A Deterrent Measure Against Computer Crime: Knowledge-based Risk-analytic Audit

Wanbil W Lee
Lingnan College

1 Introduction

Computer crime has been a key issue in management since the early 1970s (Weiss, 1974) and remains so in modern times (Loch et al, 1992; Bock and Schrage, 1993). As more people have access to computers, the opportunities for abuse also increase, for example, siphoning money and manipulation of information for personal gain attract professionals as well as amateur criminals (Parker, 1983; Riley, 1993). Computer crimes and computer-related outlaws proliferate like the "bamboo shoot after a Spring rain".

(a) Inadequacy of Existing Measures

Legislative measures may help and laws against computer related crimes have been instituted (Lee, 1984a; 1985a). In the USA, for instance, there are: (i) the *Computer Fraud and Abuse Act* of 1986 (which provides penalties for fraud and related activities connected with the computer and its access devices); (ii) the *Computer Security Act* of 1987 (which protects computer-related assets, viz hardware, software, data and documentation); (iii) the Electronic *Communications Privacy Act* of 1986 (which updates wiretap and privacy statutes for protection specifically related to advancements in technology); and (iv) the *Privacy Act* of 1974 (which protects the privacy of information related to individuals that is maintained in federal information systems). In the UK, the *Copyright Act* of 1988 provides that illegal reproduction of software can be subject to civil damages with no financial limit, and criminal penalties including fines and imprisonment while the *Computer Misuse Act* of 1990 covers three offences: unauthorised access to computer material, unauthorised access with intent to facilitate commission of further offences, and unauthorised modification of computer material.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission. www.

However, these measures are limited as legislation always lags behind the act of crime. Even when there are well justified intentions to proceed with legal action, prosecution is not straightforward. For example, victims are reluctant to report the crime for fear of negative publicity (in the case of business or government organisations) or damage to personal reputation (in the case of individuals). Critical evidence can be easily altered or erased, or difficult to prove, as in the case of theft, where the original information is still physically intact so that the owner is not necessarily denied access to or use of the stolen information. Further, the audit trail disappears or is simply non-existent in many cases of computer crime because the perpetrator almost always manages to cover up or destroy any trace of his or her act.

Management control schemes abound. However, the effectiveness of schemes such as staff awareness programme, pre-employment screening, compulsory rotation of duties, passwords control, access on a need-to-know basis and user logs has been gradually reduced as computer criminals become more manipulative and sophisticated.

(b) Need for a New Deterrent Measure

Changes in the computer industry's strategy and practice abet computer abuse and impact our lives and our privacy (Lee, 1983a). In the early days, hardware was developed first and then software. Developers were not capable of coping with the human aspects of the application systems so that considerations for control and security were put aside. The entire attention of the industry and the profession was directed towards solving the hard, technical problems or satisfying the primitive, physiological needs (in the Maslow sense). Now both hardware and software have been developed to such a level of sophistication that it is time to address soft issues, such as accessibility to and integrity of personal information. Privacy, data protection and freedom of information are of pressing concern in the age of information since it is the ready accessibility of information that makes a person vulnerable and open to abuse. For example, if a person's credit rating is tampered with, or if his or her record is altered, then there will be grievously unpredictable consequences affecting that person's business and other transactions (Sendrow, 1982).

Under poor or inappropriate control, end users may be deprived of the opportunity to benefit from the full potential of computer-based information systems. Proper control must be devised to safeguard the environment in

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission. www.ma

which computer systems perform the functions of storing, retrieving, transforming, and generating information. Strategic schemes must be developed to prevent frauds from occurring rather than detect and correct frauds after they have occurred. The following case demonstrates succinctly an example of prevention (Chen and Lee, 1989):

> In order to determine compliance with respect to the set price policies, the Price Bureau in Guangdong Province, China, undertook in November 1988, a review of the accounting records and vouchers of registered companies. The review of XYZ Co's computerized accounts disclosed that there was a discrepancy titled "illegal revenue" of RMB 230,000 Yuans. The news of this discovery was soon spread within the company and outside. As a result, before the audit team moved in to carry out the review exercise at one of XYZ's other subsidiary companies at He Nan, this He Nan subsidiary confessed voluntarily that it committed an illegal revenue of RMB 90,000 Yuans.

A multidisciplinary approach is described below, which incorporates these elements: (i) a *specialised control mechanism* which is installed within the computer to help prevent "hacking" into, for example, bank accounts and confidential personal records; (ii) a *deterrent mechanism* which has an implied control capability over the computer and its activities in information handling and information generation; and (iii) a *computer-based information system* within which are encapsulated the appropriate intelligence of auditing experts and risk analysts – that is an integration of Expert Systems concepts, Risk Management techniques and Auditing principles and procedures. This forms the basis of Knowledge-based Risk-analytic Audit (KRA Audit).

(c) Presentation

Four main topics are presented in this paper: (i) Computer Crime – a briefing on one of the most common of computer security breaches; (ii) Computer-based Audit – an overview of computer-based audit showing the progression from traditional EDP Audit to Knowledge-based Audit (KB Audit) and Risk-analytic Audit (RA Audit), culminating in KRA Audit (see Table 1); (iii) The KRA model – a description of the model together with the design issues that need to be addressed ; and (iv) Case Illustration – a simulated case of auditing the computer operations of a bank's computer network in Hong Kong, using a prototype constructed in an earlier study (Lee, 1994; Lee, 1995).

