.

In relation to where a party with whom the business transacts purports to have but lacks authority to act on behalf of a principal, a *risk control* strategy is for a business to incorporate as a contractual term of any transaction with its customers a term reflecting Article 13(3)(b) of the UNCITRAL Model Law on Electronic Commerce (See 5.8.2.1 at p363 and footnote 598). If a business incorporates Article 13 as a term in its transactions with its customers, particularly Article 13(3)(b), the risk that an Internet transaction that a business enters into is unenforceable because it was entered into by a customer who lacked authority but who purported to act for another party will be less likely to arise. This is because Article 13(3)(b) appears to remove the requirement under ordinary agency principles that an agent must have either actual, ostensible or implied actual authority to act on behalf of the principal. Instead, all a business need prove to enforce an Internet transaction against a party for whom a customer has purported to act, is that the Internet communication that the business received from the customer resulted from the customer's having a relationship with the party for whom the customer purported to act, that enabled the customer to gain access to a method used by the party for whom the customer purports to act, to identify data messages as its own.

5.8.5 EVALUATION OF RISK MANAGEMENT STRATEGIES

Again, it is useful to consider the *degree* of *consequence* and *likelihood* of risk as discussed at 2.4.4.4.1 at p102 in order to determine which risk management strategy to implement. As this risk is *medium* in consequence and *moderate* in likelihood, this type of risk is likely to be too costly to transfer by way of insurance and therefore

should be retained and managed. To retain this legal risk is also consistent with another guiding principle discussed at 2.4.4.4.4 at p107, which is that a business should only retain risks over which it has control. Here a business faced with this legal risk can control this risk by limiting who it transacts with. Assuming this risk is retained by a business, it will be necessary for the business to implement risk management strategies, such as those put forward, to minimise this risk. Compared against the general risk criteria for a business conducting Internet commerce such action would comply with the objective of minimising a business's liability, protecting a business's legal rights and obligations and, where legislation exists prohibiting the business's Internet commerce activity in certain circumstances (such as sales to underage customers), ensuring regulatory compliance.

As the level of risk is categorised as *severe*, it is recommended that this risk be brought to the attention of senor management and that research and management planning be undertaken at that level.

So what legal risk management strategies should a business implement? The risk management strategy which involves incorporating a contractual term that reflects Article 13(3)(b) of the UNCITRAL Model Law on Electronic Commerce would probably require modification of the business's Internet commerce software. However, given that this option would significantly reduce one aspect of this risk it is suggested that on a cost benefit basis the cost of managing this aspect of this risk is commensurate with the benefit obtained.

A similar argument applies in relation to the risk management strategy involving the business blocking transactions with customers whose Internet service provider domain falls within a jurisdiction that prohibits transacting with the business and, in the case of the sale of tangible goods, blocking transactions whose delivery address falls within a jurisdiction that prohibits such transactions. That is, although implementation of this option will involve additional cost, it is suggested that on a cost benefit basis the cost of managing this aspect of this risk is commensurate with the benefit obtained.

The most problematic situation for business in regard to this risk is in relation to the sale of products or services that are, at law, age restricted. Only one risk management strategy was put forward to reduce this aspect of this risk. This risk management strategy, the use of digital signatures, will add transaction costs and may deter potential customers, as it requires the business's customer to also incur cost and acquire digital signature software and digital certificates. Given, however, the penalties that a business may be exposed for statutory non-compliance a business may have little choice but to implement this option. Keeping in mind also that this risk level is *severe,* senior management should be involved in deciding which risk management strategy to adopt, particularly if risk retention without implementation of any risk reduction strategies is being considered. If the business opts not to implement such a risk management strategy, at the very least, the business should make it clear to prospective customers that the business is only prepared to transact with a person who is legally permitted to transact with the business, and a mechanism

should be used such as, where the Internet commerce is web based, a button which must be clicked, that requires the customer to attest to his or her age.

The risk management strategies put forward and the recommended risk management strategies are set out in table form in Table 64 at p429.

5.9 Risk of a business incurring liability in relation to the acceptance of on-line payments

The discussion here focuses on whether acceptance of payment through the Internet **("on-line payment")** creates additional contractual risks for businesses that conduct Internet commerce. By way of background, a brief overview of on-line payment systems is provided.

5.9.1 ON-LINE PAYMENT SYSTEMS- AN OVERVIEW

There are several mechanisms for effecting on-line payment and it is relevant to include here a brief discussion of how such payment mechanisms operate[612]. The mechanisms available for effecting on-line payment can be categorised in several

---

[612] For more detailed descriptions of the various methods by which on-line payment can be effected refer to: Alan Tyree, *Digital Cash*, Butterworths, Sydney, 1997; Graham JH Smith et al, "Payment Mechanisms for Internet Commerce", Ch 9, in *Internet Law and Regulation*, A Specially Commissioned Report, FT Law & Tax, London, 1996; Henry Perritt Jr, "Legal and Technological Infrastructures for Electronic Payment Systems", 2 *Rutgers Computer & Technology Law Journal*, Volume 22, 1996, pp 1-60; Roger Clarke, "Net-Based Payment Schemes", 1 December 1996, http://www.anu.edu/people/Roger.Clarke/EC/EPMEPM.html; Thomas J Smedinghoff, "Online Payment Options", chapter 7, in *Online Law : the SPA's Legal Guide to doing Business on the Internet*, Thomas J. Smedinghoff, editor, Addison-Wesley Publishing, Reading, Massachusetts, 1996; US Department of Treasury, "An Introduction to Electronic Money Issues- Toward Electronic Money and Banking: The Role of Government", US Department of Treasury, September 19-20 1996, Washington, DC; Chris Reed and Lars Davies, "Digital Cash- the Legal Implications", IT Law Unit, Centre for Commercial Law Studies, Queen Mary & Westfield College, London, 1995; Andreas Crede, "Electronic Commerce and the Banking Industry: The Requirement and Opportunities for New Payment Systems Using the Internet, *Journal of Computer-Mediated Communication*, Volume 1, No 3, http://www.usc.edu/dept/annenberg/vol1/issue3/crede.html.

ways and consequently have not been described consistently in the literature. Some writers choose to draw the distinction between those mechanisms that effect payment through the direct exchange of tokens and those payments that are effected by means of an instruction from a customer to a third party who in turn effects payment to the business with whom the customer is conducting Internet commerce[613]. Other writers have chosen to draw the distinction between electronic cash systems operating on Electronic Funds Transfer principles and "true" electronic cash[614]. Others again prefer to draw the distinction between on-line payment mechanisms that identify a customer "Identified Electronic Payment Systems" and mechanisms that can be used without the customer being identified "Anonymous Electronic Payment Systems"[615]. A different approach taken has been to categorise payments as either an "evolutionary approach" (credit card and debit card payments), "revolutionary approach" (digital cash) or "integrated approach" (stored value card)[616]. Yet another approach has been to categorise on-line payment mechanisms into the following four categories: (i) digital cash, (ii) payment clearance systems, (iii) secure credit cards

---

613 Thomas J Smedinghoff, "Online Payment Options", chapter 7, in *Online Law : the SPA's Legal Guide to doing Business on the Internet*, Thomas J. Smedinghoff, editor, Addison-Wesley Publishing, Reading, Massachusetts, 1996, page 105, para 7.1.

614 Graham JH Smith et al, "Payment Mechanisms for Internet Commerce", chapter 9, in *Internet Law and Regulation*, A Specially Commissioned Report, FT Law & Tax, London, 1996, pp 115-116, paras 9.7- 9.73; Chris Reed and Lars Davies, "Digital Cash- the Legal Implications", IT Law Unit, Centre for Commercial Law Studies, Queen Mary & Westfield College, London, 1995, pp 1-9, paras 1-1.3.

615 Andrew Dahl, Leslie Leswick, *Internet Commerce*, New Riders Publishing, Indianapolis, Indiana, 1996, Chapter 3, p 75.

616 Roger Clarke, "Net-Based Payment Schemes", 1 December 1996, http://www.anu.edu/people/Roger.Clarke/EC/EPMEPM.html.

and (iv) smart card based systems."[617] Another approach has been to categorise the various on-line payment mechanisms into the following categories: e-mail approach (whereby payment is effected by way of credit card without actually exchanging credit card information on the Internet), unencrypted credit cards, encrypted credit cards, electronic credit cards, electronic checks and electronic cash[618].

Adding to this confusion, new mechanisms for on-line payment are continuously being developed making it practically impossible to exhaustively categorise the various forms which on-line payment mechanisms can take. For the purposes of discussing the risks associated with accepting on-line forms of payment, the various on-line payment mechanisms will be categorised into one of four categories: (i) unsecure credit card payments, (ii) secure credit card payments and other secure on-line payment mechanisms employing electronic funds transfer principles (iii) electronic cheques and (iv) digital cash. Each of these categories will be briefly discussed.

5.9.1.1 Unsecure credit card payments

The first category, "unsecure credit card payments", simply refers to the use of a credit card by a customer to effect payment for an Internet transaction without additional security precautions. In such instances, on-line payment is effected by the customer providing unencrypted credit card details by e-mail or through a form

---

617 Andreas Crede, "Electronic Commerce and the Banking Industry: The Requirement and Opportunities for New Payment Systems Using the Internet, *Journal of Computer-Mediated Communication*, Volume 1, No 3, http://www.usc.edu/dept/annenberg/vol1/issue3/crede.html.

618 Andrew Dahl, Leslie Leswick, *Internet Commerce*, New Riders Publishing, Indianapolis, Indiana, 1996, Chapter 3, pp 72-74.

provided on the business's web page which is transmitted to the business with whom the customer is transacting.

5.9.1.2 Secure credit card payments and other secure on-line payment mechanisms employing electronic funds transfer principles

The second category, "secure credit card payments and other on-line payment mechanisms that employ electronic fund transfer principles", refers to payment mechanisms that apply electronic fund transfer principles and therefore are effected through a third party clearing system (for example, a bank or credit card company). Several on-line payment systems fall into this category such that it is useful to subcategorise these systems further. For the purposes of the discussion here, which makes no attempt at being definitive, three sub-categories are used, although it should be noted that some on-line payment systems may utilise elements from more than one sub-category. The three subcategories are: (i) on-line credit card payment systems that use secure channels such as Secure Hypertext Transfer Protocol (secure HTTP) or Secure Sockets Layer (SSL) to ensure credit card information is transmitted securely; (ii) on-line credit card payment systems that use encrypted e-mail applications (for example, credit card details are transmitted using the encryption program Pretty Good Privacy); (iii) on-line credit card payment systems that use a protocol designed specifically for effecting secure payments such as Secure Electronic Transaction **("SET")**, Open Financial Exchange, CyberCash Credit Card Protocol, Homebanking Computer Interface, Micro Payment Transfer Protocol and Joint Electronic Payments Initiative. It is not necessary for the purposes of the discussion in this chapter to describe in detail the various protocols that have been

developed in this regard. It is therefore proposed to consider further only one protocol, SET, whose use, given its development and endorsement by two of the major credit card companies, VISA and Mastercard, is likely to become prevalent.

The SET protocol requires customers to register with a Certificate Authority before SET payments can be effected[619]. Upon registration a customer receives a digital certificate that contains the customer's account number and expiration date which is encrypted. All businesses that wish to accept SET payments must be similarly be registered[620]. To effect a SET payment, a registered customer, during the course of ordering on-line (eg during the course of completing an on-line order form on a business's web page), will trigger the SET protocol by selecting a payment mechanism (eg payment by credit card) whose operation is governed by the SET protocol. In such instances, the selection by the customer of a SET payment mechanism will result in a message being transmitted to the business with whom the customer is transacting indicating which payment card brand will be used for payment[621].

The business then transmits a certified version (that is, a digital certificate authenticating a party's digital signature) of both its encryption public key and the encryption public key of the payment gateway that the business's bank uses, as well as a unique transaction identifier to the customer's software. The customer's software

---

619 Refer to *Book 1: Business Description- Secure Electronic Transaction Specification*, version 1, May 31 1997, p 37, para 4.2.

620 Refer to *Book 1: Business Description- Secure Electronic Transaction Specification*, version 1, May 31 1997, p 48, para 4.3.

then verifies the business's digital certificate and the digital certificate of the business's bank. These certificates are used later in the payment process.

The customer's software then creates two separate messages termed "Order Information" and "Payment Instructions". The "Order Information" message contains the unique transaction identifier, brand of payment card being used and the transaction date. This message is intended to be used by the business[622]. The "Payment Instructions" message contains processing information intended for the business's bank such as the customer's credit card number, the expiration date, the purchase amount agreed to by the buyer and description of the customer's order[623]. The customer's software then generates a "dual" digital signature in respect of the "Order Information" and the "Payment Instructions" by calculating a message digest of both messages, concatenating the two digests, computing a message digest of the result and encrypting the message digest using the customer's private key[624]. This "dual" signature is attached to both the "Payment Instructions" and the "Order Information" separately. The "Payment Instructions" message is encrypted with a randomly generated symmetric key. This symmetric key, along with the customer's account information is then encrypted with the public key of the business's bank. Both the "Order Information" and the "Payment Instructions" is transmitted to the

---

621 Refer to *Book 1: Business Description- Secure Electronic Transaction Specification*, version 1, May 31 1997, p 56, para 4.4.

622 Keith Lamond, "Credit Card Transactions Real World and Online", 1996, http://rembrandt.erols.com/mon/ElectronicProperty/klamond/credit_card.hm.

623 Keith Lamond, "Credit Card Transactions Real World and Online", 1996, http://rembrandt.erols.com/mon/ElectronicProperty/klamond/credit_card.hm.

business. The business's software verifies the identity of the customer and checks that the "Payment Instructions" have not been tampered with. The business's software then processes the order which includes obtaining authorisation through a device termed a "Payment Gateway" that is operated by the business's bank or a designated third party that processes credit card payments. If authorisation is given, the business transmits a confirmation response to the customer. The business then delivers the goods or performs the services requested by the customer.[625]

5.9.1.3 Electronic cheques

The third category, "payment by electronic cheque", refers to payment mechanisms that emulate paper-based cheques. Thus, a customer is issued with several serial identification numbers representing blank cheques in the same way that a customer receives a chequebook comprising numbered blank cheques. Digital signatures are used by the customer's software to sign, endorse and authenticate the customer. Electronic cheques are distinguished from on-line payment systems that are based on electronic funds transfer principles in that an electronic cheque can be sent directly from a customer to a business directly without going through an intermediary (such as a bank)[626]. In such systems an electronic cheque could bounce[627]. The FTSC

---

624 *Book 1: Business Description- Secure Electronic Transaction Specification,* version 1, May 31 1997, para 4.4.

625 This description of the SET procedure is a simplified description and for ease of understanding several steps have been omitted. For a detailed description of the SET procedure refer to *Book 1: Business Description- Secure Electronic Transaction Specification*, version 1, May 31 1997.

626 Thomas J Smedinghoff, "Online Payment Options", in *Online Law : the SPA's Legal Guide to doing Business on the Internet*, Thomas J. Smedinghoff, editor, Addison-Wesley Publishing, Reading, Massachusetts, 1996, p 115, para 7.6.

627 Smedinghoff, "Online Payment Options", para 7.6.

model provides for a chequebook which generates electronic cheques. Public key cryptography is used to sign cheques when they are written and processed.

5.9.1.4 Digital cash

The fourth category, "payment by digital cash", involves payments that seek to emulate payments made with physical cash. Such payment mechanisms typically involve the business receiving a signal (called a token, coin, digital cash) that can be re-used by the business in further transactions much in the way physical cash can be re-used. Several models for digital cash payment mechanisms exist. Some representative approaches include:

"Cash" stored on the customer's hard disk, such as the payment system, "ecash", developed by Digicash[628] whereby software is used that enables ecash to be "withdrawn" from a bank and then stored on the customer's hard disk. It is relevant to note that Digicash filed for bankruptcy protection in November 1998 in the US and it is therefore uncertain how long ecash will continue to be offered. Under the ecash model both the on-line business and its customers must have a bank account with a bank which issues ecash[629]. Upon obtaining an account, the bank issues the customer

---

[628] Digicash's eCash is offered by St George Bank in Australia. Interestingly, Digicash has not been a success in relation to its micropayment eCash scheme in the US, the only US Bank to offer eCash, the Mark Twain Bank, having decided to cease offering Digicash's eCash micropayment system (Tim Clark, "Digicash loses US toehold", CNET News.com, http://www.news.com/News/Item/o,4,259899,00.html?st.ne.fd.gif.k).

[629] In fact, this category of digital cash would also fall into the third payment category discussed above, as a third party is involved whose role is to operate as a clearing system. Once the customer has transmitted payment of 'cash' to the party with whom the customer is transacting, the 'payment is checked by the customer's bank which in turn informs the party with whom the customer is transacting whether the 'cash' is clear. See the documentation issued by Digicash "How ecash works inside", at http://www.digicash.nl/ecash/docs/works/index.html, "Electronic

with a digital signature containing a random seed, which is used to generate ecash,[630] and with encryption software developed by Digicash[631]. In order to use ecash a customer must first deposit money into the account that has been opened with a bank that issues ecash. To obtain ecash from the account, the customer makes a withdrawal using the software provided by the bank. The bank checks the digital signature used by the customer. Once authenticated, the customer's software generates a series of encrypted serial numbers each number representing a cash denomination nominated by the customer. Each serial number is stored in a "digital envelope" which "hides" the actual serial numbers used by the customer. The ecash is then validated by the bank with its digital signature and the value the ecash represents is withdrawn from the customer's account. The "digital envelope" is removed upon receipt of the validated ecash by the customer's software. In this way, the bank used by the customer for obtaining ecash cannot trace a particular serial number to the customer. Payment by ecash is effected by the customer simply choosing to pay by ecash (when such option is offered by the business with whom the customer is transacting). The customer's software will select the serial numbers that represent the amount payable and then transmits them to the business. The business's software will transmit the ecash to the customer's bank. The customer's bank records the serial numbers of the spent ecash (in this way the bank can ensure that ecash is not double-spent; if the

---

Payments with ecash", at: http://www.digicash.nl/ecash/ecash.html, and "Information for new ecash users", at http://www.digicash.nl/ecash/new_users/.

630 Andrew Dahl, Leslie Leswick, *Internet Commerce*, New Riders Publishing, Indianapolis, Indiana, 1996, chapter 4, p 88.

serial numbers have already been recorded then the business is advised.)[632] and the ecash is deposited in the business's ecash account;

"Cash" stored in smart cards that can only be used when a smart card reader is attached to the customer's computer such as the model developed by Mondex. Mondex has developed a digital cash system that requires both the customer and the business to acquire a Mondex smart card and attach to their computers a smart card reader[633]. Mondex cards can be 'locked' by a customer with a code so that others cannot use the card. In addition, Mondex cards use digital signatures to ensure that the card is not fraudulently used by others and to verify that the business receiving payment via Mondex is the intended recipient:

> The shopkeeper's terminal requests payment of a certain amount, and transmits a digital signature with the request. Both cards check the authenticity of each other's message.
>
> The customer's card checks the digital signature and, if satisfied, sends the amount, with its own digital signature attached. At this point, the value is deducted from the total value in the customer's card.
>
> The chip card in the shopkeeper's terminal checks the digital signature and, if satisfied, sends acknowledgment, again with a digital signature.
>
> Only now - after the amount has been deducted from the customer's card - is value added to the card in the shopkeeper's terminal. This is to prevent the possibility of duplication or unauthorised creation of value. The digital

---

631 Refer to the Digicash documentation "Electronic Payments with ecash", http://www.digicash.nl/ecash/ecash.html.

632 Refer to the Digicash documentation "How ecash works inside", http://www.digicash.nl/ecash/docs/works/index.html.

633 See the documentation issued by Mondex at: http://www.mondex.com/mondex/cgi-bin/printpage.pl?english+global&technology_internet.html.

> signature from this card is checked by the customer's card and if OK, this ends the process.[634]

"Cash" provided by a third party (for example, a bank) under a notational system. This last category of digital cash could equally fall into the third category discussed above, being a payment mechanism that involves a third party to operate as a clearing system. An example of this payment mechanism is CyberCoin micropayment system developed by CyberCash Inc. Under this system for effecting micropayments, a customer transfers 'cash' (up to a maximum of US$80 per day) from the customer's account into a 'wallet' that is stored on the customer's hard disk. A record of the 'cash' transferred by the customer into the customer's 'wallet' is recorded by the customer's bank but no 'cash' is actually stored on the customer's hard disk:

> For small payments on the Internet, ranging from $0.25 to $10.00, the CyberCoin system can be used in the US. Consumers use an existing bank account to transfer money to an Electronic Wallet. Money is never moved onto or stored on the consumer's PC. CyberCoin is a notational system. When the consumer transfers money into his/her wallet, it is legal record of the money, but not the money itself. When money is moved with CyberCoin, it is "noted" by existing banking networks and deducted or added to the proper account. Until delivery of the goods has reached the consumer's computer through the transfer of the encrypted key, the funds will not be moved. When it confirmed that the message digest has reached the consumer's hard disk, the money is instantaneously moved to the merchant's "CashRegister." At the of each business day, the true funds are reconciled within the existing banking networks, similar to the ways bank accounts are managed today. In a CyberCoin transaction, the financial information is encrypted and digitally signed, but the message itself is not.[635]

---

634 Mondex, "Mondex Security- The Chip and the Protocol" at; http://www.mondex.com/mondex/cgi-bin/printpage.pl?english+global&technology_security2.html

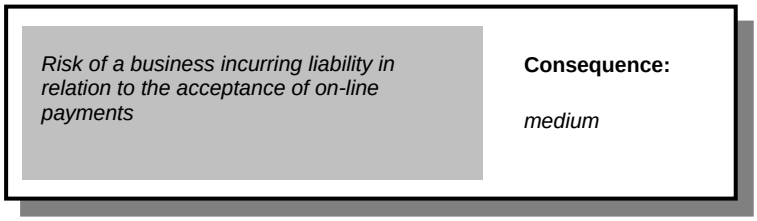
635 Open Information Interchange, "OII Standards and Specification List- Electronic Payment Mechanisms", http://www2.echo.lu/oii/en/payment.html http://www2.echo.lu/oii/en/payment.html#CyberCash, November 1997.

Public key cryptography is used to ensure that transactions are secure. It should be noted that Cybercash has recently abandoned the use of wallets opting for an alternative payment interface.

5.9.2 ANALYSIS OF THE CONSEQUENCE OF THE RISK EVENTUATING

The *consequence* of this legal risk, as concluded in the discussion that follows, is depicted in Figure 23:

Figure 23 EVALUATION OF THE CONSEQUENCE



The consequence of this risk eventuating is that the business will have to bear the loss associated with a repudiated on-line payment. The extent to which a business will bear a loss associated a repudiated on-line payment will be largely governed by the contractual agreement entered into by the business with each issuer of the forms of payment it decides to accept. Based on the practice adopted in off-line credit provider agreements, where risk is allocated to businesses that accept credit card payments by telephone, it seems likely that issuer agreements for on-line forms of

payments will, in all probability, allocate risk or at least some degree of risk to the business.

It should be noted that the Australian Securities Investment Commission established a consultative forum in March 1999 to review the rules governing the allocation of risk associated with acceptance of on-line forms of payment by businesses, including the Electronic Funds Transfer Code of Practice. There is some suggestion that in future more risk will be allocated to the bank issuing the on-line form of payment[636].

Again, it is difficult to generalise about this risk given that several variables will affect an assessment of the consequences such as the value of the goods or services transacted on the Internet. Absenting a change in the current allocation of risk, the consequence of this risk is categorised as *medium*. That is, the consequences would not threaten the survival or continued effective function of the business's Internet commerce activities but could subject the business's Internet commerce activities to significant review or changed ways of operating. See for example the following commentary on the effect of just one aspect of this risk, the risk that payment is made by an imposter and consequently will be repudiated by the party whom the imposter purported to be:

> When fraud does, in fact, strike an online store, its impact can be severe. Tom Arnold, Chief Technology Officer at CyberSource, a developer of Internet commerce solutions and fraud detection services, paints a startling picture of the actual damages a merchant can suffer from one fraudulent sale.

---

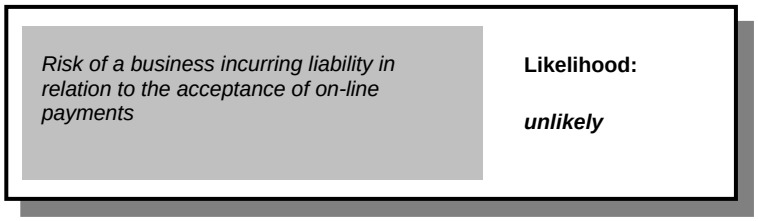
[636] Tim Boreham, "Call to post banks Net fraud bills, *The Australian*, 19 March 1999, http://www.theaustralian.com.au/masthead/theoz/state/4379100.htm.

> For example, in the case of a stolen laptop computer, Arnold explains, "There's the actual price of the laptop, the storage and shipping cost, the 3% discounted creditcard service fee paid to the card companies and banks, and then the additional fee of [US]$1-10, which is a chargeback fee when a customer denies a charge." For this reason, it is easy to see how even one fraudulent sale can take a big bite out of a merchant's profits, and why online merchants can't afford to ignore this problem[637].

5.9.3 ANALYSIS OF THE LIKELIHOOD OF THE RISK EVENTUATING

The *likelihood* of this legal risk, as concluded in the discussion that follows, is depicted in Figure 24:

Figure 24 EVALUATION OF THE LIKELIHOOD



A business that accepts on-line payments, whether the payments are made by credit card, secure credit card or any other form of electronic funds transfer, digital cash or electronic cheque, faces three contractual risks: (i) that the payment made will be dishonoured by the issuer of the form of payment used by the customer (for example, where payment has been accepted in the form of digital cash, the digital cash issuer may refuse to honour the payment on the ground that the digital cash proffered by the business's customer was forged, or, if payment was effected by

---

[637] Lucie Kim, Staff Writer, E-Commerce Times, "Report: Online Shopping Fraud Bites Merchants,

electronic cheque, the cheque bounced), (ii) that a customer makes a payment on-line but subsequently repudiates that payment by falsely claiming that the payment was made by an imposter[638] and (iii) that the payment is made by an imposter and consequently will be repudiated by the party whom the imposter purported to be[639].

A relevant factor in analysing the likelihood of risk is that that all new forms of on-line payment incorporate security mechanisms to prevent forgery and to protect against false repudiation by a customer. Furthermore, in relation to the acceptance of credit card payments, mechanisms have been developed and are starting to be implemented, such as the Secure Electronic Transaction protocol, which make it increasingly difficult for an imposter or a forger to make on-line payments, or for a customer to repudiate a payment made by falsely claiming that the payment was made by an imposter.

In relation to the risk that payment is made by an imposter and is consequently repudiated by the party whom the imposter purports to be, the most likely instance in which this circumstance will arise is when a customer has fraudulently obtained the credit card details and identity of a third party. Credit card payment on-line is probably the most vulnerable to misuse by imposters compared to other forms of payment such as digital cash or electronic cheques for two reasons. The alternative forms of on-line payment available are usually only available for use in relation to

---

Not Buyers", *E-Commerce Times*, December 4, 1998 http://www.ecommercetimes.com/news/articles/981204-1a.shtml.

638 Henry H Perritt, Jr, "Payment Infrastructures for Open Systems", 1995, http://ming.law.vill.edu/chron/articles/dir.htm.

639 Henry H Perritt, Jr, "Legal and Technological Infrastructures for Electronic Payment Systems",

on-line payments. Thus, the only way in which an imposter can obtain the details about a party's "account" is by intercepting an on-line payment. In contrast, payment by credit card is used far more widely (payment by credit card is a common form of payment in relation to commerce conducted off-line), and consequently the opportunities for an imposter to intercept details of a party's "account" are far greater. Also, it may be easier to intercept "account" details of a party's credit card when used off-line, as the Internet-only forms of payment usually incorporate security protection mechanisms, such as encryption of "account" information which are often not employed in relation to credit card payments made in the context of commerce conducted off-line (eg when credit card payment is made by the telephone, or payment is made by credit card in a store the "account" details of the credit card are not encrypted)[640].

In view of the increased use or implementation of secure methods of effecting on-line payment such as Secure Electronic Transaction protocol, however, the likelihood of this risk eventuating is reduced:

> According to Melissa Bane, an industry analyst with the Yankee Group, "Online credit card fraud may be on the rise as more consumers join in online commerce, but proportionately, incidents of fraudulent charges aren't really increasing."

1996, 22 *Rutgers Computer & Technology Law Journal* 1, p 30.

640 See for example, the instance documented in Scam Watch, " Businesses pay the price for online credit fraud" by Steve Gillmor, *MoneyCentral Microsoft, 14 August 1998*, http://moneycentral.msn.com/articles/smartbuy/scam/1546.asp quoting an executive from the company ClearCommerce: "Stealing a legitimate number -- last Christmas we helped some merchants uncover this kid who would go in Dillards', watch people sign their credit card receipts, and write down the number. Then he went back to his home computer and started placing orders for computer hardware, T-shirts and games."

> Erina DuBois, analyst at the Gartner Group, agrees. "Due to better technology and increased awareness, we're seeing an overall decline in fraud as a result of stolen credit card numbers."
>
> Phillip Windley, Chief Technology Officer of iMall, a popular shopping community site, reports that, "The actual incidence of online fraud is very small. It is the case that merchants get bad credit card numbers, that are either stolen or fabricated, as an offer of payments for goods, particularly for high-cost items, like computers and electronic goods. However, in most cases, it is immediately obvious."[641]

In contrast with the other legal risks discussed in this chapter, some quantitative data is available in relation to one aspect of this risk. This is because businesses regularly keep data on how many Internet transactions are fraudulent. The term fraudulent can encompass a number of circumstances but here it is assumed that it applies to Internet transactions where a party repudiates an Internet transaction by falsely claiming that the on-line payment was made by an imposter and where the on-line payment is made by an imposter and consequently is repudiated by the party whom the imposter purports to be. Based on the data that is publicly available, approximately 1% of Internet transactions are fraudulent[642] although for individual companies amounts up to 20% have been reported and one company that provides anti-fraud services estimates that 5-6% of a net business's transactions are

---

641 Lucie Kim, Staff Writer, E-Commerce Times, "Report: Online Shopping Fraud Bites Merchants, Not Buyers", *E-Commerce Times*, December 4, 1998 http://www.ecommercetimes.com/news/articles/981204-1a.shtml.

642 See for example, Kara Swish, "Seller Beware Consumers Aren't the Only Ones Who Risk Being Swindled Online", *Wall Street Journal Interactive*, December 7, 1998, http://interactive.wsj.com/public/current/articles/SB912732372726038000.htm. See also Gregory Dalton, "Visa And CyberSource Target Online Fraud", *InformationWeek*, (09/01/99, 8:02 p.m. ET), http://www.techweb.com/wire/story/TWB19990901S0026 who reported that "Jim Degracia, senior vice president for electronic commerce at Visa, said fraud rates for online sales are .09 percent, slightly higher than the .08 percent for off-line sales".

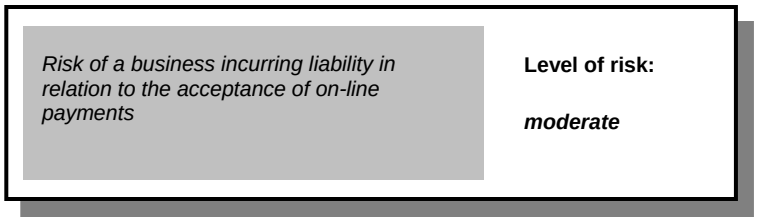
643 Craig Bicknell, "Credit Card Fraud Bedevils Web", *Wired News*, 2 April 1999, http://www.wired.com/news/print_version/business/story/18904.html?wnpg=all.

fraudulent[643]. Interestingly, it is reported that Internet fraud rates actually are lower than their traditional mail and telephone order counterparts. Unfortunately no data is publicly available in relation to the other aspect of this risk, the risk that an on-line payment made by a customer will be dishonoured by the issuer of the form of payment used by the customer[644]. Overall, the likelihood of this risk is categorised as *unlikely*, that is the risk could eventuate at some time.

5.9.4 LEVEL OF RISK

The *level* of this legal risk, as concluded in the discussion that follows, is depicted in Figure 25:

Figure 25 EVALUATION OF LEVEL OF RISK



As noted at 5.9.2 at p 384, the consequence of the risk of a business incurring liability in relation to the acceptance of on-line payments will depend on the value of the transaction, as well as the fees imposed by the issuer of the form of payment the

644 Scam Watch, " Businesses pay the price for online credit fraud" by Steve Gillmor, *MoneyCentral Microsoft, 14 August 1998,* http://moneycentral.msn.com/articles/smartbuy/scam/1546.asp.
645 Tips provided by the founder of AntiFraud.Com at http://www.antifraud.com/tips.htm.

business accepts (such as the service fee paid to credit card companies and the chargeback fee when a customer denies a charge). The *consequence* was assessed as being *medium* given these costs. The *likelihood* of this risk was assessed at as being *unlikely*, that is the risk could eventuate at some time. This is because most Internet commerce systems employ mechanisms that check for on-line fraud. As the *consequence* of this risk is *medium* and the *likelihood* of risk is *unlikely*, the level of this risk is *moderate*. The evaluation of this legal risk is depicted in table form in Table 63 at p426.

5.9.5 SOME RISK MANAGEMENT STRATEGIES

An obvious *risk control* strategy in relation to each of the risks identified above is for a business to check whether a credit card used by a customer has been stolen although there will always be occasions where the loss of a party's credit card or the misappropriation of a party's "account" details has gone undetected and therefore has not been reported.

Another *risk control* strategy is to ensure that the business's e-commerce computer system employs mechanisms such as SET, which incorporate procedures for verifying a party's identity, such that an imposter is detected, or a party is precluded from repudiating a transaction by falsely claiming that the transaction was conducted by another party. In fact any system, which like SET uses digital signatures to verify the identity of the parties with whom a business transacts provides a useful *risk control* strategy. How digital signatures work and the risks associated with using

digital signatures are considered in more detail in the discussion immediately following.

A *risk control* strategy in relation to the risk that a payment will be dishonoured by the issuer of the form of payment used by a customer is to ensure that the business only accepts on-line forms of payment which the issuer guarantees to honour. In other words the risk is transferred from the business to the issuer.

Another *risk control* strategy includes not accepting an order unless complete information is provided including full address and phone numbers[645]. It has been suggested that orders originating from countries such as Romania, Pakistan, Russia and Belarus should be treated as suspect[646].

A similar *risk contro*l strategy is to not accept any order originating from a free, web-based, or E-mail forwarding address, that is the customer must provide an ISP or domain based address[647].

Another *risk control* strategy is to telephone the phone number provided by the customer in the customer's order:

> We have alerted many cardholders that their card information was being used by making this phone call.
>
> On the other hand, the party on the other end may have never heard of the"customer." This results in a call to the issuing bank of the credit card to alert their fraud department[648].

---

646 Advice given by Yahoo!Store to merchants participating in its online mall as reported in Lucie Kim, Staff Writer, E-Commerce Times, "Report: Online Shopping Fraud Bites Merchants, Not Buyers", *E-Commerce Times*, December 4, 1998 http://www.ecommercetimes.com/news/articles/981204-1a.shtml.

647 Tips provided by the founder of AntiFraud.Com at http://www.antifraud.com/tips.htm; and in Lucie Kim, Staff Writer, E-Commerce Times, "Report: Online Shopping Fraud Bites Merchants, Not Buyers", *E-Commerce Times*, December 4, 1998 http://www.ecommercetimes.com/news/articles/981204-1a.shtml.

Another *risk control* strategy is to not accept large orders[649].

A further *risk control* strategy is to not accept orders whose shipping address is different from the billing address[650].

A *risk control* strategy used by at least one business is to use the HTTP_USER_AGENT and REMOTE_ADDR code on all its order forms.

> This line works with most form handlers such as FormMail, cgi email and others. The exact syntax varies with the form handler, but it provides information on the computer used to send the order, including the IP address. The IP address can then be traced to its owner - usually an ISP. You can then contact the ISP System Administrator and inform them of the illegal activity. Members are provided an automated way to do this. Check the documentation for your particular form handler or cgi script for implementation of this input field[651].

In relation to accepting electronic checks a *risk control* strategy is for businesses to telephone the account holder's bank and verify the account number, account holder's name and current funds to clear the check before processing the order[652].

Another *risk control* strategy is to use antifraud services such as Cybersource, where each Internet transaction is analysed on-line and scored as to its likelihood of being a legitimate purchase, and ClearCommerce, a software application that identifies and blocks typical fraudulent patterns[653]. Interestingly, Visa will give businesses who use Cybersource to reduce the incidence of fraud, what has been

---

[648] Tips provided by the founder of AntiFraud.Com at http://www.antifraud.com/tips.htm.
[649] Lucie Kim, Staff Writer, E-Commerce Times, "Report: Online Shopping Fraud Bites Merchants, Not Buyers", *E-Commerce Times*, December 4, 1998 http://www.ecommercetimes.com/news/articles/981204-1a.shtml.
[650] Kim, http://www.ecommercetimes.com/news/articles/981204-1a.shtml.
[651] Tips provided by the founder of AntiFraud.Com.
[652] Tips provided by the founder of AntiFraud.Com.

termed a "significant"discount off the approximately 2 percent-3 percent it charges them to process credit card transactions[654]. In addition, technologies are presently being developed that are designed to turn Internet transactions into the equivalent of face-to-face transactions[655]:

> A new security system championed by IBM and others is one as well as one promoted by Netscape, while banks and credit card companies such as Bank of America and Visa are promoting smart cards[656].

A *risk control strategy* which, for reasons of cost and inconvenience imposed on the customer (the customer has to obtain a public and private key and a digital certificate) is more likely to be taken up in relation to business-to-business Internet commerce, is for a business to configure its on-line payments system such that on-line payment is accepted only if a digital signature is used by the customer. In this way, the business could verify the identity of its customer by using the customer's public key. This would considerably reduce the risk that a business conducts Internet commerce with a party that is an imposter, or with a customer who later falsely repudiates the transaction. A more detailed discussion of how digital signatures work and their use as a risk management strategy is discussed at 5.10 at p397.

A *risk transfer* strategy is to obtain insurance. One insurance company, an Atlanta-based insurance and risk management firm, Hamilton Dorsey Alston Co., offers

---

653 Kim, http://www.ecommercetimes.com/news/articles/981204-1a.shtml and Steve Gillmor, Scam Watch, " Businesses pay the price for online credit fraud" *MoneyCentral Microsoft, 14 August 1998,* http://moneycentral.msn.com/articles/smartbuy/scam/1546.asp.

654 Gregory Dalton, "Visa And CyberSource Target Online Fraud", *InformationWeek*, (09/01/99, 8:02 p.m. ET),http://www.techweb.com/wire/story/TWB19990901S0026.

655 Gillmor, Scam Watch, http://moneycentral.msn.com/articles/smartbuy/scam/1546.asp.

656 Gillmor, Scam Watch, http://moneycentral.msn.com/articles/smartbuy/scam/1546.asp.

insurance policies with coverage up to $1 million that cover illegal electronic fund transfers and credit card theft. The company will insure Australian businesses[657]. The premiums, ranging from US$2,000 per year to US$60,000 per year, are calculated on the volume of transactions of the business's web site and the business's web revenue. The company commenced issuing insurance policies only to those business's whose Internet commerce web site is NCSA-certified, although Hamilton Dorsey Alston Co, foresees insuring non-certified businesses in the in the future as this area of insurance matures and data on the risks involved is collected[658].

There is, however, an option for transferring this risk for those businesses that use a certain type and class of VeriSign Digital IDSM Certificate in relation to receiving online payments. This is because VeriSign offers a protection plan, called the NetSureSM Protection Plan whereby it will assume the risk associated with certain occurrences including where a business relies on the certificate provided by an imposter who impersonates a third party using a VeriSign digital certificate[659]. The amount that VeriSign will pay by way of compensation is limited by the Class of digital certificate used by the imposter. This amount ranges from $1,000 for reliance on a Class 1 certificate to $100,000 for reliance on a Server Certificate. A claim made by a business in instances where a party has impersonated a third party using a

---

657 Sari Kalin, IDG News Service, "NCSA to assure secure transactions by certifying Web sites", *Netscape World*, August 1996, http://www.netscapeworld.com/netscapeworld/nw-08-1996/nw-08-ncsa.html.

658 Kalin, IDG News Service, http://www.netscapeworld.com/netscapeworld/nw-08-1996/nw-08-ncsa.html.

Verisign digital certificate will reduce the available certificate lifetime limit of the business's NetSureSM Certificate. This in effect reduces the amount that a business can claim if this risk eventuates again.

5.9.6 EVALUATION OF RISK MANAGEMENT STRATEGIES

As discussed earlier at 2.4.4.4.1 at p 102, it is useful to consider the *degree* of *consequence* and *likelihood* in determining which risk management strategy to adopt. Because the consequence of this risk is *medium* and the likelihood is *unlikely*, this type of risk should be retained and managed, provided the business has sufficient reserves. Retaining this risk is in accordance with another guiding principle discussed at 2.4.4.4.4 at p107, which is that a business should only retain risks over which it has control. Here a business faced with this legal risk can take steps to control the circumstances under which it transacts with and accepts payment from a customer. In addition, the business should manage the risk by adopting some or all of the risk management strategies discussed earlier at 5.9.5 at p391. Compared against the general risk criteria for a business conducting Internet commerce this would achieve the objective of protecting the business's legal rights and interests.

So what risk management strategy or risk management strategies should a business adopt? In terms of cost of implementation all of the risk management strategies may be costly in that they involve reconfiguring or modifying the business's Internet commerce software. The use of anti-fraud services such as Cybersource and

---

659 VeriSign, *NetSureSM Protection Plan*, Version 1.0 - June 20, 1997, https://www.verisign.com/repository/netsure/; VeriSign, *NetSureSM Protection Plan Summary*,

ClearCommerce is likely to involve even more cost to the business to implement. The use of digital signatures not only involves a cost to the business but also may deter potential customers who will also have to acquire digital signature software and digital certificates in order to transact with the business. Without reference to a specific business, and knowledge of its particular needs and the products or services that it sells, it is difficult to definitively state which risk management strategy should be implemented by a business. A business in weighing the cost of implementing an option against the benefits it brings should, however, keep in mind that it is preferable if possible to transfer this risk by way of insurance and if that is not possible, because this risk level is high, retention of this risk without implementation of a risk management strategy or risk management strategies to reduce this risk is simply not an option.

The risk management strategies put forward and the recommended risk management strategies are set out in table form in Table 64 at p429.

5.10 The use of encryption and digital signatures as a risk management strategy

It is useful to examine more closely one particular risk management strategy that has been put forward in relation to some of the legal risks discussed in this chapter, that is the use of encryption and digital signatures. The discussion that follows involves examining what is encryption and how digital signatures work. The discussion will include examining in more detail how encryption and digital

---

https://www.verisign.com/repository/netsure/summary/.

signatures can be used to manage specific legal risks and the drawbacks of using this technology as a risk management strategy.

5.10.1 WHAT IS ENCRYPTION?

The term **"encryption"** refers to the technique of encoding data or information **("plaintext")** to render it into an unreadable form **("cyphertext")** except by those parties who know the code or cypher[660] **("key")** to decrypt the data or information. Encryption has several key applications in relation to Internet commerce: (i) it can be used to keep Internet communications private; (ii) it can be used to authenticate or verify that an Internet communication was sent by the party from whom the Internet communication is purported to be sent; (iii) it can be used to authenticate the integrity of an Internet communication, that is, verify that an Internet communication had not been altered after or during transmission; (iv) it can be used to prevent false repudiation of an Internet communication by a party on the ground that an imposter and not the party transmitted the Internet communication; and (v) it can be used to record the date on which an Internet communication took place through the use of time/date stamping.