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission. www

Table 1: Summary of Various Audit Approaches

Types of Audit	Description
EDP Audit	Audit using computer techniques or audit of computer-based systems
KB Audit	Audit using Knowledge-based or Expert Systems techniques or audit of Knowledge-based Systems
RA Audit	Audit using Risk Management techniques
KRA Audit	Extension of EDP Audit by combining the capabilities of KB Audit and RA Audit

2 Computer Crime

(a) Basic Concept

Computer crime can be *computer-aided* or *computer-related*. In the former case, computers are used to manipulate other computers in order to effect a computer crime. That is, the computer is the tool or instrument used to commit the crime, for example, corporate espionage is the most prevalent computer-aided crime world-wide. In the latter, the information stored within the computer is manipulated to the detriment of the subject (an individual, a group of individuals, or an organisation) of that information, and the computer itself is subject to attack, that is, the computer is the target of the crime, for example, sabotage, wiretapping/bugging and terrorism (Forcht, 1994).

There is a large variety of unlawful activities or security vulnerabilities (Sieber, 1986; Neumann, 1995). For example, we are warned of "the new criminal" (Parker and Nycum, 1974); we are urged to look into "privacy policies and practices inside the organisation" (Smith, 1993); we are advised to address "computing and accountability" (Nissenbaum, 1994); and we are alerted to "cyberpunk" (Hafner and Markoff, 1991) and "threats, viruses and countermeasures" (Blanton and Rosenberger, 1991).

(b) Related Concepts

Computer abuse, a closely related issue to computer crime, is any intentional act that may or may not violate criminal laws but involves the computer such that the perpetrator makes a gain or the victim suffers

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission. www.ma

a loss or both. In data diddling, a common form of computer abuse, for example, a data entry operator, who is assigned to handle data entry of overtime hours, enters the overtime hours of other employees under his own employee number so that he gets the pay. In this case, the perpetrator – the data entry operator – gains what the victim – the employer or the other employees or both – lose.

Computer fraud, another commonly related issue, occurs when someone uses the computer directly or indirectly to deliberately misrepresent or deceive, or to cover up the embezzlement of goods, services or information. Here are some common types of computer fraud: (i) Trojan horse – the secret insertion of computer instructions in a computer program to perform unauthorised acts when the program is executed; (ii) salami – an unauthorised, covert process of taking small amounts (slices) of money from sources using the computer, for example, putting into the criminal's own account the fractions that remained after rounding up or down to the nearest cent in interest rate calculations; and (iii) ATM fraud – a fraudulent act through an automatic teller machine to fake a deposit, to erase a withdrawal, or otherwise to divert funds from another person's account through a stolen PIN (personal identification number).

3 Computer-based Audit

(a) Traditional Audit

Audit is to ensure that no malpractice takes place. The process consists of essentially three steps: (i) to *accumulate* evidence about quantifiable information related to a specific economic entity; (ii) to *evaluate* the collected evidence; and (iii) to *report* the quality of the quantifiable information against established criteria by a competent, independent person - the auditor. In this context, evidence can be any information used by the auditor and takes many forms; "economic entity" which is always qualified by the time period involved is in most cases a legal entity such as a firm or a government agency; and "quantifiable information" implies that the information involved is verifiable in accordance with some pre-set criteria.

In general, there are two types of audit: *operational audit* which is a review of the organisation's operating procedures and methods in order to evaluate efficiency and effectiveness, and *compliance audit* which is to determine that specific procedures or rules set down by management are followed (Aren and Leobbecke, 1994). The following steps, taken together, encompass both operational audit and compliance audit: (i) to take a snapshot

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission. www

of the current situation; (ii) to study and compare the findings from the snapshot with established requirements (standards); (iii) to determine compliance with or violation of the standards; and (iv) to recommend managerial, remedial actions where necessary and appropriate.

(b) EDP Audit

Since the early 1950's, the computer has been applied increasingly to solve accounting problems. Billing, payroll, inventory control, and sales analysis were among the earliest and most successful applications. With the application of computer-based accounting information systems and new technologies, auditors were in urgent need of additional tools and methodologies because conventional ones were becoming inadequate and invalid. Computer-based techniques (Cash et al, 1977) and Computer or EDP Auditing (Weber, 1988; Watne and Turney, 1990) were developed.

EDP Audit can be *audit around the computer, audit through the computer* or *audit with the computer*. In the case of audit around the computer, this means simply the matching of the input against the output and the reconciling of discrepancies, if any, and the computer is treated merely as a black-box and is "bypassed" in the audit operations (Milko, 1973). In the audit through the computer approach, the computer and its associated software are the target of audit (Milko, 1973; Cerullo and Corless, 1984). Lastly, in the audit with the computer approach, the computer and the software become both the target of audit and the tools of auditing (Jancura and Beger, 1973).

Typically, in these approaches, dual-purpose testing is applied directly to the hardware and the software components of the systems. Briefly, dual-purpose testing means concurrent performance of compliance testing (to determine whether the prescribed controls are functioning as designed) and substantive testing (to verify details of transactions and balances and to analyse review procedures applied to financial information). However, the diagnosis and determination of an EDP audit depend entirely on the relationship between output and input. The failure to address loopholes and opportunities for computer crimes and changes brought about by the more sophisticated applications of the computer itself made this approach inadequate (Mastromano, 1980; Andersen, 1982; Bariff, 1982; Mertan and Severance, 1983; Varsarhelyi, 1984; Munter and Ratcliffe, 1985; Davis and Weber, 1986).