There are several encryption software programs available for use in relation to Internet commerce. Basically, these programs fall into two categories, those that enable the use of encryption for e-mail (eg the software program, PGP (Pretty Good Privacy)) and those that enable the use of encryption for transactions conducted on

---

[660] When data or information is encrypted with a code, each character is replaced with a substitute character. When data or information is encrypted with a cypher, the data or information as a whole

the World Wide Web (eg. Netscape 3.0 provides for the use of encryption in relation to Internet transactions). There are two encryption techniques that are utilised in relation to Internet commerce: public key encryption and single key encryption. A simplified description of each technique is provided below.

5.10.2 WHAT IS SINGLE KEY ENCRYPTION?

Single key encryption (sometimes referred to as "symmetric encryption" or "synchronous encryption") is a form of encryption that uses a single key to encrypt and decrypt Internet communications. The key is generated randomly by a computer using a mathematical algorithm and, depending on the algorithm employed by the encryption software program (eg Data Encryption Standard (DES), International Data Encryption Algorithm (IDEA)), the key length can vary. In simple terms, the longer the key length is the harder the key is to "unlock".

Two drawbacks are associated with the use of single key encryption in relation to Internet commerce: first, it is not regarded as safe to exchange a key on the Internet; it is therefore necessary for transacting parties to organise to exchange the key securely off-line. Clearly this makes single key encryption unsuitable for Internet transactions that do not involve a continuing trading relationship, as it is unlikely that potential customers to a one-off transaction with a business would wish to incur the delay involved with exchanging a key off-line in advance; (ii) Secondly, because both parties must know the key, notwithstanding a party's efforts to keep the key secret,

---

is converted, rather than character by character. Roger Clarke, "Cryptography issues in plain text", *Privacy Law and Policy Reporter*, May 1996 Vol 3, No 2, p 24.

the key may nevertheless be compromised through the conduct of the other party. Single key encryption, however, is faster than the alternative form of encryption, public key encryption.

5.10.3 WHAT IS PUBLIC KEY ENCRYPTION?

Public key encryption (sometimes referred to as "asymmetric encryption" or "asynchronous encryption") involves the use by each transacting party of a mathematically matched pair of keys, a public key and a private key to encrypt and decrypt Internet communications. Like single key encryption, the matching keys are generated by a computer using a mathematical algorithm (such as RSA and Diffie-Hellman). It is 'computationally unfeasible'[661] to reverse calculate a private key from the public key even if the algorithm used to create the public key is known[662]. Again, key length can vary, the longer the key length the harder it is to "unlock" the key.

Unlike single key encryption, however, the keys are not shared between transacting parties. Rather, each party must have a matched pair of keys. The paired keys operate to separate the function of encrypting and decrypting an Internet communication. To encrypt an Internet communication a party must encode the Internet communication with the public key of the party with whom it transacts. Once encrypted, the Internet communication can be transmitted to the receiving party (eg by e-mail or World Wide Web) in privacy. To decrypt the Internet communication,

---

661 Charles R Merrill, "Cryptography for Attorneys-Beyond Clipper", 1994, http://ming.law.vill.edu/chron/articles/merrill.htm (a version of this article was published in *Data Law Report*, September 1994).

662 Lorijean G Oei, "Primer on Cryptography", in *Online Law : the SPA's Legal Guide to doing Business on the Internet*, Thomas J. Smedinghoff, editor, Addison-Wesley Publishing, Reading,

the receiving party must use its private key (the receiving party's public key *cannot* decrypt an Internet communication that has been encrypted with its own public key).

In order for public key encryption to function, a party's public key is made freely available to parties with whom the party seeks to transact. This can be achieved by "publishing" the public key in registries on the Internet or in newspapers or by the party individually disclosing its public key to the party with whom it is transacting (this aspect is considered in detail later in this chapter). A party's private key must be kept secret. Where a party's private key is compromised (eg it has been disclosed to unauthorised parties) a new key pair must be generated and both the earlier private key and public key must be revoked. Notice of the revocation will also need to be given and this is typically achieved by "publishing" the revocation in the public key registry in which the party's public key was "published".

Public key encryption eliminates the problem associated with single key encryption, that both transacting parties have access to the key that must be kept secret. This is because the key that must be kept secret in relation to public key encryption, the private key, is not shared. Public key encryption, however, does slow Internet communications, more so than single key encryption and for this reason it is often used in combination with single key encryption. For example public keys are used to exchange a single key, which is then used in that session only ("session keys")[663].

Massachusetts, 1996, p 501, para 31.3.

[663] Personal communication made by Professor Graham Greenleaf on around 18 February 2000.

5.10.4 WHAT ARE DIGITAL SIGNATURES?

In the context of Internet commerce, a digital signature is an encrypted attachment to an Internet communication that enables the receiving party to verify that the Internet communication it has received was actually sent by the party that purported to send it, and that the Internet communication was not altered during, or after, transmission. A digital signature can be attached to an Internet communication regardless of whether the contents of the communication are encrypted.

Two techniques are used for attaching digital signatures to Internet communications: (i) public key encryption and (ii) hash functions. Basically, the party transmitting the Internet communication employs a software program that applies a mathematical function known as a "hash function" to the Internet communication that is intended to be transmitted. The hash function converts the Internet communication into a fixed-length string of characters, called a hash value. The software program then encrypts the hash value using the transmitting party's private key. This encrypted hash value constitutes a digital signature. The digital signature is usually attached to the Internet communication and is then transmitted to the receiving party.

The receiving party verifies that an Internet communication was not altered during, or after, transmission, and that it was sent by the party purporting to send it by: (i) decrypting the digital signature using the transmitting party's public key and (ii) applying the same hash function employed by the transmitting party to the Internet communication. If the receiving party is able to decrypt the digital signature

this verifies that the party who purported to send the Internet communication actually sent the Internet communication. This is because only the transmitting party's public key can decrypt a digital signature encrypted with the transmitting party's private key[664]. If the Internet communication has not been altered after the transmitting party affixed its digital signature, the hash value calculated by the receiving party will match the decrypted digital signature. If an Internet communication has been altered during, or after, transmission, the decrypted digital signature will not match the hash value calculated by the receiving party. In this way the party receiving an Internet communication can verify that the Internet communication was sent by the party purporting to send it and that it was not altered during or after transmission.

Digital signatures are often used in combination with encryption. This enables a party to transmit an Internet communication in private, which additionally can be authenticated in relation to the sending party's identity and the Internet communication's integrity.

5.10.5 WHAT CONTRACTUAL RISKS CAN ENCRYPTION AND DIGITAL SIGNATURES ADDRESS?

As noted in the discussion of specific contractual risks, encryption and digital signatures can be used as a risk management strategy in relation to several contractual risks. The following section contains a discussion in more detail of how digital signatures can be used for such a purpose. This involves revisiting the risks for which the use of digital signatures was identified as a possible risk management strategy:

---

[664] Oei, p 47.

5.10.5.1 Digital signatures can be used to minimise the risk of incurring liability in relation to acceptance of on-line payment

Digital signatures can be used to minimise, if not eliminate, two of the risks identified with accepting on-line payment, namely: (i) the risk that a business accepts on-line payment made by an imposter that is subsequently repudiated by the party whom the imposter purports to be, and (ii) the risk that a party with whom the business transacts subsequently repudiates the payment by falsely claiming that the business transacted with an imposter.

If a business configured its on-line payments system such that on-line payment was only accepted if a digital signature was used, the business could verify the identity of its customer by using the customer's public key. This would considerably reduce the risk that a business conducts Internet commerce with a party that is an imposter, or with a customer who later falsely repudiates the transaction.

But in order to ensure that customer is who the he or she purports to be it is necessary for a business to check that the customer has not assumed another party's identity and simply generated its own matched pair of keys in that party's name. One solution that has been developed in response to this problem is public key certification. Public key certification involves the certification (as to identity and sometimes other information such as country of residency and age of the key holder) of a party's public key by a Certification Authority. For a fee, and after producing evidence of identity (such as a driver's licence or passport), a Certification Authority will certify a party's public key. A business that transacts with a customer whose public key has been certified by a Certification Authority can then check that the

customer is whom the customer purports to be by checking the customer's identity with the Certification Authority through Certificate Revocation Lists (CRLs).

By taking this additional step, a business may be able to transfer the risk of conducting commerce with an imposter. This is because if a Certification Authority erroneously or negligently verifies a customer's key, the business would be likely to have a cause of action in negligence against the Certification Authority for wrongly certifying the customer's key.

In some overseas jurisdictions specific public key certification legislation has been enacted to facilitate the use of Certification Authorities and digital certificates. It is relevant at this point to briefly consider the most commonly cited example of such legislation, the Utah Digital Signature Act 1996[665]. Basically, in addition to according legal recognition of digital signatures, the Utah Digital Signature Act 1996 sets up a framework for the certification of public keys by Certification Authorities. It encourages Certification Authorities to provide key certification services by offering a licensing scheme for Certification Authorities[666] and limiting the liability of certification authorities that are licensed[667]. Provided that the certification authority has materially complied with the requirements set out in section of the Act, a Certification Authority is effectively granted immunity from any liability in the event that a party's public key was erroneously or negligently certified. In other

---

[665] Other legislation (mostly yet to be enacted or implemented) that creates a legislative framework for public key certification includes: the UNCITRAL Draft Uniform Rules on Electronic Signatures (12 December 1997); the Illinois Electronic Commerce Security Act (15 December 1997 draft) and the US Electronic Financial Services Efficiency Act 1997.

[666] Part 2 of the Utah Digital Signature Act 1996.

circumstances that give rise to exposure to liability, a mechanism exists for limiting the liability of a licensed Certification Authority. Details of these aspects are discussed later in this chapter. It should be noted that the legislative implementation of public key certification legislation has been criticised by some commentators, one argument being that all that is necessary is legislation that accords legal status to digital signatures and that to implement such legislation would give rise to 'a set of inappropriate rules that will fundamentally skew a dynamic infant marketplace and "lock in" a set of business models that the market would otherwise reject'[668]. In particular, the limitation of liability of Certification Authorities has been identified as shifting 'an immense liability burden' onto parties that use digital signatures[669]. The liability that a party is exposed to in the event that the party's private key is compromised and fraudulently used by another party, is substantially greater than the liability which a party would be exposed to in the analogous situation where the party's credit card number has been misappropriated and fraudulently used off-line:

> Under the Utah Act, the individual whose key was used to sign the document bears unlimited liability if they failed to exercise "reasonable care" to protect their private key. The Act also imposes difficult evidentiary burdens on the individual. So, if a subscriber (let's call her "Grandmom," just to put things in perspective) doesn't exercise due care, and her key is stolen resulting in losses totaling $25,000 prior to revocation of her key, that subscriber bears the loss--i.e., Grandmom loses her house. Or, if Grandmom does exercise due care and her key is still misappropriated, she must present a court with "clear and convincing" evidence (the standard under the Utah Act) to overcome the presumption that a document signed with her digital signature was in fact signed by her. In either case, the result doesn't comport with well-

---

667 Section 46-3-309 Utah Digital Signature Act 1996.

668 Bradford Biddle, "Public Key Infrastructures and "Digital Signature" Legislation: 10 Public Policy Questions", 3 March 1997, http://www.cooley.com/scripts/article.ixe?id=ar_1502, para 1.

669 C Bradford Biddle, "Legislating Market Winners- Digital Signature Laws and the Electronic Commerce Marketplace", 1997, http://www.w3journal.com/7/s3.biddle.wrap.html.

> established consumer protection laws (compared with the legislatively imposed $50 consumer liability limit for credit card losses, or the fact that one cannot be bound by a fraudulent handwritten signature). Moreover, no rational consumer would agree to accept this level of risk in a marketplace transaction. The benefits of having a certificate simply do not outweigh the very real possibility of facing extraordinarily large unreimbursed losses.[670]

At present no jurisdiction in Australia has implemented public key certification legislation. The policy direction that will be taken in Australia is presently unclear with differing policy stances being taken across National, State and even departmental divisions. The Electronic Commerce Expert Group Report has recommended against introducing a detailed legislative framework for digital and electronic signatures. Instead the Electronic Transactions Act 1999 (Cth) takes a "light touch" functional equivalence approach by implementing provisions that effectively give the same legal status to digital signatures as paper-based signatures. The Act does not, however, implement a public key authentication framework. The National Office for Information Economy (and, before the creation of this office, the Department of Communications and the Arts), however, has been spearheading the introduction of a national public key authentication framework which appears to involve the introduction of public key certification legislation. A paper written by the Office of Government Information Technology suggests that the proposed national authentication scheme will draw on the options set out in the Standards Australia publication, "Strategies for the implementation of a Public Key Authentication Framework (PKAF) in Australia" SAA MP75-1996. The preliminary report of APEC

---

[670] C Bradford Biddle, "Legislating Market Winners- Digital Signature Laws and the Electronic Commerce Marketplace", 1997, http://www.w3journal.com/7/s3.biddle.wrap.html.

Telecommunications Working Group has, in the form of an attachment, set out some particulars the public key certification legislation expected to be implemented in Australia. The information is in the form of answers provided to a questionnaire answered by APEC members, so the information is at best cursory. It is possible however to glean that public key certification legislation was anticipated and that such framework would limit the circumstances in which a Certification Authority could be liable. The framework did not, however, envisage following the Utah Digital Signature Act 1996, which additionally limits the measure of damages payable in the circumstances where a licensed Certification Authority is liable. It is further anticipated that Certification Authorities may only certify a digital signature if the standard of identification currently required to obtain a passport or open a bank account is met. The proposed framework also includes a scheme for cross-certification at both a national and international level. Details of the proposed national public key certification legislation are expected to be made publicly available in the near future.

At the State level, there is, at the time of writing, no legislative initiative for implementing a public key authentication framework although, as discussed earlier in this chapter, the Victorian Electronic Commerce Framework Bill (Vic) takes a similar approach to the Commonwealth Electronic Transactions Act 1999 (Cth) by adopting a functional equivalence legislative approach, and according digital signatures the same legal status as paper-based signatures.

Should, however there be enacted a national public key authentication framework or any such State legislation such legislation may affect the usefulness of requiring a customer to use a digital certificate as a mechanism for transferring the risks associated with accepting on-line payment to a Certification Authority, as they may limit the circumstances in which a Certification Authority is liable in negligence to a third party (in the context of the discussion here, liable to a business). Nevertheless for a business to refuse to do accept on-line payment from customers unless the payment is accompanied by a certified digital signature is in itself a risk control strategy in relation to the risks of conducting commerce with an imposter or with a customer who subsequently repudiates an Internet transaction by falsely claiming that an imposter entered into the disputed transaction and not the customer.

However, if a business requires its customers to use digital signatures when effecting on-line payment (whether certified or not certified), a business will severely limit its pool of potential customers, as presently the use of digital signatures, in the context of Internet commerce, is not widespread. Moreover, to require customers to utilise digital signatures when making on-line payments will add transaction costs to both the customer and the business as each party will have to acquire the relevant digital signature software. Further, if the business requires a customer's digital signature to be certified this will increase transactional costs. Therefore, the use of digital signatures to minimise the risks associated with accepting on-line forms of payment will only be cost effective if the value of the Internet transaction is high, or

if the business has a continuing trading relationship with the same customer, such as with business-to-business Internet commerce.

5.10.5.2 Digital signatures can be used by business to ensure effective incorporation of standard terms

As noted earlier at p 352, the requirement by a business that its customers attach digital signatures when signifying acceptance of a business's standard terms, is *unlikely* to satisfy the requirements for incorporating terms by way of signature. As some doubt exists as to the legal status of digital signatures at common law, it is not recommended that businesses use digital signatures as a risk management strategy until this uncertainty has been removed by digital signature legislation or judicially.

5.10.5.3 Digital signatures can be used by a business to minimise the risk of contracting with a party that is unauthorised to conduct Internet commerce

Earlier in this chapter at 5.10.5.1 starting at p404, the role of Certification Authorities was discussed. In addition to certifying a party's identity, a Certification Authority can, if it uses extensions such as the X.509v3 standard defined by the International Telecommunication Union, certify additional information such as the party's age and country of residence, and, where a party is acting on behalf of a principal, that the party is authorised to do so[671]. The X509 standard presently forms 'the basis for most certification schemes used on the Internet'[672]. A business can minimise the risk of entering into an Internet transaction with a party that is unauthorised to do so by requiring that each customer confirm that it is lawful

---

671 Dave Kosiur, "Role of Digital Certificates Looks Secure", *PC Week*, April 28, 1997, p 117.
672 "OOI Information Security Standards", http;//www2.echo.lu/oii/en/secure.html.

according to the laws of the country (or jurisdiction) in which the customer resides for the customer to engage in Internet commerce with the business. Such confirmation (which, for example, could take the form of an e-mail) could be accompanied by a certified digital signature which, in addition to certifying the customer's identity, specified details of the customer's age (if an individual) and country of residence. Such digital certificate could be checked by the business with a Certification Authority.

5.10.5.4 Digital signatures could be used to minimise the risk of being contractually bound to a term that was erroneously altered during or after transmission

A business could, by using digital signatures, ensure that a customer with whom it was conducting commerce would be alerted if the customer received an Internet communication that was erroneously altered during or after transmission. If, when communicating to a customer the terms on which a business is prepared to conduct commerce, a business attached a digital signature, a customer could if he or she checked the business's digital signature, detect if the proposed terms had been altered during or after transmission. This would minimise the risk that a business would be contractually bound to terms that were altered during or after transmission.

5.10.5.5 Digital signatures will satisfy the signature element of the Statute of Frauds writing requirement in some jurisdictions

The uncertain legal status of digital signatures at common law has been discussed earlier in this chapter at p286. Thus, only in relation to the Commonwealth jurisdiction where legislation has been enacted that equates digital signatures with

paper-based signatures can it be said definitively that the signature element of the Statute of Frauds writing requirement will be satisfied if digital signatures are used.

5.10.6 DRAWBACKS ASSOCIATED WITH THE USE OF ENCRYPTION AND DIGITAL SIGNATURES

Although the use of encryption and digital signatures may minimise a number of contractual risks associated with Internet commerce, there are several drawbacks associated with the use of encryption and digital signatures. Collectively these drawbacks raise doubts about the effectiveness and, in particular, the cost-effectiveness of adopting encryption and digital signatures for minimising the contractual risks associated with Internet commerce, particularly in relation to Internet transactions whose value is low. These doubts may well, in the future, dissipate once the use of encryption and digital signatures becomes more widespread, digital signatures are legislatively given the same effect as signatures and technically superior encryption software is developed. For the time being, however, business should be aware that the use of encryption and digital signatures does carry with it a number of drawbacks which may adversely affect the cost effectiveness of their use.

The drawbacks associated with the use of encryption and digital signatures are as follows:

5.10.6.1 Encryption not error free

Encryption and digital signatures, or more accurately the software programs that enable their use in relation to Internet commerce are not error free. This in turn creates risks for businesses that utilise encryption and digital signatures. For example, in September 1995, '...two Berkeley graduate students discovered a flaw in

Netscape's implementation of the RSA algorithm, which allowed them to decrypt encrypted messages in a matter of seconds.'[673] Thus, a business, by using encryption and digital signatures as a risk management strategy, in turn risks introducing an additional risk, that is the risk that the business's key or its customers' keys can be cracked, which in turn brings about the risk of being defrauded through an imposter purporting to act on behalf of the business or assuming the identity of a party whose digital signature has been cracked by the imposter.

It is by no means suggested that the degree of risk is so high that a business should not use encryption and digital signatures, however it is important for a business to be aware that the use of encryption technologies will not be entirely error free and their use can expose the business to additional risks. Moreover, as newer technical solutions are being developed the degree of risk associated with encryption software that is not error-free will lessen.

5.10.6.2 Lack of interoperability in encryption and digital signature software

Another drawback associated with the use of encryption and digital signatures is that, at least for the time being, the software that enables the use of encryption and digital signatures in relation to Internet commerce is not often inter-operable: 'A key challenge today in relation to open electronic commerce and open communications is the coherence of, and interworking between formal standards and publicly available and other specifications for end-to-end security between parties who may not be

---

[673] C. Bradford Biddle, "Comment: Misplaced Priorities: The Utah Digital Signature Act and Liability Allocation in a Public Key Infrastructure", Summer, 1996, 33 *San Diego Law Review*

known to each other'[674]. There are several reasons for the non-interoperability of encryption and digital signature software programs.

First, several protocols[675] exist for utilising encryption in relation to the Internet and software. Basically they can be divided into two categories, those protocols that enable the use of encryption for Internet commerce conducted via the world wide web (Secure Sockets Layer (SSL) and Secure Hypertext Transfer Protocol (SHTTP)) and those protocols that enable encryption to be used for e-mail (there are several protocols, such as Secure Multipurpose Internet Mail Extensions (S/MIME), MIME Object Security Services (MOSS), Message Security Protocol (MSP) and Privacy Enhanced Mail (PEM)). As a rule, software programs that follow different protocols are not compatible with each other although it is understood that with the development of Cryptographic Application Programming Interfaces it is possible for software to support multiple methods of encryption[676].

Secondly, as described earlier in this chapter at pp398 - 400, there are two forms of encryption that are utilised in the context of Internet commerce, public key encryption (asymmetric encryption) and single key encryption (symmetric

---

1143, pp 1184-1185 .

674 OOI Information Security Standards", http://www2.echo.lu/oii/en/secure.html.

675 There are several protocols for utilising encryption in relation to Internet transactions. Basically they can be divided into two categories, those protocols that enable the adoption of encryption in relation to Internet commerce conducted via the world wide web and those protocols that enable encryption to be used for e-mail. There are two protocols available for using encryption on the world wide web, Secure Sockets Layer (SSL) and Secure Hypertext Transfer Protocol (SHTTP). In relation to the use of encryption for e-mail there are several protocols including Secure Multipurpose Internet Mail Extensions (S/MIME), MIME Object Security Services (MOSS), Message Security Protocol (MSP) and Privacy Enhanced Mail (PEM).