Many new problems are introduced as a result of the application of more advanced approaches and the current technological impact on the business, its operation, and its environment. The first problem is the matching

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission. www.ma

of the cost (difficulty) against the benefit of having modern information technologies incorporated into manual and labour intensive audit procedures. Two main difficulties encountered are: (i) the limits that database systems place on generalised audit software packages restrict the intended scope of audit; and (ii) the complex interactions between an organisation's information systems, such as the on-line interactive order processing system and inventory control system of a wholesaler, further complicate the audit operations and increase the audit cost (Varsarhelyi, 1985).

The second problem is that complex tools and techniques – such as computerised internal control questionnaires and audit trail sampling – are used in conducting an audit assignment because auditors must deal with a vast amount of hard data, for example, account balances and cash receipts. This set of data may, however, be scattered among many subsystems in an organisation (as in the case of a distributed data base system), so auditors must integrate the subsystems involved in order to collect the data and to provide the required information in a useful form. These techniques may not be familiar to the auditors and thus become an extra burden (Garner and Pinnis, 1984).

The third problem is that risks of subjectivity exist when auditors seek, with varying degrees of faith and competence, to verify that a judgement already made is reasonable and is made in accordance with official standards (say, AICPA, 1988). The auditors rely heavily on their subjective interpretation of the collected data in generating and evaluating alternative solutions. Also, verification and judgement invariably take place under uncertainty. While automated, integrated systems may bring about a certain degree of reduction of the risks, the time taken to run the audit exercise may be prolonged and the budget for audit thus becomes more constrained. The time available, in virtually all cases, to judge the quality of audit decisions is limited, and automated and integrated systems make it more difficult to comply with that time limit.

The fourth problem is that the audit process must be equipped with technologically sophisticated tools and techniques so as to match the way the modern business is run (for example, group operation), the environment in which modern business systems operate (for example, multi-national), and the structure of a modern business system (for example, distributed data processing systems). Making audit decisions are therefore more difficult, and inappropriate or incorrect decisions more costly (Lee, 1983b).

To solve these problems, auditors and information managers need an innovative methodology and up-to-date knowledge and skills of

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission. www

information technology. Consequently, intelligent computer-based systems and risk-analytic procedures have been introduced, leading to KB Audit and RA Audit respectively (Lee, 1988).

(c)KB Audit and Expert Systems

Expert systems is an area of interest in "artificial intelligence", which is a branch of computer science. Briefly, artificial intelligence makes use of the computer to solve problems just like a human expert does (Forsyth, 1984; Yazandi, 1985; Rich and Knight, 1991), while expert systems, as a field, is concerned with encapsulating human intelligence (to be stored in a *knowledge base*) and harnessing human expertise in whatever field that expert services are required and programmed for (by the *inference engine*) (Michie, 1980; Buchanan and Duda, 1983; Cox, 1984; Hayed-Roth, 1984; Yager, 1985; Waterman, 1986; Anderson, 1992).

Nowadays, the tasks of building expert systems are simplified by using a special type of software called *expert system development shell*. The shell is a framework designed and constructed to assist knowledge engineers (for example, the Knowledge-based systems developers) in increasing a knowledge base by structuring, testing, modifying and expanding the knowledge obtained from the expert. Typically, a shell consists of a set of knowledge acquisition tools, a battery of test cases (to verify the knowledge base created), and an interface mechanism (to facilitate the development process). The data and knowledge captured and stored in the knowledge base are the domain-related information and the rules relevant to the applications of interest (Hayes-Roth et al, 1983; Weiss and Kulikowski, 1984; Gilmore and Howard, 1986; Debenham, 1989; Gonzalez and Dankel, 1993).

Expert systems have been applied successfully in the past to solve different kinds of problems, for example, medical diagnosis (Shortliffe, 1975), computer systems configuration based on customer specifications (McDermatt, 1981), and auditing (Lee, 1986; Chu, 1989). Indeed, expert systems will eventually help conserve and preserve human intelligence – particularly an individual's accumulated intuitive, and tacit and practical experience and knowledge – that the natural hereditary process sometimes fails to accomplish. However, in planning and adopting an expert systems approach, possible limitations and challenges of applying artificial intelligence should also be considered (Bobrow et al, 1986; Luconi et al, 1986; Socha, 1988; Mykytyn et al, 1990).

Of particular interest here are the expert auditing systems. Table 2 shows a number of expert audit systems and their functions, which have

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission. www.ma

Table 2: Expert Audit Systems

Expert Systems	Functions	Author(s)
TAX ADVISOR	for income and transfer tax planning using an artificial intelligence rule-based model which is refined and verified by a panel of taxation experts	Michaelsen, 1982
AUDIT PLANNER	for making materiality judgements and providing recommendations of a planning level of materiality for the overall audit, subject to the characteristics of the company being audited, the perceived needs of the users of the financial statements, the degree of risk associated with the audit, and the auditor's attitude towards the risks involved	Steinbart, 1984
Internal Controls Evaluation	for investigating the process by which experienced auditors evaluate internal accounting controls using a computational model	Meservy, 1985
INTERNAL-CONTROL-ANALYZER	for evaluating internal accounting control on the integration of database technology into information management activities, and on the formulation of a large corporate wide database	Gal, 1985
AUDITOR	for assessing the adequacy of a company's allowance for bad debts	Dungan and Chandler, 1985
EDP-XPERT	for making judgements on the reliability of controls in advanced computer environments	Hansen and Messier, 1985
TICOM	for identifying the strengths and weaknesses of a client's accounting information systems, aiming to provide a "computer-assisted method of designing, analysing, and evaluating internal control systems"	Bailey et al, 1985
Audit Opinion	for audit opinion decisions	Dillard and Mutchler, 1986
Citibank's Pension Cheques	for processing, at Citibank, accurate pension cheques on application of a new tax laws	Keyes, 1992
Investment Counselling	for helping investment counsellors advise clients about investment opportunities and strategies	Heuer et al, 1992

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission. www

been described in the literature.