676 Dorothy E Denning, "Encryption Policy and Market Trends", February 19, 1997, http://guru.cosc.georgetown.edu/~denning/crypto/Trends.html.

encryption). Some software programs utilise only one form of encryption. Others use a combination of public key and single key encryption (especially those that provide for digital signatures). Again, software programs that differ in the forms of encryption utilised will not generally be inter-operable.

Finally, non-interoperability can also arise even when the transacting parties use the same software program. For example the software program may not be interoperable across platforms (for example an encryption and digital signature software program for use on PCs may not be interoperable with the same software program for Macintosh computers). Also, the same program may not be interoperable between applications. For example, an encryption and digital signature software program for use with the Internet Explorer web browser may not be interoperable with the Netscape Navigator web browser. Further non-interoperability may also arise where the bit length of the code or cypher utilised by each party differs. For example, even if transacting parties use RSA's encryption software programs they may not be interoperable because they use different size keys.

The lack of interoperability considerably reduces the usefulness of encryption and digital signatures as a risk management strategy. Clearly the number of customers with whom a business can transact will be limited if a business insists that its customers use digital signatures and encryption according to its specifications only. Customers who wish to transact with a business which imposes such requirements may find that, even if they already own digital signature and encryption software, they must acquire different software so as to achieve compatibility with the

business's software. Whilst this problem is likely to disappear as protocols are implemented that allow interoperability, for at least the time being, the use by a business of encryption and digital software, and the requirement that its customers use this, will discourage customers. Again, it is important for businesses to be aware of this drawback associated with using encryption and digital signatures.

5.10.6.3 It may not be possible when a dispute arises to verify digital signatures that are used today

Digital signature technology is constantly evolving in such a way that it may not be possible in the future to verify digital signatures that are used today:

> We have already seen that the formatting of data is changing continuously. It appears that digital signature standards are also likely to undergo continuous evolution. Hashing algorithms that have been used in the short history of digital signatures include MD2, MD4, MD5, and the Secure Hashing Algorithm - 1 (SHA-1). There are frequent proposals for improving upon these algorithms as new cryptanalytic attacks are found, more efficient hashing mechanisms are devised, and computer hardware (for example the move from 16 bit to 32 bit machines) changes algorithm requirements. Similarly, the signature algorithms are undergoing rapid evolution in terms of cryptographic key size, and even adoption of entirely new cryptographic techniques, such as the move to elliptic curve based algorithms from those based on factoring products of prime numbers. The net result of all this constant improvement is that signatures applied to messages today will likely not be verifiable even ten years hence, unless verifying applications maintain a complex and ever growing array of hashing and signature algorithms. If the old signature and hashing algorithms were replaced for reasons of security, there is a question of whether the old signature should be verified at all.[677]

It is not impossible that a dispute arising in relation to an Internet transaction would arise after such time after the transaction was conducted that the digital signature is no longer verifiable, given the pace of technological change these days.

---

[677] David Fillingham, "A Comparison of Digital and Handwritten Signatures", Paper for MIT 6.805/STS085: Ethics and Law on the Electronic Frontier, Fall 1997, http://www-swiss.ai.mit.edu/6805/student-papers/fall97-papers/fillingham-sig.html.

This drawback is significant where digital signatures are used in relation to transactions involving a long term trading relationship, or a transaction whose performance may involve a long period of time, which is more likely to arise in relation to business-to-business Internet transactions. It should also be noted that digital signatures are more likely to be used in business-to-business Internet transactions than in business-to-consumer transactions, given the inconvenience and cost factor involved in using digital signatures in business-to-consumer transactions, and the fact that the value of business-to-business Internet transactions are greater.

5.10.6.4 Encryption and digital signatures are not "crackproof"

Another drawback associated with using encryption and digital signatures, to minimise the contractual risks associated with Internet commerce, is that neither technique is "crackproof". There are two ways in which encrypted Internet communications or digital signatures can be "cracked". First an Internet communication can be "cracked" through a party trying to guess the key. Secondly, an Internet communication can be "cracked" through a party trying to analyse the algorithm to deduce the key or decrypt the message from cypher text to plain text[678].

Presently it is considered that, in order to secure an Internet communication, a key length such as that used in Netscape Navigator 3.0, which offers 128-bit RC4 and 168-bit Triple-DES, is more than sufficient[679]. However, with the advent of faster

---

678 Lorijean G Oei, "Primer on Cryptography", in *Online Law : the SPA's Legal Guide to doing Business on the Internet*, Thomas J. Smedinghoff, editor, Addison-Wesley Publishing, Reading, Massachusetts, 1996, p 502, para 31.5.

679 Dorothy E Denning, "Encryption Policy and Market Trends", February 19, 1997, http://guru.cosc.georgetown.edu/~denning/crypto/Trends.html.

processors the optimum key length may well change. Each time a business is forced to upgrade its encryption and digital software to employ stronger encryption there will be additional transactional costs. In addition, each time a business upgrades its software, its customers too will have to obtain or upgrade their software so that it employs the same key length as the key length used by the business. This, too, adds transactional costs.

Finally, it should be noted that the US government presently bans the export from the US of cryptography and cryptographic products thatr employ more than 56 bit keys. Whilst encryption and digital signature software that employ longer keys is produced outside the US, the US accounts for more than 70% of the world's software[680]. Accordingly, even if an Australian business legally obtained encryption and digital signature software that used encryption strong enough to act as a deterrent there might be a problem with compatibility of that software (which is presumably developed outside the USA) with the software that its customers use, if its customers obtained encryption and digital signature software from the USA.

5.10.6.5 Lack of legal recognition of digital signatures

As discussed earlier in this chapter at p286, digital signatures are not presently accorded the status of signatures under *common law* in Australia. Again, it should be noted that the Electronic Transactions Act 1999 (Cth) accords digital signatures the same legal status as paper-based signatures. Similarly, the Electronic Commerce

---

[680] Review of Policy Relating to Encryption Technologies (The Walsh Report), February 1997, http://www.efa.org.au/Issues/Crypto/Walsh/walsh.htm, para 4.5.3.

Framework Bill (Vic), if passed, will accord digital signatures the same legal status as paper-based signatures. If digital signature legislation is enacted by only some jurisdictions, as is the case now where only the Commonwealth has enacted such legislation, and not on a national basis, the effectiveness of using digital signatures as a risk management strategy is limited to Internet transactions that are governed by the jurisdictions that have implemented such legislation. Thus, at present, if a business relies on using digital signatures as a risk management strategy, it faces the risk that such use will be effective only in relation to Internet transactions governed by Commonwealth law.

5.10.6.6 Use of digital signature technology adds transaction costs

As already noted, the use of digital signature technology will involve additional costs to conducting Internet commerce, such as the purchase by the business of the relevant software and the cost of upgrading the technology from time to time. In addition, the business will incur transactional costs associated with using the technology. It is rumoured that the cost to business of obtaining an X509 V3 certificate under SET will be US $10 for each certificate[681]. Clearly, a business contemplating a risk management strategy that involves the use of digital signatures will have to factor in this additional cost in determining whether to implement such a risk management strategy.

---

[681] E-mail to the ICA list from: sbaaaro@au1.ibm.com (Michael B. Aaron, IBM AP Finance Consulting(Australia)), Wed, 24 Mar 1999 09:18:59 +1100, Subject: RE: Westpac backs Camtech.

5.10.6.7 Public Key Infrastructure and its attendant legal risks

The use of public key certification in connection with the use of digital signatures and encryption brings about attendant legal risks. A national public key infrastructure framework may well address the drawbacks that are identified below. There is insufficient publicly available information about the national public key infrastructure initiative being developed by the Commonwealth government, however, to definitively confirm this. Moreover, the Electronic Commerce Expert Group Report recommended against implementing such a legislative framework. If such recommendation is followed the risks identified in this discussion will need to be managed by a business that uses digital signatures. The risks associated with public key certification include the following risks.

5.10.6.7.1 Risk that the Certification Authority is not legitimate.

If a business adopts as a risk management strategy the requirement that its customers use certified public keys the business faces a new risk, the risk that the customer's Certification Authority itself is not legitimate and colludes with a customer who is an imposter. It is therefore not only necessary for a business to check a customer's public key certificate but it is also necessary for the business to verify the customer's Certification Authority. A Certification Authority is typically verified by checking the public key certificate of the Certification Authority with a higher level Certification Authority whom the business can trust. This may involve checking several levels of public key certificates until the business is satisfied that the

Certificate Authority is legitimate. This in turn adds to transaction costs and time costs.

5.10.6.7.2 Risk that a Certification Authority's certificates are not reliable

At the moment, there is no uniform standard in Australia for Certification Authorities to employ when certifying a party's digital signature or public key. Accordingly, a business that requires its customers to use certified public keys, when conducting Internet commerce, cannot be certain that a Certification Authority has applied sufficiently stringent standards to guard against an imposter falsely obtaining certification. A business could address this issue by requesting, from the Certification Authority, a statement which specifies the procedures followed by the Certification Authority when certifying a public key and evaluating whether the standards employed by the Certification Authority are acceptable to the business. Clearly, to do so will add transaction and time costs to an Internet transaction.

The national public key infrastructure framework initiative, whose implementation in light of the Electronic Commerce Expert Group Report is now unclear, intended that a root authority would be set up which would be responsible for ensuring that Certification Authorities comply with set standards for certification[682].

5.10.6.7.3 Risk that certificate has been revoked

A party that uses certified digital signatures and encryption may discover that the security for its private key has been compromised. The party may subsequently

---

[682] APEC Telecommunications Working Group, Preliminary Report entitled TELWG16/BFSG/3.e/2, undated, http://www.apecsec.org.sg/telewg/16tel/bfsg/matrix/TELWG16-BFSG-3e-2.html.

decide to no longer transact business with the key pair, of which the private key has been compromised. A business therefore faces the risk of transacting with a customer whose key has been revoked which in turn gives rise to the risk of repudiation of the transaction by the customer. Typically, notice of revocation of a party's certified key pair is given in through certificate revocation lists[683]. Thus, a business that requires digital signatures and encryption to be used by its customers as a risk management strategy must additionally check that a customer's key has not been revoked by reference to certificate revocation lists. This adds transaction costs as well as time costs to the conduct of Internet commerce.

5.10.6.7.4 Risk that liability of a Certification Authority is excluded or limited

Another risk associated with the use of public key certification is the risk that, in the event that a Certification Authority provides a false or misleading certificate, liability of the Certification Authority is legislatively excluded or limited. Whilst it was suggested earlier that the use of public key certification could in itself constitute a risk management strategy, because it would result in the transfer of risk to a Certification Authority, a business should be aware that liability of the Certification Authority may be limited legislatively.

At present, because no public key authentication framework legislation exists in Australia the ordinary rules of negligence (and statutory derived causes of action under the Trade Practices Act 1974 (Cth) and State and Territory Fair Trading Acts)

---

683 C Bradford Biddle, "Comment: Misplaced Priorities; The Utah digital Signature Act and Liability Allocation in a Public Key Infrastructure", Summer, 1996, 33 *San Diego Law Review* 1143, pp 1151-1152 .

will apply in the event that a Certification Authority provides a false or misleading certificate. It is relevant to note that the national public key infrastructure initiative proposes to limit the liability of Certification Authorities[684]. The extent to which liability would be limited, however, is unknown, although again it is understood that the Australian scheme does not propose to follow the Utah Digital Signature Act 1996. The Utah Digital Signature Act, in addition to excluding the liability of a Certification Authority in specified circumstances, limits the liability of licensed Certification Authorities exposed to liability to an amount not exceeding the 'recommended reliance limit'[685] where there is a 'loss caused by reliance on a misrepresentation in the certificate of any fact that the licensed certification authority is required to confirm'; or a failure by the Certification Authority to comply with the procedural standards set out in the Act. The recommended reliance limit is a maximum value specified by the Certification Authority and the party whose public key is certified for which the certificate can be relied[686]. Under the Utah Digital Signature Act 1996, a licensed Certification Authority's liability is further limited to paying compensatory damages only. Liability for punitive or exemplary damages, damages for lost profits or opportunity, damages for pain and suffering[687] are expressly excluded by the Utah Digital Signature Act where the Certification Authority is licensed. Again it should be noted that the Electronic Commerce Expert

---

684 APEC Telecommunications Working Group, Preliminary Report entitled TELWG16/BFSG/3.e/2, undated, http://www.apecsec.org.sg/telewg/16tel/bfsg/matrix/TELWG16-BFSG-3e-2.html.
685 Subsection 46-3-309 (2) of the Utah Digital Signature Act, 1996.
686 Subsection 46-3-309 (2)(b) of the Utah Digital Signature Act, 1996.
687 Subsection 46-3-309 (2)(c) of the Utah Digital Signature Act, 1996.

Group has recommended against implementing a legislative framework in relation to the use of digital signatures beyond ensuring the legal effect of their use and ensuring their functional equivalence with paper-based signatures.

5.10.6.8 Risk of liability if key is lost

A further risk faced by businesses that adopt digital signatures and encryption is the risk of incurring liability if the business compromises the security of its private key. Obviously, if a business loses or otherwise compromises its private key the business will be exposed to the risk that another party will obtain access to and uses the business's private key. In order to manage this additional risk, a business must implement mechanisms for protecting its private key and for detecting a security compromise of the business's private key and for revoking the business's key certificates as soon as a loss is discovered. This will add to a business's transaction costs.

5.10.7 SUMMARY OF THE LEGAL RISKS ASSOCIATED WITH THE USE OF DIGITAL SIGNATURES

To summarise, the use of encryption and digital signatures as a risk management strategy itself creates additional risks and costs. For the reasons outlined above, the use of encryption and digital signatures as a risk management strategy, at present, has many drawbacks. Furthermore, given that not only must the cost of using encryption and digital signatures be borne by a business, but also by each of its customers, who must also acquire an encryption and digital software program that is compatible with the encryption and digital signature software employed by the business, the use of encryption and digital signatures may even discourage customers from transacting

with the business. For these reasons, it may well be that the use of encryption and digital signatures to minimise the contractual risks associated with conducting Internet commerce may not, at present, be cost effective.

5.11 Outcome of applying step 3 in relation to Internet commerce

The outcome of step 3 of the legal risk management process as applied in relation to Internet commerce is summarised in the following table:

Table 63 LEGAL RISK MANAGEMENT IN RELATION TO INTERNET COMMERCE

STEP 3	SELECTED LEGAL RISKS	CONSEQUENCES OF RISK EVENTUATING	Conseq-uence rating[a]	Likeli-hood rating[b]	Level of risk[c]	Risk priori ty (level #)
ANALYS-ING THE IDENTIF-IED LEGAL RISKS	The risk that an Internet transaction is unenforceable for failure to satisfy the Statute of Frauds writing requirement.	The consequence of this legal risk eventuating is that a business cannot enforce an Internet transaction, which is subject to, but does not comply with, the Statute of Frauds writing requirement.	low	unlikely	low (acceptable)	level 4
	The risk that a business becomes contractually bound to terms unintentionally.	The loss that a business would incur if this risk eventuated would be the cost associated with being contractually bound to an Internet transaction on terms that the business can't or would rather not fulfil. In such circumstances, if the business failed to fulfil its contractual obligations the business would be liable for breach of contract. Under contract law, the measure of damages payable to a plaintiff for breach of contract is the amount of money necessary to place the innocent party (plaintiff) in the position he or she would have occupied if the contract had been performed[688]. Thus, where a business is selling products or services to a consumer through the Internet the amount of damages would, at the very least, be the cost to the consumer of obtaining the products or services purchased from the business elsewhere. Where a business is engaged in business-to-business Internet commerce the amount of damages payable could be considerable as there is greater scope for a plaintiff to establish that, not only should the plaintiff should be compensated for having to obtain the business's services or products elsewhere, but that the plaintiff should be compensated for any losses incurred by the plaintiff resulting from the business's breach of contract, such as the plaintiff's inability to meet a deadline for a contract with a third party that relied on the defendant business meeting its contractual obligations. If, on the other hand a business performed its contractual obligations, the consequences if this risk eventuated would be that the business could incur loss, if to perform the contractual obligation was not profitable or resulted in reduced profits.	medium	unlikely	moderate (must be treated)	level 3
	The risk that an acceptance communicated by a business does not give rise to a binding contract.	The loss that a business could incur should this risk eventuate is the cost to a business associated with losing a "sale" or "contract" as a consequence of a customer having withdrawn an "offer" made to the business. Although it is difficult to generalise here, as the value of a lost sale or contract will differ according to the product or service provided by a business, it is unlikely that that the loss of a sale will have a more serious effect on a business than threatening the efficiency or effectiveness of the business's Internet commerce activities.	low	moder ate	moderate (must be treated)	level 3

[688] *Robinson v Harman* (1848) 154 ER 363 per Parke B.

[689] Robert I Mehr and Bob A Hedges, *Risk Management in the Business Enterprise*, Richard D Irwin Inc, Homewood, Illinois, 1963, p 258.

	The risk of incurring liability in relation to the acceptance of on-line payments.	The consequence of this risk is that a business will have to bear the loss associated with a repudiated on-line payment. The amount of loss will depend on the contractual agreement entered into by the business with the issuer of the form of payment the business accepts. For example, the loss a business will incur if the business accepts payment by credit card can include the value of the transaction, storage and shipping costs, 3% credit card fee paid to the credit card issuer and the chargeback fee.	medium	unlikely	moderate (must be treated)	level 3
	The risk that a customer is not contractually bound to standard terms purportedly incorporated by a business.	The consequence to a business should this risk eventuate is the cost to the business of having to transact with a customer without being able to rely on the terms which the business had sought to incorporate. What this cost will be will, of course, depend on the terms that the business sought unsuccessfully to incorporate.	very high	unlikely	severe (must be treated)	level 2
	The risk that a business enters into a contract that is invalid because it was unauthorised.	The consequence of this risk eventuating is that an Internet transaction entered into under these circumstances is invalid at law. Any Internet transaction subsequently repudiated by the party with whom a business is transacting or believed it was transacting, will not be enforceable.	medium	moderate	severe (must be treated)	level 2

SCALE USED FOR CLASSIFYING CONSEQUENCE OR IMPACT OF A LEGAL RISK EVENTUATING

Extreme	The consequences would threaten the survival of not only the business's Internet commerce activities, but also the business, possibly causing major problems for clients, the administration of the business's Internet commerce activities or a large part of the public sector.
Very high	The consequences would threaten the survival or continued effective function of the business's Internet commerce activities or require the intervention of top level management
Medium	The consequences would not threaten the business's Internet commerce activities but administration of the business's Internet commerce activities could be subject to significant review or changed ways of operating.
Low	The consequences would threaten the efficiency or effectiveness of the business's Internet commerce activities but can be dealt with internally.
Negligible	The consequences are of negligible consequence to the business.

SCALE USED FOR CLASSIFYING LIKELIHOOD OR FREQUENCY OF LEGAL RISK

Almost certain	The risk will eventuate in most circumstances.
Likely	The risk will probably eventuate in most circumstances.
Moderate	The risk should eventuate at some time.
Unlikely	The risk could eventuate at some time.
Rare	The risk may eventuate only in exceptional circumstances.

SCALE USED FOR CLASSIFYING LEVEL OF RISK

Extreme risk (level 1)	Must be managed by senior management with a detailed plan.
Severe risk (level 2)	Detailed research and management planning required at senior level.
Moderate risk (level 3)	Manage by specific monitoring or response procedures.
Low risk (level 4)	Manage by routine procedures.

As can be seen from Table 63 at p426, only one legal risk can be considered "acceptable" , that is, capable of being retained by a business without implementation of a risk management strategy or risk management strategies to further minimise the risk. That legal risk is the risk that an Internet transaction is unenforceable for failure to satisfy the Statute of Frauds writing requirement. All the other legal risks must be "treated", that is risk management strategies to minimise the legal risks must be implemented.

The following table sets out the legal risks in order of priority, the risk management strategies available and the recommended risk management strategies.

Table 64 LEGAL RISK MANAGEMENT IN RELATION TO INTERNET COMMERCE- STEP 4

STEP 4	LEGAL RISKS LISTED IN ORDER OF PRIORITY ACCORDING TO THE LEVEL OF RISK (LEVEL #)	RISK MANAGEMENT STRATEGY/STRATEGIES AVAILABLE	RISK MANAGEMENT STRATEGY/ STRATEGIES SELECTED AND REASONS FOR SELECTION
	LEVEL 2 RISKS		
EVALUAT-ING AND SELECT-ING RISK MANAGE-STRATEG-IES MENT	The risk that a business enters into a contract that is invalid because it was unauthorised.	In relation to where a customer is prohibited at law from entering into a transaction with the business, the risk control strategy of requiring customers to use digital signatures which are certified as to a customer's age, country of residence, authority to contract or whatever factor it is necessary for the business to confirm in order that the particular Internet transaction entered into is authorised. In relation to Internet transactions which are prohibited in certain jurisdictions, the risk control strategy of blocking transactions with customers whose Internet service provider domain falls within one of those jurisdictions and, in the case of the sale of tangible goods, to block transactions whose delivery address falls within a jurisdiction that prohibits such transactions. In relation to where a party with whom the business transacts purports to have but lacks authority to act on behalf of a principal, the risk control strategy of incorporating as a contractual term of any transaction with its customers a term reflecting Article 13(3)(b) of the UNCITRAL Model Law on Electronic Commerce.	As this risk is *medium* in consequence and moderate in *likelihood*, this type of risk is likely to be too costly to transfer by way of insurance. This risk should therefore be retained and managed. To retain this risk is also consistent with the principle that a business should only retain those risks over which it has control. Assuming this risk is retained by a business, it will be necessary for the business to implement risk management strategies, such as those put forward, to minimise this risk. As the level of risk is categorised as severe, it is recommended that this risk be brought to the attention of senior management and that research and management planning be undertaken at that level.
	Risk that a customer is not contractually bound to standard terms purportedly incorporated by a business.	If a business seeks to incorporate standard terms by way of signature, the risk control strategy of incorporating terms by way of typed signature (although the additional requirement imposed by section 10 of the Electronic Transactions Act (Cth) may affect the use of typed signatures t to incorporate terms in Internet transactions governed by Commonwealth law due to the appropriateness requirement.) or electronic signature rather than by digital signature, at least until digital signatures are legislatively or judicially accorded the status of signatures. If a business seeks to incorporate standard terms by way of signature, the risk control strategy of ensuring that the customer is made aware of the significance of typing in the customer's name or using an electronic "facsimile" signature (For example, the business displays on its web page containing the terms a conspicuous notice which states "By typing in your name [or by affixing your electronic signature], you have signified that you agree to the terms displayed on this page"). If a business seeks to incorporate terms by notice, the risk control strategy of ensuring that the display of the terms	According to risk management principles this type of risk should be transferred by way of insurance because the consequences of this risk are *very high* and the likelihood *unlikely*. It is not known whether a business can insure against this type of risk. If insurance cannot be obtained, or it is not cost effective for the business to obtain insurance against this risk, then the

		sought to be incorporated appears occurs in circumstances in which it is reasonable to expect such terms. In addition, attention must be drawn to the terms.	business must retain and manage the risk. In such circumstances, the business must implement risk management strategies to minimise its exposure to this risk given that the risk level is severe. In fact it is suggested that given the level of risk, this risk requires detailed research and management planning at senior level.
	LEVEL 3 RISKS		
	Risk of incurring liability in relation to the acceptance of on-line payments.	The risk control strategy of checking whether a credit card used by a customer has been stolen although there will always be occasions where the loss of a party's credit card or the misappropriation of a party's "account" details has gone undetected and therefore has not been reported. The risk control strategy of ensuring that the business's e-commerce computer system employs mechanisms such as SET, which incorporate procedures for verifying a party's identity, such that an imposter is detected, or a party is precluded from repudiating a transaction by falsely claiming that the transaction was conducted by another party. In relation to the risk that a payment will be dishonoured by the issuer of the form of payment used by a customer, the risk control strategy of ensuring that the business only accepts on-line forms of payment which the issuer guarantees to honour. In other words the risk is transferred from the business to the issuer. The risk control strategy of not accepting an order unless complete information is provided including full address and phone numbers. It has been suggested that orders originating from countries such as Romania, Pakistan, Russia and Belarus should be treated as suspect. The risk control strategy of not accepting any order originating from a free, web-based, or E-mail forwarding address, that is the customer must provide an ISP or domain based address. The risk control strategy of telephoning the phone number provided by the customer in the customer's order. The risk control strategy of not accepting large orders. The risk control strategy of not accepting orders whose shipping address is different from the billing address. The risk control strategy used by at least one business is to use the HTTP_USER_AGENT and REMOTE_ADDR code on all its order forms. In relation to accepting electronic checks, the risk control strategy of telephoning the account holder's bank and verifying the account number, account holder's name and current funds to clear the check before processing the order. The risk control strategy of using antifraud services such as Cybersource where each Internet transaction is analysed on-line and scored as to its likelihood of being a legitimate purchase and ClearCommerce, a software application that identifies and blocks typical fraudulent patterns. The risk control strategy which, for reasons of cost and inconvenience imposed on the customer (the customer has to obtain a public and private key and a digital certificate) is more likely to be taken up in relation to business-to-business Internet commerce, of configuring the business's on-line payments system such that on-line payment is accepted only if a digital signature is used by the customer. In this way, the business could verify the identity of its customer by using the customer's public key.	Because the consequence of this risk is *medium* and the likelihood is *unlikely*, this type of risk should be retained and managed. To retain this risk is also consistent with the principle that a business should only retain those risks over which it has control. The business should manage the risk by adopting some or all of the risk management strategies identified. Without reference to a specific business, and knowledge of its particular needs and the products or services that it sells, it is difficult to definitively state which risk management strategy should be implemented by a business.

	Risk that a business becomes contractually bound to terms unintentionally .	Where a business's marketing and promotional activities on the Internet constitute making an "offer" rather than an "invitation to treat" The risk control technique of scrutinising all marketing and promotional activities on the Internet and ensuring that they cannot reasonably be understood as making "offers", unless it is so intended by the business. Where a business's purported withdrawal of an "offer" to a customer is precluded because the business's "offer" has been accepted by a customer The risk control strategy of incorporating a contractual term that is based on Article 15(a)(ii) of the UNCITRAL Model Law on Electronic Commerce, such that acceptance of a business's "offer" is deemed to take place when the Internet communication accepting the business's offer is retrieved by the business (regardless of whether the business has a designated information system). The risk control strategy of including, as a term of every transaction, a term that reproduces or replicates a strategy used in relation to contracts effected through Electronic Data Interchange, such as clause 10.2 of the Tradegate ECA Model EDI Trading Agreement. This clause effectively specifies that a transaction entered into by a business and a customer is governed by the instantaneous rule. Where during the course of negotiating the terms of an Internet transaction a "battle of the forms" situation arises such that the customer's terms override the business's. The risk control strategy of refusing to transact with a customer except under the business's terms. The risk control strategy of preventing a customer from completing an order (eg typing in or selecting order details from an order form on a web page that is then transmitted to the business) until the customer has signified acceptance of the business's terms, the rejection of which result in the customer being prevented from further progressing with the transaction. In relation to business-to-business Internet commerce, where variations of terms are more likely to be sought by customers and acceded to by a business, the risk control strategy of ensuring that a mechanism is put in place such that if terms upon which the parties agree to transact can and are varied by a customer that subsequent to any variation accepted, a follow-up communication is transmitted to the customer confirming the varied term and reiterating all other terms on which the business is prepared to transact. Where the terms of the contract negotiated between the business and a customer are altered by erroneous transmission The risk control strategy of requiring all customers' communications with the business to be "signed" with a digital signature. The risk control strategy of incorporating as a contractual term with its customers a term that reproduces or at least replicate the effect of Article 13(5) of the UNCITRAL Model Law on Electronic Commerce. Article 13(5) of the UNCITRAL Model Law on Electronic Commerce specifically precludes reliance on an Internet communication received by a party where that party knew or should have known that the Internet communication was erroneous. Where the business's computer software used for conducting Internet commerce is erroneously programmed or malfunctions so it makes or accepts offers in circumstances unauthorised by the business. The risk transfer strategy of outsourcing the production of the software used to conduct Internet commerce to a third party software developer or to purchase an off the shelf Internet commerce software package. Whilst this does not remove the risk that a business will be contractually bound to an Internet transaction on terms to which it did not intend to be bound by, the business may be able to recover the losses it has incurred as a consequence of wrongly programmed software from the third party developer, if the business ensures that a term of the software development	According to risk management principles this legal risk is the type of risk that a business should retain and manage, as the consequence of this risk is *medium*, and the likelihood of this risk is *unlikely*. To retain this risk is also consistent with the principle that a business should only retain those risks over which it has control. In addition to retaining this risk, the business should take steps to manage this legal risk. Based on an assessment that implementation is not expensive and that implementation will significantly minimise this legal risk, a business should adopt all except two of the risk management strategies put forward. The two risk management strategies excepted are the use of digital signatures and the outsourcing of the production of the software used to conduct Internet commerce to a third party. It is not, however, suggested that these two risk management strategies are not cost effective. Rather, given that the implementation of these two strategies will involve a cost to the business, it will be necessary for a business to weigh the cost of implementing these two options against the benefits of implementing these strategies before deciding whether to adopt these risk management strategies.

	or acquisition agreement provides for the recovery of losses incurred by the business as a consequence of an error or malfunction in the Internet commerce software. Furthermore, the business will need to ensure that it does not contract out its rights to sue for negligence in the event that the software is wrongly programmed. The risk control strategy of incorporating as a contractual term with all customers a term that reproduces or at least replicate the effect of Article 13(5) of the UNCITRAL Model Law on Electronic Commerce. As noted earlier, Article 13(5) precludes reliance by a party on an Internet communication received by the party which the party knew or ought to have known was erroneous.	
Risk that an acceptance communicated by a business does not give rise to a binding contract.	A risk control strategy for a business would be to implement a system such that the customer is required to confirm an order before the goods or services ordered by the customer are delivered.	As the consequence of this risk is *low* and the likelihood of risk is *moderate*, this risk is the type of risk that should be retained and managed by the business. Given that the risk level is moderate, it would be prudent for the business to implement the risk management strategy put forward to minimise this risk. Implementing this risk management strategy could involve considerable cost to a business if the business's Internet commerce software has to be reconfigured or even rewritten or modified to incorporate this option. Accordingly, it may or may not be cost effective for a particular business to implement this risk management strategy.
LEVEL 4 RISKS		
Risk that an Internet transaction is unenforceable for failure to satisfy the Statute of	Risk control strategies Record all communications transmitted by customers to the business relating to the terms on which the business has transacted with the customer. At the very least the following information should be included: the identity of the parties to the contact, the subject matter and the terms on which the parties have agreed to transact, any other material term of the contract and the signature of the party against whom a contract is sought to be enforced (from a business's perspective the signature of the customer) is necessary (see below for discussion on how the signature element of the Statute of Frauds writing requirement can be satisfied in respect of Internet commerce).	According to risk management principles this legal risk falls into a category of risk that should be retained by a business, because the likelihood is *unlikely* and the consequence of this risk eventuating is *low*. Since the level of risk is *low*, this risk is considered as "acceptable" and therefore strategies to manage this legal

	Frauds writing requirement.	If the business chooses to satisfy the signature element of the Statute of Frauds writing requirement by requiring customers to type in their name, the business should make it clear at the time the customer is prompted to type in the customer's name that the typed name constitutes a signature. In relation business-to-business transactions, particularly where there is an ongoing business relationship, the business could require a customer to use digital signatures or electronic "facsimile" signatures such as PenOp to satisfy the signature element of the Statute of Frauds writing requirement. Risk financing strategies A business may elect to retain the risk (for example, by paying for losses as and when they arise or setting aside funds on an annual or regular basis to cover any losses arising from a risk that eventuates) that an Internet transaction it has entered into will be unenforceable in the event of a dispute. Also, a business could choose to retain this legal risk and in addition choose to rely on the doctrines of estoppel, part performance or restitution should the situation arise that the business wishes to enforce an Internet transaction that is subject to but does not comply with the Statute of Frauds writing requirement.	risk need not be implemented. To retain this risk is also consistent with the principle that a business should only retain those risks over which it has control. Should a business wish to treat this legal risk, no one risk management strategy stands out as the most suitable to implement. Rather what risk management strategy to adopt will depend on factors particular to a business, such as the financial resources of the business and the value of the goods or services transacted on-line.

5.12 Some observations concerning the application of the risk analysis step and the evaluation and selection of risk management strategies step (Steps 3 and 4) of the risk management process in the context of legal risk

5.12.1 SOME ISSUES ARISING FROM THE APPLICATION OF STEPS 3 AND 4 OF THE RISK MANAGEMENT PROCESS IN RELATION TO LEGAL RISK

In applying the risk analysis step and evaluation and selection of risk management strategies step of the risk management process in the context of legal risk, the following issues were identified.

5.12.1.1 It is presently not feasible to analyse legal risk quantitatively

As discussed earlier in this chapter at 5.2 and in chapter 2 at 2.4.3.6, due to the lack of statistical data available in relation to legal risks it is presently not feasible to analyse legal risks quantitatively. As will be argued below, this is not a drawback. Rather it is a legitimate approach to analyse legal risks qualitatively. However, it is recognised that it could well be useful if legal risks could be analysed quantitatively. Thus, it is considered desirable that law firms, legal academics and others be encouraged to investigate and keep statistical data in relation to the likelihood and consequence of a legal risk eventuating. However, it should be noted that, even if such statistical data were available, according to risk management theory it is not necessarily valid to make assumptions concerning the *likelihood* of risk based on statistical data recording the frequency of the risk eventuating in the past (There is no such controversy in using historical statistical data to determine the *consequence* of risk). It is beyond the scope of this thesis to enter into a detailed discussion of the utility of historical statistical data to predict the likelihood of risk.

5.12.1.2 Applying a qualitative approach to risk analysis and evaluating and selecting appropriate risk management strategies involved an element of "gut feel" and intuition or required exercising personal expertise or personal judgment

When selecting descriptors for analysing legal risks, whether it was to categorise the *likelihood*, *consequence* or *level* of risk it was clear that this process involved an element of "gut feel" and intuition or, to put it another way, involved exercising personal expertise and judgment. Similarly, the evaluation and selection of appropriate risk management strategies involved relying on "gut feel" and intuition or exercising personal expertise and judgement to a certain degree. Thus, it appears unavoidable that a qualitative analysis involves a "subjective" element that will vary according to the individual undertaking the analysis, his or her expertise, judgment, experience and attitude to legal risk. This raises a question concerning the validity of such an approach, which will be discussed further at 5.12.3 at p439.

*5.12.1.3 Analysing the **consequence** of a legal risk at a generic level rather than by reference to a specific business can be problematic*

The application of risk management principles at a generic level to analyse the *consequence* of a legal risk has proved to be problematic. It has proven difficult to set and apply qualitative descriptors for categorising the *consequence* of a legal risk without reference to a specific business. The guidance provided in the risk management literature assumes that the descriptors will be set by reference to a specific business's risk benchmarks, such as the dollar amount beyond which the business becomes insolvent or the dollar amount beyond which the attention of senior

management is required. The validity of undertaking legal risk management on a generic level will be discussed at 5.12.2 at p437.

*5.12.1.4 Selecting descriptors denoting **level of risk** at a generic level rather than by reference to a specific business can be problematic*

Similarly, the application of risk management principles proved difficult in relation to selecting and applying *qualitative* descriptors for categorising the *level* of risk without reference to a specific business. Again, the guidance provided in the risk management literature assumes that the descriptors will be set by reference to a specific business's risk benchmarks. This raises a question concerning the validity of undertaking legal risk management on a generic level, which will be discussed further at 5.12.2 at p437.

5.12.1.5 Evaluating and selecting appropriate risk management strategies based on quantitative techniques is not feasible at a generic level rather than by reference to a specific business. Also, the use of qualitative techniques results in abstract conclusions

Another issue that arises in this chapter concerns how to evaluate and select appropriate legal risk management strategies. In the absence of a specific business to refer to, it was not possible to use the quantitative techniques discussed in chapter 2 for evaluating and selecting appropriate risk management strategies. Instead the research in this chapter focussed on using the qualitative techniques referred to in chapter 2 to evaluate and select appropriate risk management strategies. Whilst it is argued that it is valid to employ qualitative rather than quantitative techniques, the research in this chapter revealed that applying qualitative techniques tended to result in abstract conclusions.

5.12.2 A JUSTIFICATION FOR THE APPLICATION OF RISK MANAGEMENT PRINCIPLES AT A GENERIC LEVEL

The issues raised here give rise to the question: is it legitimate to apply risk management principles at a generic level? On a practical level, the research undertaken in this thesis leads to a conclusion in the affirmative. The outcome of this research now provides a framework for other businesses (and legal advisers) to follow and, where necessary, adapt in relation to applying legal risk management in the context of legal risk. Moreover, on a theoretical level it would be contrary to commonsense to argue that risk management in the context of legal risk can only be examined by reference to a specific business. Risk management textbooks as well as *AS/NZS 4360 - 1999, Risk Management* discuss the application of risk management at a generic level and there is no reason why legal risk management cannot also be discussed at a generic level.

There is importantly another reason favouring the argument that it is valid to apply legal risk management at a generic level. It was suggested in chapter 2 that legal risk management can be used as a means of identifying areas of legal uncertainty. To summarise the discussion in that chapter, the application of legal risk management provides a useful tool for pinpointing areas that are truly legally uncertain or that constitute serious legal impediments to the conduct of a given activity. By applying risk management methodology to identify the legal risks associated with a particular activity and eliminating the legal risks for which a risk management strategy exists, those legal risks which are insurmountable and therefore bring about legal uncertainty are isolated.

Used in this way here, the following areas of legal uncertainty or legal impediments to the conduct of Internet commerce were identified, which in turn suggests there is a need for law reform:

- There is some degree of uncertainty concerning whether Internet transactions that are subject to the Statute of Frauds writing requirement can satisfy the *signature* element of the Statute of Frauds writing requirement using a typed signature in relation to Internet transactions governed by the Electronic Transactions Act 1999 (Cth). Given that it was concluded that at common law a typed signature satisfies the signature element of the Statute of Frauds writing requirement in respect of paper based transactions there is an argument based on functional equivalence that the same principle should apply in relation to Internet transactions. The discussion in this chapter concluded, however, that the same principle will probably not apply in relation to those Internet transactions governed by Commonwealth legislation because of the "appropriateness" requirement set out in section 10;
- There is some degree of uncertainty concerning whether a series of Internet communications can satisfy the *memorandum* element of the Statute of Frauds writing requirement, particularly those transactions governed by the Electronic Transactions Act 1999 (Cth). Due to the nature of Internet commerce, it is unlikely that a business will be able to produce one document (even in electronic form) that contains the material terms of a contract. Instead a business will have to rely on a series of linked Internet communications to satisfy this aspect of the

Statute of Frauds writing requirement. Again taking a functional equivalence approach, since the law recognises the linking of a series of paper based documents to comprise a memorandum the law should also recognise a series of linked Internet communications to comprise a memorandum. On a narrow interpretation of section 11 of the Electronic Transactions Act 1999 (Cth), however, a series of linked Internet communications will not comprise a memorandum, since section 11 (on a narrow interpretation) only applies where at some point in time the document or documents, sought to be relied on, existed in paper form. Internet communications, however, are not likely to have originally existed in a paper form. It is argued that if government is to achieve functional equivalence in respect of Internet transactions then section 11 must be modified so that it applies even if a document did not ever exist in paper form.

Perhaps, more importantly, the risk analysis step and the evaluation and selection of risk management strategies step of the legal risk management process demonstrates that in relation to the six legal risks identified, very few could be described as truly legally uncertain to the extent that a call for law reform is absolutely necessary in order to resolve such legal uncertainty or to remove a serious legal impediment to the conduct of Internet commerce.

5.12.3 A JUSTIFICATION FOR USING QUALITATIVE APPROACHES TO ANALYSE LEGAL RISKS AND TO EVALUATE AND SELECT APPROPRIATE RISK MANAGEMENT STRATEGIES

The issues raised here also raise the question: is it legitimate to analyse legal risks and to evaluate and select appropriate risk management strategies using qualitative

techniques, particularly when these techniques can involve an element of intuition and "gut feel" or exercising personal expertise or judgment. Again, the answer is yes.

Although there has been a tendency in some recent risk management texts to emphasise the use of quantitative approaches to risk management, particularly in relation to the areas of share portfolios and derivatives, it is widely acknowledged that it is nevertheless valid to employ qualitative approaches. Unlike fields, such as physical risk and disaster management (insurance), and share portfolio and derivative trades, there is simply little or no statistical data available in relation to law and legal risk. But, to repeat the words of a classic risk management text, business decisions about risk must still be made and they have to be made in the context of whatever information about a given risk is available:

> Still, the risk manager has to make decisions based on loss probabilities and maximum loss potentials from given exposures. For some of these exposures, the facts and figures necessary for scientific decision making are simple to develop; for others, they are simply impossible. Yet decision making, like the show, must go on. Risk management decisions, therefore, often have to be made with too few facts for comfort. Moreover, a number of the available available "facts" are based on conclusions involving circumstantial evidence[689].

Given that business decisions about legal risks are going to be made, regardless of the availability of statistical data, it is argued here that it is preferable to make such decisions based on an analysis of the legal risks that is undertaken in a systematic and consistent manner. That is, it is preferable to analyse legal risks and evaluate and select risk management strategies using the systematic structural approach employed by risk management, even if it is only possible to achieve this by using a qualitative approach.

In relation to the use of "gut feel" and intuition or exercising personal judgment and expertise in the application of legal risk management, it should be noted that risk management is commonly referred to as an art and not a science[690]. It is argued here that given that the use of risk management in the context of legal risk has yet to be fully developed, there will be at times no other option available but to make an assessment relying on intuition and "gut feel" or exercising personal judgment and expertise. As a partner of top tier law firm notes:

> [Legal risks] are often not capable of actual measurement [on a quantitative basis]. So, we must use our experience (eg re likely penalties.) This is part of what the client is paying for[691].

Similarly, the National Legal Risk Management Co-ordinator of a top tier law firm states:

> …we rely on some gut feel to categorise risks. The justification is there is often no better way to do it and that with our extensive legal and business experience, and by making these judgments with relevant people from the client organisation, we make the judgments[692].

Furthermore, in relation to the application of legal risk management in the context of Internet commerce, a relatively new and uncharted area, again there will be times where there will be no other option but to make an assessment based on intuition,

---

690 For example, Robert I Mehr and Bob A Hedges in , *Risk Management in the Business Enterprise*, Richard D Irwin Inc, Homewood, Illinois, 1963, p 257 state that "In many of its aspects, risk management is an art and not a science". The authors also express the view at p 257 that "…there is room for more scientific risk management than is currently practiced but not enough to replace artful risk management."

691 Response dated 22 November 1999 to a self-completion questionnaire enquiring how the participant uses management methodology in the context of legal risk. Participants' names have not been disclosed to honour a request of some participants to remain anonymous. All responses are available on file.

692 Response dated 7 December 1999 to a self-completion questionnaire enquiring how the participant uses management methodology in the context of legal risk. Participants' names have

"gut feel", personal judgment or personal expertise, or as one risk manager, Judie Mulholland, has put it "educated guesses"[693]. Similarly, an E-business Risk Management Professional, notes that there is little choice but to rely on intuition and experience when analysing the risks associated with Internet commerce:

> In the real world of the e-business jungle, instinct is the only thing that is real. No one has done what we are doing for the specific purposes of insuring e-businesses so there is very little historical experience for us to rely on. We hire experts in specialized fields who can give us the broadest range of perspectives on any given risk[694].