The KB Audit follows essentially the systems-based contemporary audit framework (Stettler, 1981) and extends the capability of an EDP Audit by incorporating audit expertise into the audit process. It is feasible because: (i) auditing relies on both subjective and objective input and interpretation of the results; (ii) through artificial intelligence auditing expertise can be accumulated in the same way as human intelligence can be conserved and become portable and transferable; (iii) intelligent techniques have advantages of consistent decision making, independence of individual bias, transferability of critical judgement to less experienced persons, and avoidance of the frequently encountered personal conflict and face-to-face confrontation amongst the auditors and their clients; and (iv) practising auditors have not only accepted expert systems as a viable aid, especially appropriate for assisting auditor judgement in statistical sampling, risk evaluation, analytic review, internal control, going concern evaluation, and audit opinion, but have also indicated that they see no threat to them personally or to the audit profession as a whole (Hansen and Messier, 1982).

The KB Audit is characterised by a general knowledge base, automated knowledge acquisition tools, and reasoning processes. The *knowledge base*, the nerve-centre of the KB Audit approach, contains the audit methodology, the knowledge which is needed in order to make the software compatible with a human expert, and the generic structure of the problem domain. *Knowledge* refers in this context to expertise that is made up of all the required information and experience (intrinsic and intuitive) together with the psychological, social and cultural inferences that contribute towards making a person an expert. *Automated knowledge acquisition* tools are designed to be consistent with the lexical, syntactical, semantic and programmatic rules and requirements for data capture. The *reasoning processes* represent the coded causal knowledge.

(d) RA Audit and Risk Management

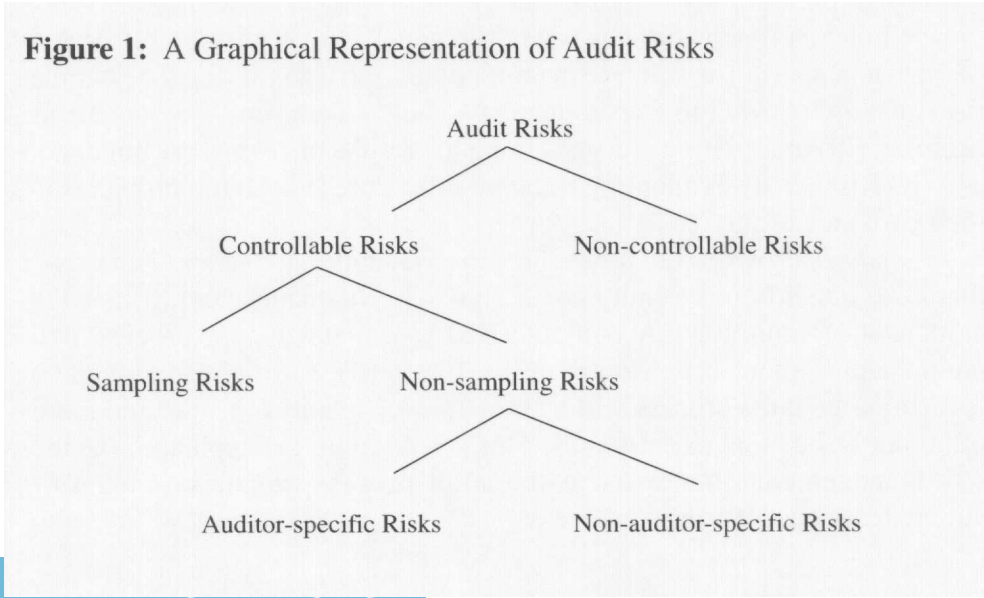
Risk may refer to the damage that can result if a threat is actualised or it may mean a measure of the expected damage given by the product of likelihood and the extent of the consequences. *Threat* is the danger that a vulnerability can actually lead to undesirable consequences, and *vulnerability* is a weakness that may result in undesirable consequences. *Risk management* is essentially the process of attempting to minimize any adverse effects of risks at the least cost. It makes use of Bayesian statistical techniques and takes an a *priori*, predictive and preventive approach (Lee, 1980; Dorfman, 1991). It differs from *insurance*

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission. www.ma

management in the sense that the latter takes a protective approach and is a tool for protection against risk by transferring risk to an insurer to whom the return is the payment of the premium. The unknown cost associated with a risk that may or may not eventuate is exchanged for a known and budgetable premium (Williams and Heins, 1989).

Audit risk (see Figure 1) is represented by the probability that the auditor gives an inappropriate audit opinion because of material errors, the auditor's failure to detect irregularities that exist, or the possibility of disclaiming an opinion or issuing a qualified or adverse opinion when, in fact, the economic facts do not support such an audit conclusion. Audit risks can be classified as *controllable risks* which occur when the auditor fails to detect a material error and *non-controllable risks* which are caused by errors that are beyond the control of the auditor, for example, a conclusion derived from a faulty process which may be due to questionable integrity of management or loose internal control. Controllable risks can be divided into *sampling risks* which occur because there are objective means for determining sampling errors for judgmental, non-randomly selected samples (although it is possible to determine and assess objectively sampling errors for randomly selected samples), and *non-sampling risks* which arise because of inherent problems associated with the interpretation or accumulation of test results. Moreover, non-sampling risks can be *non-auditor-specific*, that is due to misrepresentations to the auditor by a third party or by management, or *auditor-specific*, which can be attributed to inadequate planning and supervision, lack of audit staff integrity, lack of competent personnel to perform audit functions, or oversight errors (Warren, 1979; Steele, 1992).