This reliance on "gut feel", intuition, personal expertise or personal judgment is recognised as inevitable by the risk management textbook writers:

---

not been disclosed to honour a request of some participants to remain anonymous. All responses are available on file.

693 For example in personal e-mail from Ms Judie Mulholland, dated 19 November 1998 who provides risk management courses in relation to electronic commerce, she indicated that: "the methodology I am following for the course is derived from best practices and is based on the good old life-cycle approach and it entails a combination of methods, both quantitative and qualitative, depending on what's being assessed and how much we know about it. as to how much weighting is assigned (a lot of times that entails nothing more than an educated guess) is largely a judgement all but at best, we try to tie it back to the mission (read goals/objectives) of the decision-maker/organization" Similarly, in a personal e-mail from Mr Rick Davis, Director of Business Development and Security Strategy of Network Risk Management Services Inc (at that time)which provides risk management advice to businesses who conduct electronic commerce, dated 22 September 1998, he stated in relation to whether he used quantitative or qualitative methods for measuring risk, "Ours is a non-standard process built on proprietary methodology. It is closest to multi-attribute value theory but, as I said before, we mix in a heavy dose of wishful thinking, inference and "spin-the-bottle"..... You must remember one thing about what we do: no one ever did this before and no one (besides us) is doing [sic] now. We are writing the book on this stuff and so we have no blueprint or roadmap to lead us down the correct path. Traditional insurance is built on decades and centuries of actuarial data that we have just started to collect. Maybe by the time we actually get near our target, someone will term a new form of risk management after our methods. I wonder what they would call it....witchcraft I think..... Seriously, we have nice, standard methodology that is based from a growing matrix of complex variables and relative values. And of course, everything we do is based on the custom environment of our customer and their stakeholders. Pretty serious engagements I'd say..."

694 Response dated 20 January 2000 to a self-completion questionnaire enquiring how the participant uses management methodology in the context of legal risk. Participants' names have not been disclosed to honour a request of some participants to remain anonymous. All responses are available on file.

> There is a gap between the theory and the techniques proposed to manage risk, and what people do in practice. Intuition, expert skill, and judgement will always influence decision-making…[695]

As one respondent to the self-completion questionnaire observed:

> I justify [relying on gut feel, intuition, personal judgment and expertise] by virtue of the fact that I am not looking for an optimal point, read: single answer. Instead I am looking for acceptable tolerances. Since we can never entirely eliminate risk the question becomes: what level of risk are we willing to live with and how much is it going to cost. It always involves some kind of tradeoff and that, by definition, that [sic] requires a judgement call[696].

This leads to the conclusion that it is legitimate to analyse legal risks and to evaluate and select appropriate risk management strategies using qualitative techniques, even when this may involve an element of intuition and "gut feel" or exercising personal judgment or personal expertise.

5.13 Conclusion

This chapter evaluated further the legal risk management framework developed in chapter 2. More particularly, the research focussed on how the third (risk analysis) and fourth (evaluation and selection of risk management strategies) steps applied in practice. Applying these steps in relation to the conduct of Internet commerce demonstrated that the legal risk management framework was effective when used in

---

695 Roger Flanagan and George Norman, *Risk Management and Construction*, Blackwell Scientific Publications, Oxford, London, 1993, Ch 1, p 1. Similar comments were made by the authors at p 45: "Risk management need not be complicated nor require the collection of vast amounts of data. It is a matter of common sense, analysis, judgement, intuition, experience, gut feel and a willingness to operate a disciplined approach to one of the most critical features of any business or project in which risk is generated."

696 Response dated 28 November 1999 to a self-completion questionnaire enquiring how the participant uses management methodology in the context of legal risk. Participants' names have not been disclosed to honour a request of some participants to remain anonymous. All responses are available on file.

practice, but some limitations associated with using risk management in the context of legal risk were revealed. These limitations did not however, limit the effectiveness of the legal risk management framework developed. Rather, the limitations related to what risk management techniques can be used and the purposes for which risk management can be used when applied in the context of legal risk. Thus, for example, it was not feasible to undertake a *quantitative* analysis of the selected legal risks and instead the research involved undertaking a *qualitative* analysis of the legal risks. The research also revealed that the use of the legal risk management framework at a generic level could be problematic in comparison to the use of the legal risk management framework in relation to a specific business. For example, it was particularly difficult setting descriptors for the *consequence* of a legal risk eventuating without reference to a specific business. It was difficult also setting descriptors for the *level* of risk without reference to a specific business. Similarly *evaluating and selecting risk management strategies* without reference to a specific business resulted in conclusions that were abstract, leading to the conclusion that there are flaws associated with using risk management as a mechanism for producing a single generic risk management approach for managing the legal risks associated with Internet commerce.

By applying the legal risk management framework developed in chapter 2, several predictions concerning the benefits of using risk management in the context of legal risk were confirmed. Importantly, and in contrast with conventional legal advice, the application of risk management methodology in the context of legal risk enables legal

risks to be analysed consistently. This provides an authoritative basis for prioritising legal risks according to their seriousness and it was therefore possible to categorise the six contractual risks analysed by reference to their seriousness. This feature is desirable and stands in contrast with conventional legal advice, which is typically idiosyncratic and highly individualistic. Furthermore, risk management methodology, when applied in relation to the legal risks faced by a specific business enables legal risks to be categorised as to their seriousness based on criteria set by the business. In effect, the legal advice provided is "tailored" to the specific needs and circumstances of the business being advised. Clearly this is of practical benefit to businesses and to legal practitioners who wish to provide such legal advice.

In addition, the research in this chapter established that risk management methodology when applied in the context of legal risk can be used to pinpoint areas of true legal uncertainty or impediments to the conduct of a given activity. Thus, in relation to the legal risks associated with Internet commerce two areas of legal uncertainty were identified suggesting the need for law reform.

All in all, these findings point to the conclusion that it is useful and legitimate to apply the risk management process in the context of legal risk. This chapter marks the final part of the research undertaken in this thesis. The overall conclusions that can be drawn from the research are set out in the concluding chapter that follows.

CHAPTER 6 RESEARCH OUTCOMES AND CONCLUSIONS

6.1 Introduction

The research outcomes of this thesis are diverse. Put briefly they are:

- That risk management can usefully be applied in the context of legal risk;
- The development of a legal risk management framework based on *AS/NZS 4360 Risk Management*;
- A contribution to the discussion on the role of legal risk management in comparison with preventive law and legal compliance;
- An assessment of the scope of risk management when used in the context of legal risk including the purposes for which it can be used;
- The identification of a range of legal risks affecting businesses conducting Internet commerce;
- An evaluation of select contractual legal risks associated with conducting Internet commerce and risk management strategies; and
- The identification of some areas of legal uncertainty in relation to contracting on the Internet.

In addition to discussing some of these outcomes in more detail, this chapter summarises the limitations of legal risk management, considers the implications of this research for practice and identifies areas for further research.

6.2 Outcome of research

There are several research outcomes resulting from the research undertaken in this thesis.

At a broad level the research contributes to two disciplines that of risk management theory and that of law.

Foremost, the research established that risk management methodology can be usefully applied in the context of legal risk. More specifically, the research demonstrates that risk management can used by business as a tool for achieving legal compliance, avoiding exposure to liability and protecting legal rights and interests. This may not sound controversial but this finding expands upon present understanding of how risk management can be used in the context of legal risk. The research further points to the conclusion that risk management is an effective and, moreover, a superior technique for identifying, analysing and managing legal risk.

Risk management, when used in the context of legal risk, has two beneficial features. First, risk management through its iterative methodology and the requirement that each risk be analysed (usually in terms of *consequence* and *likelihood* of eventuating), results in *consistent* analysis of often disparate risks. In this regard, legal risk management methodology is superior to the conventional approach to providing legal advice, where a conscious effort is required to ensure that the legal advice provided is based on a systematic and consistent analysis of the legal risks. The importance of a technique that brings about a systematic and consistent analysis of legal risk should not be undervalued. For example, sloppy contracting practices are often a serious cause of uninsured losses for companies[697]. Apart from addressing the risk of serious losses, the systematic and

[697] Personal communication from Professor Brent Fisse, partner of the law firm Gilbert & Tobin, 17 June 1999.

consistent analysis of legal risks achieved through applying risk management methodology also enables legal risks to be prioritised. This feature is particularly useful, as legal advice that prioritises legal risks helps a business decide how much time and money should be spent in managing a particular legal risk, in comparison to the other legal risks that the business may face.

Secondly, the use of risk management methodology in the context of legal risk results in legal advice that is attuned to business needs, more so than is conventional legal advice. Risk management methodology requires that legal risks be analysed by reference to a business's specific financial position and categorised according to the business's risk criteria. Also, determining which risk management strategies to implement is again achieved by reference to a business's particular financial position and its risk criteria. Conventional legal advice does not typically take such factors into account. The conventional approach to giving legal advice is to provide more generic advice in the sense that often the same legal advice would be given in respect of a particular legal risk whether the client was a large business or a small business. Legal risk management, in contrast, results in the provision of more "tailored" legal advice. It seems both desirable and logical that legal advisers should provide legal advice that actively accommodates the client's perspective.

The research in this thesis also resulted in the development of a legal risk management framework based on *AS/NZS 4360 -1999 Risk Management*. Such research has not previously been attempted and the research here contributes materially to the topic of risk management and its use in the context of legal risk.

The research undertaken in this thesis also investigated the purposes for which risk management methodology can be used in the context of legal risk. The research points to the conclusion that risk management methodology is not only useful as a tool for identifying and managing legal risk. The research findings of this thesis have implications that may interest regulators and policy makers. Risk management methodology may be useful for investigating the extent to which the law is adequate or too uncertain in relation to a particular activity, which could be useful for identifying areas requiring law reform. How? As discussed in chapter 2, applying risk management to a range of identified legal risks provides a means of eliminating those aspects of the law which are perceived to, but in fact do not, create legal uncertainty. If we eliminate those identified legal risks for which a risk management strategy exists we can isolate those legal risks which are insurmountable and therefore bring about legal uncertainty. However, as noted at 6.3 there are limitations associated with using risk management as a tool for identifying areas requiring law reform. It is therefore concluded that the primary benefit of using risk management in the context of legal risk is as a tool for identifying, analysing and managing legal risk.

By evaluating the legal risk management framework developed in this thesis in relation to the conduct of Internet commerce, some questions concerning the legal uncertainty associated with Internet commerce were answered. The research established that many of the legal risks faced by businesses conducting Internet commerce are shared equally by businesses conducting off-line commerce. In relation to the six contractual risks selected for further analysis, the research showed that, at least from a business perspective, the legal uncertainty created by

these contractual risks is not as great as that suggested in the literature. Thus, the risk of entering into an invalid transaction, either because a transaction is illegal, or because a customer with whom the business deals falsely purports to act on behalf of a third party, is equally shared by businesses that conduct distance commerce such as telephone or mail order catalogue sales. Similarly, the risk of incurring liability in relation to receiving on-line payments is largely the same as the risk to businesses who receive telephone payments in relation to off-line commerce. Other contractual risks, such as the risk that a business will be contractually bound to terms that are altered by erroneous transmission, or the risk that a customer withdraws an "offer" notwithstanding that a business has already purported to accept it are comparable to the same risks faced by businesses that transact by facsimile machine when conducting commerce off-line.

In addition, the research revealed some areas of true legal uncertainty for which law reform is needed in order to eliminate inconsistency in the way the law applies to Internet commerce in comparison with commerce conducted off-line. As discussed in chapter 5, there is legal uncertainty concerning whether using a typed signature can satisfy the signature element of the Statute of Frauds writing requirement in relation to Internet transactions governed by the Electronic Transactions Act 1999 (Cth). (Interestingly, this legal uncertainty does not arise in relation to the Victorian Electronic Commerce Framework Bill (Vic)). Since typed signatures constitute signatures for the purposes of the Statute of Frauds writing requirement in relation to paper-based transactions, it is argued here that law reform is required in order that this legal principle will equally apply in relation to Internet commerce governed by the Electronic Transactions Act 1999

(Cth). True legal uncertainty also exists in respect of whether a series of Internet communications can be linked to satisfy the "memorandum" element of the Statute of Frauds writing requirement, particularly those transactions governed by the Electronic Transactions Act 1999 (Cth). Again, since the law recognises the linking of a series of paper-based documents to comprise a memorandum the law should also recognise a series of linked Internet communications to comprise a memorandum and law reform would be necessary to effect this. This outcome is surprising given that the objective of the legislation is to overcome legal impediments to Internet commerce.

Finally, this thesis seeks to inform the discussion on the comparative role of compliance, preventive law and risk management. The role of each discipline in comparison with each other has not been the subject of detailed discussion, which is perhaps surprising given the similarity and overlap between them. The research findings establish that risk management when used in the context of legal risk shares many of the objectives of compliance and preventive law. More specifically, *legal risk management* and *preventive law* share the same objectives, that is (1) to reduce or eliminate the legal liability a business may be exposed to; (2) to achieve compliance with the laws that regulate the activities of the business; and (3) to protect a business's legal rights and interests. The objectives of *compliance* are more difficult to determine. An extensive review of the literature reveals both a broad and a narrow version of compliance. The narrow version limits the objectives of compliance a single one that of achieving compliance with the laws that regulate the activities of the business. Compliance under its broader definition, however, shares the same objectives of legal risk management and

preventive law. The research further concluded that the objective of achieving "legal protection", considered by others as distinguishing compliance from legal risk, was equally an objective of legal risk management, being factored in when a business sets its risk criteria (step 1 of the risk management process).

Whilst there may be relatively minor differences in relation to the objectives of each approach, the techniques used vary significantly. Risk management approach is an iterative approach. Techniques for applying each step in the process are well defined and documented. For example, there are qualitative and quantitative techniques available for undertaking the risk analysis step and the evaluation and selection of risk management strategies step. In contrast, the techniques advocated in preventive law and compliance are not so comprehensive or well-documented. For example, both preventive law and compliance set out methods for identifying legal risks but they appear not to provide guidance for how such legal risks should be analysed. Also, these approaches provide no guidance as to how to decide which risk management strategy or strategies to implement. In fact in relation to compliance some authors suggest that there is only one option and that is to fully comply with the law.

The research points to the conclusion that risk management is superior to compliance and preventive law as those disciplines have traditionally been elucidated. Risk management methodology is such that a consistent analysis of risks and evaluation of risk management strategies is an automatic result of its use. In contrast, the techniques associated with preventive law and compliance are not designed, in the way that the risk management process is designed, to achieve a consistent analysis of legal risks and risk management strategies. This is not to

say that compliance and preventive law techniques are unsystematic. However, it is more difficult to compare legal risks using the preventive law and compliance approaches because legal risks have not necessarily been evaluated consistently in the way they would be if risk management methodology had been followed. Also, risk management uses techniques that enable strategies for managing identified legal risks to be evaluated consistently. Risk management strategies are then selected according to guiding principles such as the effect each possible strategy may have on the business's ability to fulfill its objectives. The outcome is that the risk management strategies ultimately selected automatically take into account circumstances particular to the business. Preventive law and compliance do not use such techniques and therefore it is necessary for the legal adviser who uses such approaches to consciously take into account factors particular to the business, which may be overlooked.

While the conclusion drawn in this thesis concerning the role of legal risk management is that legal risk management is superior to preventive law and compliance, the disciplines have much to offer the other. For example, the practical techniques used in preventive law for identifying legal risk could equally be useful for applying risk management methodology in the context of legal risk. Thus, notwithstanding the objections raised by some writers concerning the distinction between compliance and legal risk management, it is desirable that the disciplines converge: more specifically compliance is best understood as one key step in effective legal risk management.

6.3 Limitations associated with using risk management in the context of legal risk

In addition to the research outcomes set out above, the research undertaken in this thesis enabled the following conclusions to be drawn concerning the limitations of legal risk management.

First, it is clear that legal risk management works best when applied in respect of a specific business. Whilst it is possible to apply risk management at a broader, generic level there are some difficulties associated with using legal risk management in this way. For example, when analysing the identified legal risks it proved problematic to set generic descriptors to describe the *consequence* of a legal risk. Similarly, it proved difficult to select and apply qualitative descriptors signifying the *level of risk* without reference to a specific business. Also, because a specific business must be referred to when using *quantitative* measurement techniques it proved impossible to evaluate and select risk management strategies on a quantitative basis at a generic level. However, the research in this thesis leads to the conclusion that it is nevertheless useful and valid to apply legal risk management at a generic level. A particularly important benefit of so doing is that disparate legal risks can be analysed and evaluated systematically and consistently.

Secondly, legal risk management at present can only be used in relation to legal risks that constitute *hazards* rather than *perils*. Put briefly, a legal risk is a *hazard* if it makes a "legally related loss" *likely* or more *severe*. This may change due to ongoing scholarship in the field of law and economics.

Thirdly, it became apparent that adopting a qualitative approach to steps 3 and 4 of the legal risk management process - risk analysis and risk evaluation and selection- involved an element of "gut feel" and intuition or exercising personal

judgment and expertise. “Gut feel”, intuition, and exercising personal judgment and personal expertise do have a legitimate role to play in risk management. Further I believe that, as scholarship and application of legal risk management increases, it will become less necessary to rely on “gut feel”, intuition, personal judgment or personal expertise.

Fourthly, the research pointed to the fact that applying *qualitative* techniques for analysing legal risks tended to result in abstract outcomes compared to the result which might have been achieved if a *quantitative* analysis had been practicable. Again, I believe that as scholarship and application of legal risk management increases, more information will become available about the nature of legal risks, so that more specific qualitative analyses can be undertaken.

Finally, notwithstanding that the research in this thesis suggests that legal risk management could be useful for identifying areas requiring law reform it should be noted that risk management is not specifically designed for this purpose. Risk management, used alone, therefore is unlikely to be a satisfactory tool for identifying areas requiring law reform particularly since it is not designed to take into account competing interests, a factor integral to the law reform process

6.4 Implications of the research for practice

From the perspective of businesses, the research undertaken in this thesis is of practical benefit. As noted earlier, the thesis establishes that risk management can be used in the context of legal risk. A benefit of implementing a legal risk management system is what has been termed by some commentators as, the “reduced deterrence effect”. That is, where strategies are in place for minimising risk such that any loss that is brought about by such risk eventuating is less likely

to occur, less severe, or more predictable, a business will be less likely to be deterred from undertaking an activity for which there is a risk of exposure to loss[698]. The use of legal risk management by a business thus enables the business to take "calculated" risks, which would not otherwise have been considered advisable.

In addition, by using legal risk management a business can control the amount of time it spends on managing legal risks, as opposed to the time spent on responding to legal risks that have eventuated such as litigation proceedings, the progression of which is largely out the control of the business:

> [t]he timing and extent of [risk management] program expenditures is, for the most part, entirely within the control of corporate managers. The timing and extent of litigation- along with related disruptions and liability expenses- is generally not within management's control. [Risk management] program activities can, within some limits, be blended into the fabric of corporate production. Litigation, by contrast, comes as a unique, stubborn, demanding onslaught to corporate management and production.[699]

From the perspective of legal practitioners and other third parties concerned with analysing and managing legal risk, such as insurance assessors, the research undertaken in this thesis is also significant. Many law firms and in-house counsel are seeking to expand the range of services provided by also offering risk management services in relation to legal risk. The research in this thesis provides a framework for applying legal risk management. In particular, the checklists for each step of the legal risk management process and the sample documentation set out in chapter 2 will facilitate the application of legal risk management.

---

698 George L Head and Stephen Horn, *Essentials of Risk Management*, Insurance Institute of America, 1991, http://www.bus.orst.edu/faculty/nielson/rm/chapter1.htm.

699 Richard S Gruner and Louis M Brown, "Organizational Justice: Recognizing and Rewarding the Good Citizen Corporation", 21 *The Journal of Corporation Law*, 731, 751.

Of additional practical use are the research findings of chapters 4 and 5 of this thesis. In these chapters the legal risks associated with Internet commerce are identified and, in relation to six selected contractual risks, risk management strategies are provided and evaluated. The in-depth analysis provided contributes to the discussion on legal issues associated with the conduct of Internet commerce and will be of particular interest to those concerned with Internet commerce.

6.5 Further Research

The research in this thesis has raised some issues that would benefit from further research.

One significant policy issue concerns the extent to which legal risk management should be allowed to be used as a defence, or in mitigation, in legal proceedings. Undoubtedly, in some circumstances the fact that a business has applied legal risk management can serve as a defence:

> "For example, if a negligence suit were to be brought against a business, a documented risk management plan which demonstrates that reasonable and adequate consideration was given to the range of risks involved and that appropriate mitigation strategies were in place could be significant evidence that the organisation was not negligent."[700]

However, the extent to which a business should be entitled to use its implementation of a legal risk management system as a defence has yet to be resolved.

Another significant policy issue concerns the use in legal proceedings of a business's legal risk management records and documentation by regulators and other parties. For example, will legal compliance audits undertaken by a business

or its legal advisers, as part of the legal risk management process (that may well reveal instances of statutory non-compliance which the business subsequently chooses to ignore) be discoverable? Can the documentation kept by a business in respect of the legal risk management system it implements be used as evidence against a business in litigation, and can it be subpoenaed by regulatory authorities or other parties seeking to find evidence to support a prosecution for statutory non-compliance?

It is beyond the scope of this thesis to consider the economic and policy implications that would need to be examined to fully discuss these issues.

The use of legal risk management in relation to legal risks that constitute perils also warrants further research given that the quantitative analysis of such types of legal risks is already the subject of research. More generally, the use of quantitative techniques to analyse legal risk, an area already the subject of some research, would benefit from continued research in the context of legal risk management.

An additional area of research is the issue of how to integrate preventive law, legal compliance and legal risk management, an outcome suggested here as desirable.

Also a matter for future consideration is the operative issue of how best to implement a legal risk management system. For example, should businesses use risk management computer software? Would "expert system" software be useful?

6.6 Conclusion

---

[700] Standards Australia/Standards New Zealand Joint Technical Committee on Risk Management, "A Basic Introduction to Managing Risk using the Australian and New Zealand Risk Management Standard - AS/NZS 4360: 1999", Master Draft as at 4/1/99 p12.

To conclude, this thesis examined risk management methodology and investigated its usefulness when applied in relation to legal risk. Several risk management models were considered and a *legal risk management* framework based on the risk management model advocated by *AS/NZS 4360 -1999 Risk Management* was developed. The legal risk management framework developed was then applied in relation to the conduct of Internet commerce. In this way, the scope of the legal risk management framework could be determined.

The research undertaken in this thesis demonstrates that risk management can and should be used in the context of legal risk. By applying legal risk management, legal advisers can provide advice that analyses legal risks consistently and is more attuned to a business's needs and to its particular circumstances. These features distinguish legal risk management from the related disciplines of legal compliance and preventive law as they have been traditionally described. Further, legal risk management is not only useful as a tool for identifying and managing legal risk in a systematic and consistent way, but it can provide a means of identifying areas of legal uncertainty, which in turn may be useful for identifying areas requiring law reform.

The outcome of this research also has practical significance for legal practitioners and businesses. The checklists and sample documentation developed in this thesis are of particular practical benefit to legal practitioners and businesses who wish to apply risk management in the context of legal risk.

Finally, it is hoped that the research findings here will instigate and facilitate the use of legal risk management.

REFERENCES CITED IN THIS THESIS

Altman, Jeffrey P, 'Managing Legal Risks', *Association Management*, Jan 1998, v 50 n 1 pp 67-69.

American Bar Association, Section of Business Law, Committee on Law of Commerce in Cyberspace, Subcommittee on International Transactions, "Supporting Report for the Recommendation Committee on Law of Commerce in Cyberspace Subcommittee on International Transactions", January 1997, http://www.abanet.org/buslaw/cyber/finaires.html.

Andersen Consulting, *eCommerce: our Future Today*, A review of eCommerce in Australia, 1998.

APEC Telecommunications Working Group, Preliminary Report entitled TELWG16/BFSG/3.e/2, undated, http://www.apecsec.org.sg/telewg/16tel/bfsg/matrix/TELWG16-BFSG-3e-2.html.

Attorney- General's Department, "Explanatory Paper -Electronic Transactions Bill 1999", January 1999.

Australian Bureau of Statistics, "Press Release: Home Internet Use Grows Strongly-ABS Figures", press release dated September 6 1999, 106/99 3 Million Internet Purchases and1.5 Million Households Oline – ABS", http://www.abs.gov.au/websitedbs/d3110125.nsf/4a255eef008309e44a255eef00061e57/0c6b7ec6e6a0e5d3ca2567e400028e5e?OpenDocument. Full Report in *Use of Internet by Householders*, Australia, May 1999 (Cat. No. 8147.0).

Australian Competition and Consumer Commission, The Global Enforcement Challenge- Enforcement of consumer protection laws in a global marketplace, Discussion paper, Commonwealth of Australia, August 1997.

Australian Law Reform Commission report, *Legal risk in international transactions*, Australian Government Publishing Service, Canberra, 1996.

Australian Securities Commission (as it then was), *Issues Paper-Virtually no Liability: Securities Markets in an Electronic Age* 1997, http://www.asic.gov.au.

Australian Standard, *AS/NZS 4360 - 1999, Risk Management*, Standards Australia, Strathfield NSW, 1999.

Australian Standard *AS 3806 -1998, Compliance Programs*, Standards Australia, Homebush NSW, 5 February 1998.

Baird, Inga S and Thomas, Howard, "What is Risk Anyway?", in *Risk, Strategy, and Management*, edited by Richard A Bettis, Howard Thomas, JAI Press Inc, Greenwich, Connecticut, 1990.

Baldwin, Robert, "Risk: The Legal Contribution", in *Law and Uncertainty Risks and Legal Processes*, edited by Robert Baldwin with the assistance of Peter Cane, Kluwer Law International, London, 1997.

Becker, Brandon and Mazur, Francois-Ihor, "Symposium: Derivative Securities: Risk Management of Financial Derivative Products: Who's responsible for what?", 21 *Iowa Journal of Corporation Law* 177.

Bernstein, Peter L, *Against the Gods- The remarkable story of risk*, John Wiley & Sons, Inc, New York, 1996, p 248.

Berry, John, "Mining for E-Commerce Gold", in www.cmpnet.com, the Technology Network, 8 October 1998, http://www.webtools.com/story/TLS19981998S0001.

Bicknell, Craig, "Credit Card Fraud Bedevils Web", *Wired News*, 2 April 1999, http://www.wired.com/news/print_version/business/story/18904.html?wnpg=all.

Bodily, Samuel E, "When should you go to Court?", Harvard Business Review, Boston, May/Jun 1981, Vol 59, No 3, pp 103-113.

Boreham, Tim, "Call to post banks Net fraud bills, *The Australian*, 19 March 1999, http://www.theaustralian.com.au/masthead/theoz/state/4379100.htm.

Biddle, Bradford, "Public Key Infrastructures and "Digital Signature" Legislation: 10 Public Policy Questions", 3 March 1997, http://www.cooley.com/scripts/article.ixe?id=ar_1502, para 1.

Biddle, C Bradford,"Legislating Market Winners- Digital Signature Laws and the Electronic Commerce Marketplace", 1997, http://www.w3journal.com/7/s3.biddle.wrap.html.

Biddle, C. Bradford, "Comment: Misplaced Priorities: The Utah Digital Signature Act and Liability Allocation in a Public Key Infrastructure", Summer, 1996, 33 *San Diego Law Review* 1143, pp 1184-1185.

Braswell, Michael K, "Compliance Programs: An Alternative to Punitive Damages for Corporate Defendants", 49 *South Carolina Law Review*, Winter 1998, p247.

Brilmayer, Lea,"Symposium: Probability and Inference in the Law of Evidence: II. Bayesian Theory and its Critics: Second-order evidence and Bayesian Logic", *Boston University Law Review*, Vol 66, July 1986, p 673.

Brown, Bina, "Internet Shopping Basket Case", *The Weekend Australian*, October 30-31, 1999, p 46.

Brown, L & Dauer E, "Preventive Law- A Synopsis of Practice and Theory", ABA, *The Lawyer's Handbook*, c 3 at A3-7 to A3-10 (Rev.Ed. 1975) as reproduced in Robert M Hardaway, *Preventive Law - Materials on a Non Adversarial Legal Process*, Anderson Publishing Co., Cincinnati, 1997, p 143.

Brown, Louis M and Dauer, Edward A, *Planning by Lawyers: Materials on a Nonadversarial Legal Process*, The Foundation Press, Mineola, New York, 1978.

Brown, Louis M assisted by Rubin, Edward, *Manual of Preventive Law*, Prentice-Hall, Inc, 1950.

Butler, Grant and Lewis, Steve, "E-commerce future 'grim', *The Australian Financial Review*, April 17 1998, p 15.

Calfee, John E and Craswell, Richard, "Some effects of uncertainty on compliance with legal standards", 70 *Virginia Law Review*, 965, June 1984.

Canadian Standards Association, *Risk Management: Guideline for Decision-Makers CAN/CSA-Q850-97*, Canadian Standards Association, Ontario, Canada, October 1997.

Central Computer and Telecommunications Agency, *Legal Issues and the Internet*, HMSO, London, 1996.

Chicken, John C, *Risk Handbook*, International Thomson Business Press, London, 1996.

Choi, Soon-Yong and O'Stahl, Dale, "Electronic Payments and the future of Electronic Commerce", The Center for Research in Electronic Commerce, 1997, http://cism.bus.utexas.edu/works/articles/cyberpayments.html.

Clarke, Roger, "Net-Based Payment Schemes", 1 December 1996, http://www.anu.edu/people/Roger.Clarke/EC/EPMEPM.html.

Clarke, Roger, "Cryptography issues in plain text", *Privacy Law and Policy Reporter*, May 1996 Vol 3, No 2, p 24.

Communiqué from the Canberra Summit on E-Commerce Great Hall, Parliament House 16-17 April 1998, 17 April 1998.

Competitive Tendering and Contracting Group, Department of Finance and Administration, "Limitation of Liability and Risk Management", CTC Toolkits, http://www.ctc.gov.au/toolkits/liability/lia1.htm, last updated 19 April 1999.

Competitive Tendering and Contracting Group, Department of Finance and Administration, *Competitive Tendering and Contracting*, Commonwealth of Australia, Parkes, ACT, March 1998.

Corporate Law Economic Reform Program, Electronic Commerce: Cutting Cybertape- Building Business, Proposals for Reform, Paper No 5, Commonwealth of Australia, AGPS, 1997.

Costanzo Margot, *Problem Solving- (Essential Legal Skills Serie*s), Cavendish Publishing Limited, London, 1995.

Crede, Andreas, "Electronic Commerce and the Banking Industry: The Requirement and Opportunities for New Payment Systems Using the Internet, *Journal of Computer-Mediated Communication*, Volume 1, No 3, http://www.usc.edu/dept/annenberg/vol1/issue3/crede.html.

Crockford, Neil, *An Introduction to Risk Management*, 2nd Edition, Woodhead-Faulkner, Cambridge, 1986.

Dahl, Andrew, Leswick, Leslie, *Internet Commerce*, New Riders Publishing, Indianapolis, Indiana, 1996.

Dalton, Gregory, "Visa And CyberSource Target Online Fraud", *InformationWeek*, (09/01/99, 8:02 p.m. ET), http://www.techweb.com/wire/story/TWB19990901S0026.

Denning, Dorothy E, "Encryption Policy and Market Trends", February 19, 1997, http://guru.cosc.georgetown.edu/~denning/crypto/Trends.html.

Department of Communications, Information Technology and the Arts, "E-commerce Beyond 2000", Commonwealth of Australia, 2000: http://www.noie.gov.au/beyond2000.

"Dismantling the Barriers to Global Electronic Commerce", An International Conference and Business-Government Forum organised by the OECD and the Government of Finland in Co-operation with the European Commission, the Government of Japan and the Business and Industry Advisory Committee, 19-21 December 1997, http://www.oecd.org/subject/electronic_commerce/documents

Ducret, Alan, 'Risk Management: the ACCC, the Trade Practices Act and a Practical Compliance Program', *Australian Company Secretary*, vol 49, no 11, December 1997, p 494.

Electronic Commerce: Building the Legal Framework, Report of the Electronic Commerce Expert Group to the Attorney-General, 31 March 1998, http://law.gov.au/aghome/advisory/eceg/ecegreport.html.

Electronic Commerce- An Introduction, Information Technology Programme managed by the Directorate General for Industry of the European Commission, last updated 8 May 1996, http://www.cordis.lu/espirit/src/ecomint.htm.

Electronic Commerce Taskforce, *Report of the Electronic Commerce Task Force to the Commonwealth Law Enforcement Board*, Commonwealth of Australia, November 1996.

Gail E Evans & Brian F Fitzgerald, "Information Transactions under UCC Article 2b: The Ascendancy of Freedom of Contract in the Digital Millenium?" *UNSW Law Journal*, Volume 21(2), http://www.law.unsw.edu.au/unswlj/ecommerce/evans.html.

European Union Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data 95/46/EC.

Fasciano, Paul, "Note: Internet Electronic Mail: A last bastion for the mailbox rule", 25 *Hofstra Law Review*, 971.

Federal Bureau of Consumer Affairs, *Untangling the Web- Electronic Commerce and the Consumer*, Issues Paper No 3, AGPS, 1997.

Field, Richard L, "The Electronic Future of Cash: Survey; 1996: Survey of the Year's Developments in Electronic Cash Law and the Law Affecting Electronic Banking in the United States, 46 *Am UL Rev* 967, April 1997.

Fillingham, David, "A Comparison of Digital and Handwritten Signatures", Paper for MIT 6.805/STS085: Ethics and Law on the Electronic Frontier, Fall 1997, http://www-swiss.ai.mit.edu/6805/student-papers/fall97-papers/fillingham-sig.html.

Finkelstein, Michael O and Levin, Bruce, *Statistics for Lawyers*, Springer-Verlag, New York 1990.

Brian Fitzgerald, Leif Gamertsfelder, Tonje Gullikson, "Marketing your Website: Legal Issues relating to the Allocation of Internet Domain Names", *UNSW Law Journal*, 1998, Volume 21(2), http://www.law.unsw.edu.au/unswlj/ecommerce/fitzgerald.html.

Flanagan Roger, and Norman, George , *Risk Management and Construction*, Blackwell Scientific Publications, Oxford, London, 1993.

Friedman, Richard D, "Symposium: Probability and Inference in the law of evidence: I. Theories of Inference and Adjudication: a diagrammatic approach to evidence", *Boston University Law Review*, Vol 66, July 1996.

Gamertsfelder, Leif, "Electronic Bills of Exchange: Will the current law recognise them?", *UNSW Law Journal*, 1998, Vol 21(2), 566.

Gee and Jackson, “Bridging the Gap-Legal Education and Lawyer Competency”, 1977 *Brigham Law Review* 695.

Gilbert & Tobin Lawyers, "Internet Compliance Manual", http://www.gtlaw.com.au, 1997.

Gillmor, Steve, “Businesses pay the price for online credit fraud”, *MoneyCentral Microsoft, 14 August 1998*, http://moneycentral.msn.com/articles/smartbuy/scam/1546.asp.

Gjertson, Lee-Ann, “J & H M & M offers EPL cover, legal advice”, *National Underwriter Property and Caualty/ Risk and Benefits Management*, December 8, 1997, v 101 n 49, pp 17-19.

Goldblatt, Michael L, “Legal Audits Can Help Companies Act Preventively”, as reproduced in Robert M Hardaway, *Preventive Law - Materials on a Non Adversarial Legal Process*, Anderson Publishing Co., Cincinnati, 1997, p 194.

Greenberg, Ronald “The Lawyer’s Use of Quantitative Analysis in Settlement Negotiations”, *The Business Lawyer*, Vol 38, August 1983 1557.

Greig DW, and Davis, JLR, *The Law of Contract*, The Law Book Company Ltd, 1987, Sydney.

Gruner, Richard S “The Randolph Thrower Symposium: The role of General Counsel: Perspective: General Counsel in an era of compliance programs and corporate self-policing”, 46*Emory Law Journal*, Summer 1997, p 1113 at p1114.

Gruner, Richard S and Brown, Louis M, “Organizational Justice: Recognizing and Rewarding the Good Citizen Corporation”, 21 *The Journal of Corporation Law*, 731.

Guidelines for Managing Risk in the Australian Public Service, Joint Publication of the Management Advisory Board and its Management Improvement Advisory Committee, Report No 22, AGPS, Canberra, October 1996.

Haimes, Yacov, *Risk Modeling, Assessment, and Management*, John Wiley & Sons, Inc, New York, 1998, pp 55-56.

Hardaway, Robert M, *Preventive Law - Materials on a Non Adversarial Legal Process*, Anderson Publishing Co., Cincinnati, 1997.

Head, George L and Horn, Stephen, *Essentials of Risk Management*, Insurance Institute of America, 1991, http://www.bus.orst.edu/faculty/nielson/rm/chapter1.htm.

Hedrick, Charles L, “Introduction to the Internet Protocols- Routing”, Rutger’s University, 1987, http://oac3.hsc.uth.tmc.edu/staff/snewton/tcp-tutorial/sec6.html.

International Chamber of Commerce, "General Usage for Internationally Ensured Commerce (GUIDEC)", 1997, http://www.iccwbo.org/guidec2.htm.

International Finance & Commodities Institute, Introduction to Risk Management website: http://risk.ifci.ch/OtherRisks.htm.

"Internet Protocols and Software Tools", http://www.hcc.hawaii.edu/iss/unix/module2.html.

Johnston, Jason S, "Bayesian Fact-Finding and Efficiency: Toward an economic theory of liability under uncertainty", 61 *Southern California Law Review*, 1987, 137.

Kalin, Sari, IDG News Service, "NCSA to assure secure transactions by certifying Web sites", *Netscape World*, August 1996, http://www.netscapeworld.com/netscapeworld/nw-08-1996/nw-08-ncsa.html.

Kaye, DH, "IV Practice and Procedure: Statistics for Lawyers and Law for Statistics", a review of *Statistics for Lawyers* by Michael O Finkelstein and Bruce Levin, Springer Verlag, New York, 1990 *Michigan Law Review*, Vol 89, May 1991 p 1520.

Kemberry, Jonathon, Senior Attorney at Arnheim Tite & Lewis, "Solving a legal conundrum on a world scale", 1998, http:.//www.global-ecom.net/inside.asp?insideid=55.

Kim, Lucie, Staff Writer, E-Commerce Times, "Report: Online Shopping Fraud Bites Merchants, Not Buyers", *E-Commerce Times*, December 4, 1998 http://www.ecommercetimes.com/news/articles/981204-1a.shtml.

Koehler, Jonathan J and Shaviro, Daniel N, "Veridical Verdicts: Increasing Verdict Accuracy through the use of Overtly Probabilistic Evidence and Methods", *Cornell Law Review*, Vol 75, January 1990, p 247.

Kosiur, Dave, "Role of Digital Certificates Looks Secure", *PC Week*, April 28, 1997, p 117.

"OOI Information Security Standards", http://www2.echo.lu/oii/en/secure.html.

Labaton, Stephen, "Can Defendants Cry 'E-Sanctuary' and Escape the Courts*?*, *The New York Times*, September 22, 1999.

Lamond, Keith, "Credit Card Transactions Real World and Online", 1996, http://rembrandt.erols.com/mon/ElectronicProperty/klamond/credit_card.htm.

Lance Rose Law Office, "Build a Safer Web Site-Webmasters can lower their legal risks even when the laws are uncertain", http://www.netlaw.com/explaind/warnings.htm, 1996-97.

Law Commission, “Electronic Commerce Part One- A guide for the Legal and Business Community”, NZLC R50, October 1998, Wellington, New Zealand.

Leonard, Peter, Partner, Gilbert & Tobin who in “Response to the Attorney-General’s Speech Regarding the Draft Digital Agenda Copyright Bill and the Draft Electronic Transactions Bill”, 12 March 1999, http://www.gtlaw.com.au/pubs/index_Internet.html.

Lewis, Steve and Beer, Stan, “‘Wait and see’ Australians are late starters”, *The Australian Financial Review*, April 17 1998, p 17.

“Licensing of Trusted Third Parties for the provision of Encryption Services”, Public Consultation Paper on Detailed Proposals for Legislation, March 1997, http://www.dti.gov.uk/pubs/.

MAB/MAIC Report No. 23, *Before you sign the dotted line…ensuring contracts can be managed*, May 1997.

Maynard, Ian, “Development and Implementation of Risk Management Strategy”, in David Elms, Editor, *Owning the Future- Integrated Risk Management in Practice*, Centre for Advanced Engineering, University of Canterbury, Christchurch, New Zealand, August 1998.

McCullagh, Adrian; Little, Peter; Caelli, William; “Electronic Signatures: Understand the Past to Develop the Future”, *UNSW Law Journal*, 1998, Volume 21(2) 452.

McDonald, John, “Risk Management in a Large Corporate Organisation”, in David Elms, Editor, *Owning the Future- Integrated Risk Management in Practice*, Centre for Advanced Engineering, University of Canterbury, Christchurch, New Zealand, August 1998, Chapter 9, p130.

Mehr, Robert I and Hedges, Bob A, *Risk Management in the Business Enterprise*, Richard D Irwin Inc, Homewood Illinois, 1963.

Merrill, Charles R, “Cryptography for Attorneys-Beyond Clipper”, 1994, http://ming.law.vill.edu/chron/articles/merrill.htm (a version of this article was published in *Data Law Report*, September 1994).

Miller, Howard B, “The Randolph W Thrower Symposium: The role of the general counsel: Perspective: Law Risk Management and the General Counsel, 46 *Emory Law Journal* 1223, Summer 1997.

Milne, Nancy, 'Fiduciary Issues: Compliance Systems- Risk Management in Due Diligence', *Australian Company Secretary*, vol 48 no 8, September 1996.

Mondex, "Mondex Security- The Chip and the Protocol" at; http://www.mondex.com/mondex/cgi-bin/printpage.pl?english+global&technology_security2.html.

Nagel, Stuart, "Literature on Computer Software and Legal Decision Making", *Law Library Journal*, 1990, vol. 82, p 749.

Nagel, Stuart S, "Applying Decision Science to the Practice of Law", *The Practical Lawyer*, Vol 30, No 3, April 15 1984, p 13.

National Advisory Council on Consumer Affairs, Consumer Protection in Electronic Commerce- Draft Principles and Key Issues, National Advisory Council on Consumer Affairs, October 1997;

National Office for the Information Economy entitled *E-Commerce-beyond 2000*, 1999, http://www.noie.gov.au/ecom/HOME/Policy/Economic_Impacts_Study.

National Research Council, *Science and Judgment in Risk Assessment*, National Academy Press, Washington DC 1994.

Nimmer, Raymond T and Krauthouse, Patricia, "Article: Electronic Commerce, New Paradigms in Information Law", 1995, 31 *Idaho Law Review*, 937.

OECD, "Electronic Commerce Opportunities and Challenges for Government" (the Sacher Report), 12 June 1997, OECD.

Oei, Lorijean G, "Primer on Cryptography", in *Online Law: the SPA's Legal Guide to doing Business on the Internet*, Thomas J. Smedinghoff, editor, Addison-Wesley Publishing, Reading, Massachusetts, 1996.

Open Information Interchange, "OII Standards and Specification List- Electronic Payment Mechanisms", http://www2.echo.lu/oii/en/payment.html#CyberCash, November 1997.

Pastin, Dr Mark, President of the Council of Ethical Organizations "A study of organizational factors and their effect on compliance" in *Proceedings of the Second Symposium on Crime and Punishment in the United States, DC Corporate Crime in America- Strengthening the "Good Citizen" Corporation*, United States Sentencing Commission, September 8 1995, Washington, page 142.