Figure 1: A Graphical Representation of Audit Risks



Reproduced with permission of the copyright owner. Further reproduction prohibited without permission. www

Risk management has been applied successfully to a variety of domains, for example, finance and investment (Hertz, 1964; Spetzler, 1968; Johnson and Khan, 1976), EDP and software (USDC/NBS, 1979; Perry, 1982; Boehm, 1989; Rainer et al, 1991; Sherer, 1992), computer/data security (Campell and Sands, 1979; Ross, 1979; Lee, 1984b and 1985b), and auditing (Warren, 1979; Lee, 1983b; Grobstein et al, 1985). In operational terms, risk management is concerned with containing risks, which may have been ignored or overlooked in the past. Table 3 shows the four major steps in risk management (Australian Public Service Board, 1981; Ansell and Wharton, 1992).

Table 3: Four Major Steps in Risk Management

Steps	Functions
Identification	to persuade and to obtain senior management commitment to Risk Management, meaning to set objectives for the exercise, to identify and assign responsibilities, and to set system boundaries in terms of personnel, hardware, software, etc
Evaluation	to identify threats (both actual and potential), to analyse risk and vulnerability, and to perform risk assessment
Decisions	to review undesirable events and to evaluate identified control measures
Action	to develop a comprehensive risk management plan, to test the selected controls, to carry out continuous monitoring, and to have a contingency plan ready to be brought into action when a disaster occurs

While this framework has been used widely for a considerable period of time, non-specialists still face the difficulties of (i) identifying the possible risks that are relevant to the problems on hand; (ii) starting a risk analysis exercise; (iii) interpreting and presenting the results once they are obtained; and (iv) Risk Analysis adopting standard procedures in solving problems in their own area of interest.

Analysis provides the procedures to: (i) identify and assess audit risk, that is, to quantify uncertainty and assign losses/damages, and (ii) test the associated assumptions. A computerised risk management process will undoubtedly extend its power and utility. If expertise (artificial intelligence) is incorporated, the process will be more powerful and versatile, and more importantly, be more user-friendly. This is RA Audit, the application of the risk management framework to the audit process (whether manual or automated) (Lee, 1985b).

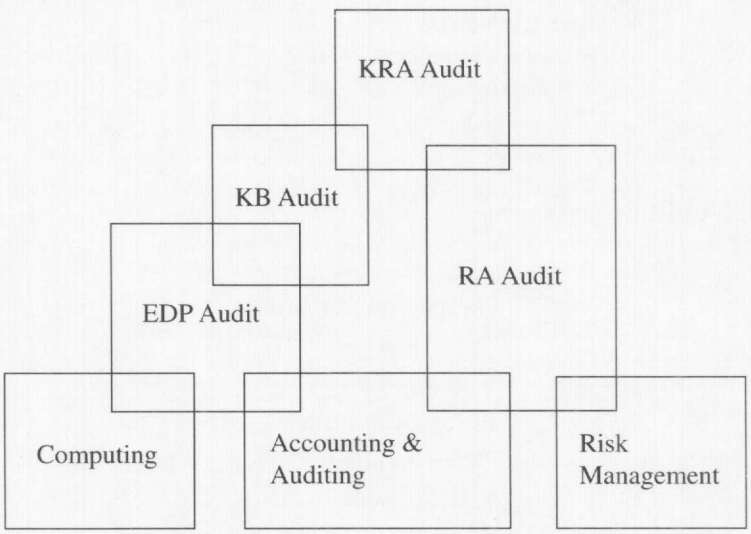
Reproduced with permission of the copyright owner. Further reproduction prohibited without permission. www.ma

4 The KRA Model

(a) Theoretical Framework

The theoretical framework, on which the multidisciplinary approach is built and in which the conceptual relationship linking the diverse fields is accommodated, is depicted in Figure 2. As shown in Figure 2, the KB audit evolves from EDP Audit which is in turn developed from the Computing and Accounting/Auditing disciplines and application areas. RA Audit emerges as a result of applying Risk Management to Accounting/Auditing problems. KRA Audit is an extension of the capabilities of the advanced KB Audit and RA Audit.

Figure 2: Conceptual Relationship Linking KRA Audit to Other Disciplines



(b) Design of the Model

Three design issues must be resolved: (i) the design must address the strategic requirements of selection of the best tool(s), knowledge acquisition, and an interactive mode of operation; (ii) the design must have the built-in capacity of Risk Estimation (discovery and identification), Risk Evaluation (measurement) and Risk Control (decision) (Courtney, 1977), which together with the Database (DB) and the Knowledge Base(KB), make up the major components of the model; and (iii) the design must align the functions of the model (see Figure 3) with the audit process (see Figure 4) (Varsarhelyi, 1985).