Patry, Marc W; Wexler, David B; Stolle, Dennis P; Tomkins, Alan J, "Conceiving the Lawyer as Creative Problem Solver: Article: Specific Applications: Better Legal

Counseling Through Empirical Research: Identifying Psycholegal Soft Spots and Strategies", 34 *California Western Law Review* 439, Spring, 1998.

Perritt Jr, Henry H, *Law and the Information Superhighway*, John Wiley & Sons, Inc, New York, 1996.

Perritt Jr, Henry H, "Legal and Technological Infrastructures for Electronic Payment Systems", 1996, 22 *Rutgers Computer & Technology Law Journal* 1, p 30.

Perritt Jr, Henry H, "Payment Infrastructures for Open Systems", 1995, http://ming.law.vill.edu/chron/articles/dir.htm.

Peterson, Mark A, *New Tools for Reducing Civil Litigation Expenses*, R-3013-ICJ, The Institute for Civil Justice, Rand Publications Series, 1983.

Press release of Senator Richard Alston, Minister for Communications, Information Technology and the Arts, Deputy Leader of the Government in the Senate dated 23 June 1999 at http://www.dca.gov.au/nsapi-graphics/?MIval=dca_dispdoc&ID=3981&template=Newsroom.

Professional Development Committee of the Council of the Law Society, "Proposal for a European Parliament and Council Directive on a Common Framework for Electronic Signatures-Comments by the Professional Development Committee of the Council of the Law Society", June 1998, http://techpolicy.ise.ac.uk/carc/sign/lawsoc.html.

Purchasing Australia, Commonwealth of Australia, *Managing risk in procurement- A handbook*, Australian Government Publishing Service, Canberra, 1996.

Reed, Chris, and Davies, Lars, "Digital Cash- the Legal Implications", IT Law Unit, Centre for Commercial Law Studies, Queen Mary & Westfield College, London, 1995.

Reid, Katharine; Clark, Eugene and Cho, George, "Legal Risk Management for Geographic Information Systems", *Journal of Law and Information Science*, Volume 7 No 2, 1996, p 170.

Report of Joint Committee of Public Accounts, Parliament of Australia inquiry into the commercial and revenue implications of the growth in electronic commerce, 27 May 1998: http://www.aph.gov.au/house/committees/jcpa/termscom.htm.

Review of Policy Relating to Encryption Technologies (The Walsh Report), February 1997, http://www.efa.org.au/Issues/Crypto/Walsh/walsh.htm.

Rissland, Edwina, "Comment: Artificial Intelligence and Law: Stepping Stones to a Model of Legal Reasoning", *Yale Law Journal*, Vol 99, June 1990, p 1957.

Robertson, RJ, "Electronic Commerce on the Internet and the Statute of Frauds", *South Carolina Law Review*, Summer 1998, vol 48, p787.

Robinson Thomas, John, "Note: Legal Responses to Commercial Transactions Employing Novel Communications Media", March 1992, 90 *Michigan Law Review* 1145.

Rosenoer, Jonathan, "Late-Night Thoughts on Electronic Commerce", *Law Technology Product News"*, p 42, col 1, October 1996, http://www.ljx.com/ltpn/october96/late_night_p42.html.

Heather Rowe, "Electronic Commerce: Legal Implications of consumer oriented electronic commerce" *Computer Law and Security Report*, vol 14 no 4 1998 232 at 236

Sadgrove, Kit, *The Complete Guide to Business Risk Management*, Gower Publishing Limited, Hampshire,k England, 1996, p 20.

Salter, TA, "The indivisibility of risk- the need for its systematic analysis and treatment", *Benefits and Compensation International*, May 1997, volume 26 no 9, pp 7-18.

San Miguel, Greg, an advertorial in *Company Lawyer*, vol 13 no 1, February 1997, p 72.

Saxby ,Stephen, "CLSR Briefing: Lack of jurisdiction defence rejected in Domain Name Dispute", *Computer Law and Security Report*, Vol 13, no 3 1997, p 210.

Saxby, Stephen ,"CLSR Briefing: Minnesota successfully claims jurisdiction over Internet services" *Computer Law andd Security Report*, Vol 13 no 2 1997, p 142.

Saxby, Stephen, "CLSR Briefing: No personal jurisdiction found in web site dispute", *Computer Law and Security Report*, Vol 14 no 2. 1998, p 143.

Schwartz, Warren F and Beckner III, C Frederick, "Article: Toward a theory of the meritorious case": Legal uncertainty as a social choice problem", 6 *George Mason University* Law Review, Summer 1998, 801.

Sharpe, Brian, "Problems in AS 3806 Implementation", *Compliance News*, Vol 10, July 1999, pp 7- 11 at p 9.

Sharpe, Brian, *Making Legal Compliance Work*, CCH Australia Limited, North Ryde, 1996.

Sharpe, Brian, and Dennings, Randal, *A Guide to AS 3806 -1998, Compliance Programs SAA HB133-1999*, Published by Standards Australia, Homebush NSW, 1999.

Sigler J, & Murphy, J, *Interactive Corporate Compliance: An Alternative to Regulatory Compulsion,* Quorum Books, New York, 1988, pp 79-107.

Silverstein, Alan, "Under the Hood of the World Wide Web", Paradesa Media, 1996-1997, http://www.learnthenet.com/english/html/70alan.htm.

Simensky, Melvin and Osterberg, Eric C, in "The Insurance and Management of Intellectual Property Risks", 17 *Cardozo Arts & Entertainment Law Journal* 321.

Smedinghoff , Thomas J, editor, *Online Law : the SPA's Legal Guide to doing Business on the Internet,* Addison-Wesley Publishing, Reading, Massachusetts, 1996.

Smith, Graham JH et al, *Internet Law and Regulation,* A Specially Commissioned Report, FT Law & Tax, London, 1996.

Standards Australia/Standards New Zealand Joint Technical Committee on Risk Management, "A Basic Introduction to Managing Risk using the Australian and New Zealand Risk Management Standard - AS/NZS 4360 - 1999", Master Draft as at 4/1/99.

Starke QC, J; Seddon, NC; Ellinghaus MP, *Cheshire and Fifoot's Law of Contract*, 6th Australian Edition, Butterwort

stats.electronic commerce in australia, april 1998, a study compiled by www.consult for the Department of Industry, Science and Tourism, 25 May 1998, http://www.dist.gov.au/html/new.html.

Steering Group of the Electronic Commerce Task Force, *Report of the Electronic Commerce Task Force to the Commonwealth Law Enforcement Board*, Commonwealth of Australia, November 1996.

"Summary of Electronic and Digital Signature Legislation" sponsored and maintained by the Information Technology and Electronic Commerce (ITEC) Law Department of the Chicago law firm McBride Baker & Coles: http://www.mbc.com/ds_sum.html.

Swish, Kara, "Seller Beware Consumers Aren't the Only Ones Who Risk Being Swindled Online", *Wall Street Journal Interactive*, December 7, 1998, http://interactive.wsj.com/public/current/articles/SB912732372726038000.htm.

Szafran, Marc E, "Note: A Neo-Institutional Paradigm for Contracts formed in Cyberspace: Judgment Day for the Statute of Frauds", 1996, 14 *Cardozo Arts & Entertainment Law Journal* 491.

Tax and the Internet, Discussion Report of the Australian Taxation Office Electronic Commerce Project Team on the challenges of electronic commerce for tax administration, AGPS, August 1997.

Taylor Eubank, Katherine, "Paying the Costs of Hazardous Waste Pollution: Why is the Insurance Industry raising such a stink?", *University of Illinois Law Review*, 1991, 173, 189.

The Auditor-General, *Risk Management in ATO- Small Business Income – Australian Taxation Office*, Commonwealth of Australia, The Auditor-General Audit Report No. 19, 1997- 98.

The Auditor-General, *Risk Management in the Australian Taxation Office*, Commonwealth of Australia, Audit Report No. 37, 1996-1997.

The Auditor-General, *Risk Management by Commonwealth Consumer Product Safety Regulators* Australian Government Publishing Service, Audit Report No. 12 1995-96.

"The Emergence of Electronic Commerce- Overview of OECD's Work", OECD Policy Brief No 1 November 1997 on Electronic Commerce, http://www.oecd.org/subject/electronic_commerce/documents.

The Emerging Digital Economy, Report of the Secretariat of Electronic Commerce, http://www.ecommerce.gov/EmergingDig.pdf, p 21.

The Presidential/Congressional Commission on Risk Assessment and Risk Management, *Risk Assessment and Risk Management in Regulatory Decision-Making*, Final Report Volume 2 1997.

Toy, Peter, "Class Action Exposure and Compliance Programs", *Compliance News*, Vol 10, July 1999, pp 11- 13.

Tyree, Alan, *Digital Cash*, Butterworths, Sydney, 1997.

Tyree, Professor Alan, *PINS and Signatures*, http://www.law.usyd.edu.au/~alant/inchoate.html.

UNCITRAL Model Law on Electronic Commerce, Excerpt from the Report of the United Nations Commission on International Trade law on the work of its twenty-ninth session (28 May-14 June 1996) General Assembly, Fifty-first Session, Supplement No. 17 (A/51/17), http://www.un.or.at/uncitral/texts/electcom/ml-ec.htm#top.

Understanding Risk Management in the APS-an ongoing challenge, an address to SES Officers in the Australian Customs Service by Pat Barrett AM, Commonwealth Auditor General, Tuesday, 26 March 1996, Canberra, Public Sector Accounting Centre of Excellence, Working Paper Series No. 1996.

United Nations Commission on International Trade Law, "Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce (1996)", http://www.un.or.at/uncitral/texts/electcom/ml-ec.htm.

US Department of Treasury, "An Introduction to Electronic Money Issues- Toward Electronic Money and Banking: The Role of Government", US Department of Treasury, September 19-20 1996, Washington, DC.

van der Smissen, Betty, JD, *Legal liability and risk management for public and private entities: sport and physical education, leisure services, recreation and parks, camping and adventure activities*, Anderson Publishing Co, Cincinnati, 1990.

Vaughan, Emmett J, *Risk Management*, John Wiley & Sons, Inc, New York, 1997.

VeriSign, *NetSureSM Protection Plan*, Version 1.0 - June 20, 1997, https://www.verisign.com/repository/netsure/; VeriSign, *NetSureSM Protection Plan Summary*, https://www.verisign.com/repository/netsure/summary/.

Victor, Marc B, "Ch 17 Litigation Risk Analysis™ and ADR" in John H Wilkinson, editor, *Donovan Leisure Newton & Irvine ADR practice book*, Wiley Law Publications- John Wiley & Sons, Inc, New York, 1990, pp-307-332.

Victor, Marc B, "The Proper Use of Decision Analysis to Assist Litigation Strategy", *The Business* Lawyer, Vol 40, February 1985, p 619.

Victor, Marc B, "How Much is a Case Worth? Putting Your Intuition To Work To Evaluate the Unique Lawsuit", *TRIAL*, July 1984, Vol 59, No 3, p 103-113.

Vose, David, *Quantitative Risk Analysis: A Guide to Monte Carlo Simulation Modelling*, John Wiley & Sons, Chichester, 1996.

Waldman, Adam R, "Comment: OTC Derivatives & Systemic Risk: Innovative Finance or the Dance into the Abyss, 43 *American University Law Review* 1023, Spring 1994.

"WWWIntro- WWW Acronyms", 1996, http://www.slis.ua.edu/wwwintro/www.htm.

Zammit, Joseph P and Galant, Felice B, "Legal Considerations in Doing Business on the WWW", published in conjunction with the thirteenth annual Computer Law: Negotiating Complex Transactions Seminar on April 28 and 29 1997, http:/www.ljx.com/internet/zammit.html.

Zinn, Herbert I Esq "Putting It All in Motion: Designing and Implementing an Effective Compliance Program" as reproduced in Robert M Hardaway, *Preventive Law - Materials on a Non Adversarial Legal Process*, Anderson Publishing Co., Cincinnati, 1997, p 199.

APPENDIX 1 SELF-COMPLETION QUESTIONNAIRES

Two self-completion questionnaires were developed, one for legal practitioners and risk managers who used risk management methodology in the context of legal risk entitled "How do you use risk management in the context of legal risk" **("Questionnaire 1")**, and one for risk managers who used risk management methodology in the context of Internet commerce entitled "How do you use risk management in the context of electronic commerce?" **("Questionnaire 2")**. Six participants agreed to respond to the self-completion questionnaire. Two participants were risk managers who used risk management methodology in the context of Internet commerce. They were sent Questionnaire 2. The other participants were sent Questionnaire 1. Of the other participants, two participants were risk managers who used risk management in the context of legal risk. Two participants were legal practitioners who used risk management methodology in the context of legal risk. In order to respect some participant's wishes the names of participants have not been disclosed.

QUESTIONNAIRE 1 HOW DO YOU USE RISK MANAGEMENT IN THE CONTEXT OF LEGAL RISK?

1. Are you familiar with the risk management methodology used in Australian Standard AS/NZS 4360 Risk Management 1999? (Australian Standard AS/NZS 4360 Risk Management 1999 characterises the risk management process as an iterative process involving the following: (1) establishing the context, (2) identifying risks, (3) analysing the identified risks, (4) evaluating and prioritising the identified risks and accepting those risks evaluated as "acceptable", (5) treating the remaining risks, (6) monitoring and reviewing the risk management system implemented, (7) communicating and consulting with relevant stakeholders throughout the risk management process.)

2. If yes, do you follow the risk management methodology used in Australian Standard AS/NZS 4360 Risk Management 1999 when applying risk management in the context of legal risk or do you use another methodology?

3. If you use a methodology different from that set out in the Australian Standard, could you describe the methodology and indicate from where you learnt this methodology?

4. When you evaluate a legal risk, do you use a qualitative (for example, use descriptive terms to categorise the significance of a legal risk) or quantitative approach (use statistical data to evaluate the significance of a legal risk)?

5. If you use a qualitative approach to evaluating legal risk, what techniques do you use? For example, Australian Standard AS/NZS 4360 Risk Management 1999 advocates using three scales to qualitatively analyse risk: (a) a scale for categorising the consequence of a risk, (b) a scale for categorising the likelihood of risk and (c) a scale for categorising the overall level of risk. Each risk is categorised according to its *consequence* and *likelihood*. Plotted on a matrix this enables the overall level of risk to be determined. Please provide as much detail as you can- it is very important for me to learn how risk management is used in practice.

6. Also, do you find that you have to rely on "gut feel" and intuition or, to put it in another way, your judgement and expertise when you evaluate a legal risk taking a qualitative approach? If yes, how do you justify doing so?

7. If you use a quantitative approach to evaluating legal risk please describe the techniques you use. Again, your answer is very important to my research.

8. Do you use quantitative or qualitative techniques when evaluating and selecting strategies for managing a legal risk? Please describe in detail the techniques you use.

9. If you use qualitative techniques to evaluate and select strategies for managing legal risks do you find that you have to rely on "gut feel" and intuition or, to put it in another way, your judgement and expertise? If yes, how do you justify doing so?

10. Do you see any difference between risk management when used in the context of legal risk and compliance? If yes, what are the differences?

11. Please specify how you would like to be cited eg Joe Bloggs, Risk Manager, XYZ Co.

QUESTIONNAIRE 2 HOW DO YOU USE RISK MANAGEMENT IN THE CONTEXT OF ELECTRONIC COMMERCE?

1. Are you familiar with the risk management methodology used in Australian Standard AS/NZS 4360 Risk Management 1999? (Australian Standard AS/NZS 4360 Risk Management 1999 characterises the risk management process as an iterative process involving the following: (1) establishing the context, (2) identifying risks, (3) analysing the identified risks, (4) evaluating and prioritising the identified risks and accepting those risks evaluated as "acceptable", (5) treating the remaining risks, (6) monitoring and reviewing the risk management system implemented).

2. If yes, do you follow the risk management methodology used in Australian Standard AS/NZS 4360 Risk Management 1999 or do you use another methodology?

3. If you use a methodology different from that set out in the Australian Standard, could you describe the methodology and indicate from where you learnt this methodology?

4. When you evaluate/analyse the risks associated with e-commerce do you take qualitative (for example, use descriptive terms to categorise the significance of a risk) or quantitative approach (use statistical data to evaluate the significance of a risk)?

5. If you take a quantitative approach, what techniques do you use to evaluate/ analyse the risks associated with electronic commerce? Please provide as much detail as you can- it is very important for me to learn how risk management is used in practice.

6. If you take a qualitative approach, what techniques do you use to qualitatively evaluate/analyse the risks associated with electronic commerce? Again, your answer is very important to my research.

7. Also, do you find that you have to rely on "gut feel" and intuition or, to put it in another way, your judgement and expertise when you evaluate a risk taking a qualitative approach? If yes, how do you justify doing so?

8. Do you use quantitative or qualitative techniques when evaluating and selecting strategies for managing a risk? Please describe in detail the techniques you use.

9. If you use qualitative techniques to evaluate and select strategies for managing risks do you find that you have to rely on "gut feel" and intuition or, to put it in another way, your judgement and expertise? If yes, how do you justify doing so?

10. Do you use risk management methodology to identify and manage the *legal* risks associated with electronic commerce?

11. If yes, do you think the legal risks associated with electronic commerce pose a significant impediment to the conduct of e-commerce?

12. Also, are there any legal risks in particular that you regard as posing a significant impediment to the conduct of e-commerce?

13. Please specify how you would like to be cited eg Joe Bloggs, Risk Manager, XYZ Co.

APPENDIX 2 DEFINITION OF TERMS AND VOCABULARY

Table 65 TERMS

ADMA Code of Conduct	Australian Direct Marketing Association's Standards of Practice
Australian business	A business, whose Internet commerce activities are conducted, from a location physically based in Australia, with parties who may be located within the same State/Territory in which the business is located, or with parties located interstate or overseas.
browser	A software application that is installed on a computer that enables the computer to access various features of the Internet (e-mail, ftp) but primarily to access the world wide web. In relation to the world wide web, a browser enables access to and reads another party's home page. This act is commonly referred to as 'browsing' or 'surfing the net'.
Bulletin Board System	A local computer system independent of the Internet, into which users can dial-in to download/upload files and to chat[701].
CISG Convention	United Nations Convention on Contracts for the International Sale of Goods.
contractual risks	The contractual risks to businesses associated with conducting Internet commerce.
cyphertext	Plain text that through the application of encryption has been rendered into an unreadable form.
download	To copy information transmitted on the Internet onto your own computer.
Electronic Commerce Expert Group Report	Report of the Electronic Commerce Expert Group to the Attorney-General entitled "Electronic Commerce: Building the Legal Framework", 31 March 1998.
Electronic Data Interchange (EDI)	Protocol for the exchange of messages in standardised form from one computer to another.
encryption	The technique of encoding data or information ("plaintext") to render it into an unreadable form ("cyphertext") except by those parties who know the code or cypher ("key").

[701] glossary, *internet.au*, 18 April 1997

formation	Formation of a contract.
hash value	A mathematical algorithm, which, if applied to an Internet communication, results in a compressed form of the Internet communication.
header	The top of an e-mail or newsgroup message that specifies where the message came from and when it was sent[702].
home page	A document that has been uploaded onto a server that is linked to the Internet. The document is formatted, usually in HTML, so that it can be accessed and read (browsed) by any computer that is linked to the Internet. The document can comprise text into which a combination of images, sound and movies, hypertext links and other interactive features have been embedded. The term home page is often used to describe the entry page or front page of a business's web site. The term is also used to describe an individual's personal web page.
HTML (Hyper Text Markup Language)	The code used for formatting web pages so that they can be browsed by any computer that is linked to the Internet regardless of that computer's specifications.
HTTP (Hyper Text Transport Protocol)	The retrieval method used to read web pages.
hypertext link	Text in a web page that, when selected, conveys the user to another web page or hypertext link whether on the web page owner's web site or the web site of another party.
IIA Code of Practice	Internet Industry Association Code of Practice.
Internet commerce	The trade and commercial activity (including advertising and marketing activity) that takes place on the Internet between a business and its customer whether it be business-to-business commerce or business -to-consumer commerce.
Internet communication	All messages, data or information that can be transmitted through the Internet including e-mail messages and data and messages transmitted by way of browser.
Internet transaction	A contract conducted on the Internet.
key	The code or cypher that can decrypt cyphertext.
legal risk management	The application of risk management in relation to the legal matters that affect a business's activities.

[702] glossary, *internet.au*, 18 April 1997

legal risks associated with establishing identity	The legal risks associated with Internet commerce that arise because Internet commerce lacks face-to-face contact.
memorandum in writing	The first element of the Statute of Frauds writing requirement, that is, the existence of a memorandum upon which is written the material terms of the contract agreed to by the transacting parties.
newsgroup	Network of newsgroups[703].
OECD	Organisation for Economic Co-operation and Development
Off-line commerce	Commerce that is conducted off the Internet.
on-line payment	Payment made through the Internet.
performance	Performance of a contract.
plaintext	Unencrypted data or information.
public key encryption	A form of encryption that uses a mathematically matched pair of keys, a public key and a private key to encrypt and decrypt data or information.
risks	Aspects of a business's activities that may result in exposure to significant loss.
server	A computer that stores information that is available to external users[704].
SET	Secure Electronic Transaction- a protocol designed specifically for effecting secure payments on the Internet.
single key encryption	A form of encryption that uses a single key to encrypt and decrypt data or information.
Statute of Frauds writing requirement	The legislative requirement (derived from the Statute of Frauds 1677 (UK)) that in order for specific categories of contract to be enforceable they must be evidenced in writing and signed by the party against whom a contract is sought to be enforced.
UNCITRAL	United Nations Commission on International Trade Law
URL	Uniform Resource Locator - the "address" by which a web page's location is identified.

---

[703] glossary, *internet.au*, 18 April 1997
[704] glossary, *internet.au*, 18 April 1997

web	World Wide Web
web page	A file located on a server that is coded in HTML. This file enables both graphical elements and text to be displayed on a computer that is connected to the Internet regardless of the operating system or browser used to access the Internet.
web site	The web pages of a party that are hypertext linked, often with navigation icons or bars, so as to form a single site.