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission. www

Figure 3: The KRA Model

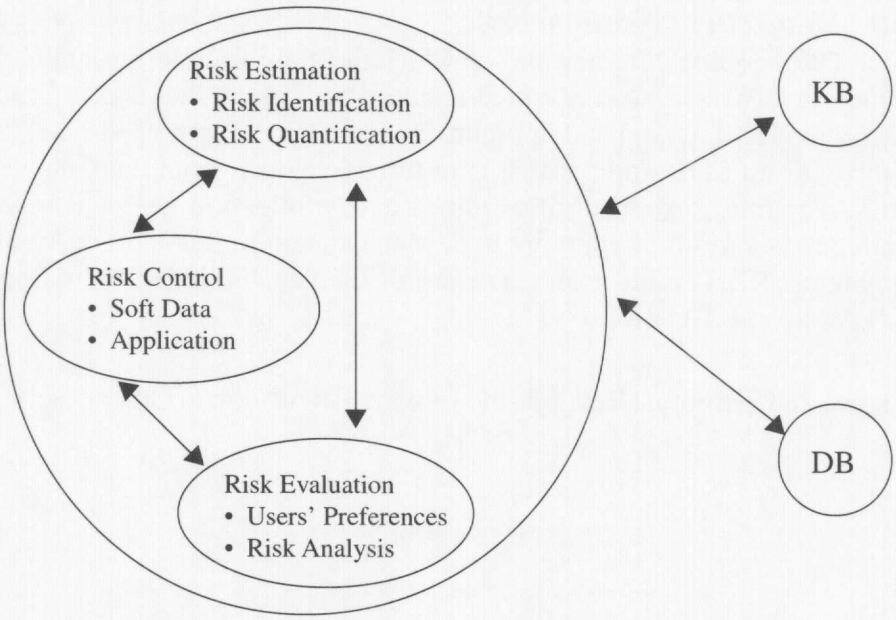
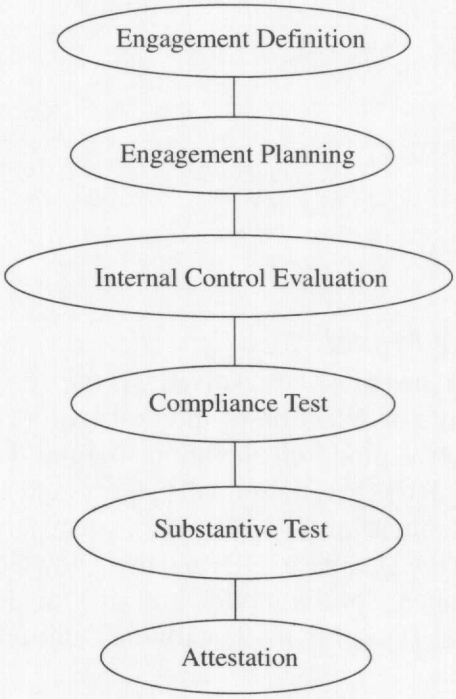


Figure 4: Audit Process

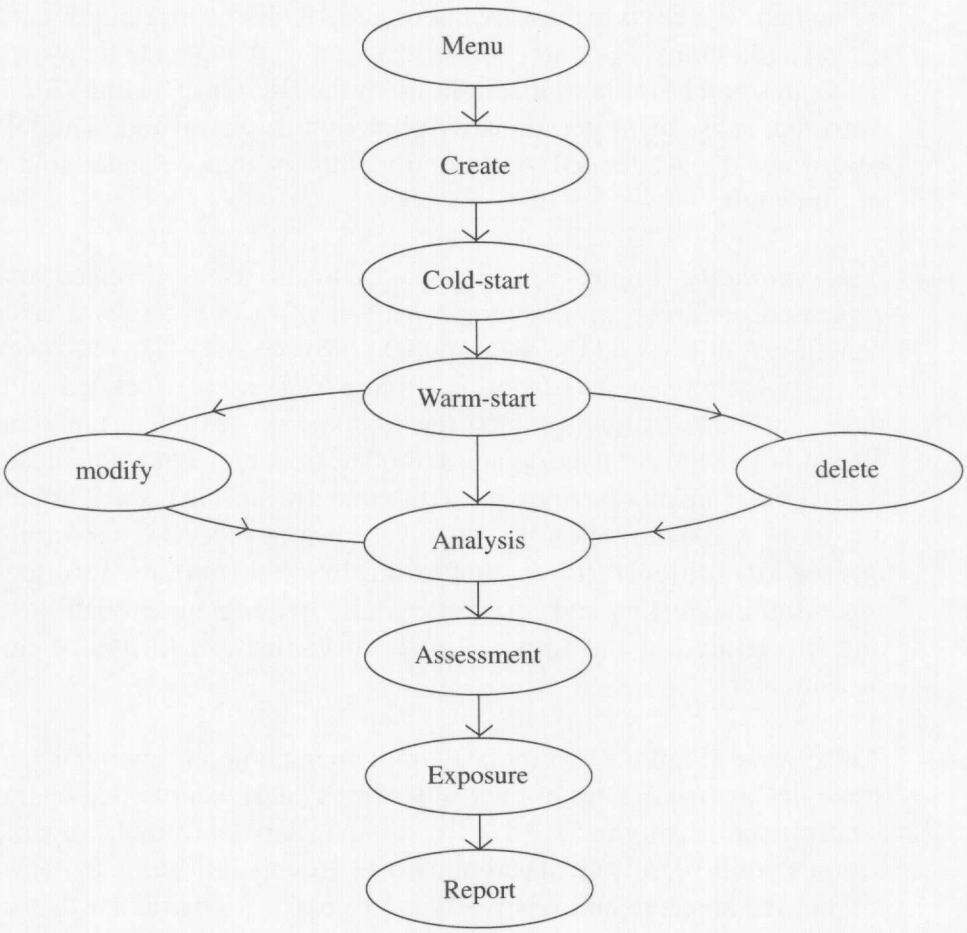


Reproduced with permission of the copyright owner. Further reproduction prohibited without permission. www.m

(c) Operations of the Prototype

A prototype, based on the KRA model functionalities, has been constructed (Lee, 1995). The instruction set of the prototype is displayed in Figure 5.

Figure 5: Prototype of KRA



The interrelationship between the model (Figure 3) and the prototype (Figure 5) can be described as follows:

(1) *Risk estimation* (Figure 3): After taking a complete inventory of the potential pure risks (areas for audit) in physical, psychological and social terms (discovery and identification), and quantifying these risks, users should remember that risk discovery is a subjective and intuitive

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission. www

process. During the discovery and identification stages, users can adopt either a warm-start or cold-start procedure (Figure 5). *Warm-start* (for users who need a lead to kick off the procedure) provides, for a given application (a particular audit project), a pre-programmed list of risk factors (audit items). The user can, as a result of examining the given list, add items to or delete items from the list. The discovery and identification of risk factors can be performed iteratively until the user is satisfied. The DB is in this case interrogated to discover, retain/discard or add audit items. *Cold-start* (for users who wish to create their own list from scratch) initiates the build-up of the list. Once a cold-start is executed, subsequent iterations will function as warm-start. The DB here stores the list created. As an option, this list may be added to the system's DB.

(2) *Risk evaluation* (Figure 3), with respect to the users' revealed and expressed preference, refers to the analysis of risks in terms of cost/benefit and utility, and the measurement of those risks. This involves *analysis, assessment* and *exposure* (Figure 5). Losses associated with the identified risks (audit items) must be *measured* to determine the effect of these losses on the organisation. The measurement will indicate the risks that are most serious, and consequently most in need of urgent attention. While the measurement strives towards objectivity, a certain degree of subjectivity is unavoidable. Personal preference, organisational history and corporate culture in assigning probabilities and in estimating the impact on the organisation influence the measurement.

3) *Risk control* (Figure 3) formulates implementation and maintenance strategies by making use of the result of risk analysis provided by the *report* function (Figure 5) and of the soft data derived from the organisation's political, historical and other background indicators. In determining the absolute and relative "seriousness" of a particular factor, based on threat and vulnerability analyses, decision makers need to assign an exposure rating (an estimate of likelihood of possible loss or harm in a computer system) of factor (Pfleeger, 1989). The final conclusion would be based on the exposure rating plus any necessary adjustment due to the decision maker's collection of soft data. The results can be retrieved using the report function.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission. www.m

Details of the instructions of the prototype are briefly described in Figure 6. Besides being interactive, the prototype is also cyclic and iterative. The user can back-track at any step for further clarification and restart using fresh or re-discovered data in a cyclic fashion iteratively. For example, the user may step backwards from the "exposure" step to the "assessment" step to reassess a damage value or to the "analysis" step to reassign a probability figure, and so on. The next section illustrates the operation of the KRA prototype.

Figure 6: The Instruction Set of the Prototype

DIRECTORY or MENU – displays a list of all the applications currently available

EXPOSURE – computes exposure of all risk factors (rf) in the currently activated list using the following formula:

ALE = (10 exp (p + D -3)/4.

where ALE is the annual loss expectancy,

P is the frequency of occurrence rating, and

D is the damage rating

(Note: Typically, ALE is the estimated loss due to the occurrence of a certain event. For convenience of planning, for example, ALE is usually assumed on an annual basis. There is a number of formula or algorithms developed for this purpose, for example, RISKCALC^{R} in Pfleeger (1989, pp 465-467); and others in Rainer et al (1991). The higher its ALE, the more risky is the event, that is, more prone to computer crime and more protective precaution needed.)

CREATE – allows creation of a new list of rf

DELETE – allows deletion of an existing list of rf

MODIFY – allows changes to be made to an existing list of rf

WARM-START – allows call-up of an existing list of rf and enables MODIFY

COLD-START – same as CREATE

ANALYSIS – allows assignment of a probability to an identified rf

ASSESSMENT – allows assignment of a value (damage/loss) to an identified rf

REPORT – provides an interpreted report of the result

5 Case Illustration*

(a) Scenario

The Deretrach Bank Limited operates as a multi-national. It adopts a management structure whereby both the information systems and the audit

*The name of the bank is fictitious to preserve the anonymity of the organisation. The story has been dramatised but it is indicative of an actual situation.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission. www

functions are placed at the very top level. Each of these functions is under the charge of an executive director. Upon a Board resolution, an annual review of its information systems function was undertaken, with particular focus on its Information Management Centre in Hong Kong.

The audit exercise was thus initiated, and at the same time the KRA approach was adopted. A steering committee was formed, comprising the Director of Audit (chair), the Director of IS, the Director of the Computer Centre, and an Analyst. The team was assembled with the Analyst as the Project Manager, assisted by a Programmer and an operator. These steps correspond to *engagement definition* and *engagement planning* (Figure 4).

The team proceeded with the KRA procedures, and the process (simplified for illustration) started with a review of the Centre, its operating environment and its physical environment. Using face-to-face interviews and on-site observations, the team examined: (i) the *operating* environment – relevant reference documentation, users' guides, storage of data and software, personnel, etc, and (ii) the *physical* environment – the power supply, network facility, insurance policy, etc. Steps were taken to identify vulnerability of the Centre, to assess probabilities of occurrence, and to estimate possible damage (see Data Collected). These steps correspond to *internal control evaluation*. The data collected provided input for the *compliance test* and *substantive test*, and an update (for illustration purpose) of the DB (see Outcome Observed). These constituted the basic knowledge base for *attestation* (Figure 4).

(b) Data Collected

(1) A major fire in the computer room would result in costs for repair, re-equipment, and recovery, estimated at $40,000,000 but occur once in 100 years.

(2) A Programmer could write a small routine to operate on the payroll program to generate random duplicates of cheques for monthly-paid staff in the Programmer's bank account number. Such fraud could cost the bank $10,000 per year.

(3) The operator mistakenly executed an old version of a loan repayment update program. The system was not well documented and the original programmer left long ago. To rectify the mistake would need about half an hour of machine time which would cost about $100, plus interruption and inconvenience to other systems and the customers. This happened quite frequently.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission. www.ma

(4) An intermittent software error in the routine to calculate loan repayments could cause an estimated understatement of $10 on the average repayment.

(5) Loss of a detail file would result in a cost of $1,000 to recover, and the frequency of such a loss was once every 100 working days.

(6) Restarting a job that was aborted by an operator error would cost about $10 and such restarts could happen 12 times a day.

(c) Outcome Observed

(1) Risk discovery and identification: Assume that we choose a warm-start (WARM-START), and obtain a list of risk factors (which is provided through the database). Figure 7 shows the output.

Figure 7: List of Risk Factors (Warm Start)

```
HARDWARE
        FIRE
        AIR CONDITIONING
        WATER DAMAGE
        POWER LOSS
        EXPLOSIONS
        VANDALISM
        CIVIL DISORDER
        ACCIDENTAL ERASURE
        CPU FAILURE
        PERIPHERAL FAILURE
        TELECOM FAILURE
        MEDIA DAMAGE
SOFTWARE
        OS SOFTWARE
        SUPPORT SOFTWARE
        APPLICATION SOFTWARE
        DATA INTEGRITY
        PROGRAM ERROR
        INPUT ERROR
PERSONNEL
        OPERATOR ERROR
        PROGRAMMER ERROR
        MAINTENANCE ERROR
        USER ERROR
        MALICIOUS INTENT
        FRAUD
        ESPIONAGE
```

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission. www

Frequently, we are attracted by either a large or a small figure. In this case, on examining the list of risks presented, we were attracted to the $40,000,000 and the $10 (items 1 and 6 respectively, of Data Collected); also we thought it was a good idea to include an amount in between, so we picked the $1,000 in (item 5 of Data Collected). We refined the list using MODIFY (Figure 8), noting that the examination process was carried out iteratively.

Figure 8: Refined List After Having Applied MODIFY

```
HARDWARE
     FIRE

SOFTWARE
     DATA INTEGRITY
     PROGRAM ERROR

PERSONNEL
     OPERATOR ERROR
     OPERATOR ERROR
     MALICIOUS INTENT
```

(2) Measurement: A probability rating and a damage rating were assigned to each of the identified risks. When triggered off, ANALYSIS (Figure 9) assigned the probabilities and ASSESSMENT (Figure 10) assigned damaged values.

Figure 9: The Result of Having Applied ANALYSIS

```
RISK FACTORS                          PROBABILITY
     HARDWARE
          FIRE                            1
     SOFTWSRE
          DATA INTEGRITY                  4
          PROGRAM ERROR                   3
     PERSONNEL
          OPERATOR ERROR 1                6
          OPERATOR ERROR 2                7
          MALICIOUS INTENT                4

PROBABILITY CODE:
0     -    VIRTUALLY IMPOSSIBLE
1     -    ONCE IN 100 YEARS
2     -    ONCE in 10 YEARS
3     -    ONCE IN 5 YEARS
4     -    ONCE IN 100 DAYS
5     -    ONCE IN 10 DAYS
6     -    ONCE A DAY
7     -    10 TIMES A DAY
```

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission. www.ma

Figure 10: The Result of Having Applied ASSESSMENT

RISK FACTORS	PROBABILITY	DAMAGE
HARDWARE		
FIRE	1	6
SOFTWARE		
DATA INTEGRITY	4	3
PROGRAM ERROR	3	1
PERSONNEL		
OPERATOR ERROR 1	6	2
OPERATOR ERROR 2	7	1
MALICIOUS INTENT	4	4

PROBABILITY CODE:
0 - negligible
1 - about $10
2 - about $100
3 - about $1,000
4 - about $10,000
5 - about $100,000
6 - about $5,000,000
7 - about $100,000,000

These steps were followed by EXPOSURE (Figure 11) from which the Annual Loss Expectancy (ALE) was obtained.

Figure 11: The Result of Having Executed EXPOSURE

RISK FACTORS	PROBABILITY	DAMAGE	ALE($)
HARDWARE			
FIRE	1	6	2,500
SOFTWARE			
DATA INTEGRITY	4	3	2,500
PROGRAM ERROR	3	1	2.50
PERSONNEL			
OPERATOR ERROR 1	6	2	25,000
OPERATOR ERROR 2	7	1	25,000
MALICIOUS INTENT	4	4	25,000

RISK FACTORS	RANK
OPERATOR ERROR	1
MALICIOUS INTENT	1
FIRE	2
DATA INTEGRITY	2
PROGRAM ERROR	3

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission. www.

(3) Decision: A report was then requested. Based on the input to the KB the KRA provided its advice to the user (Figure 12).

Figure 12: The Result of Having Executed REPORT

```
THE ANALYSIS INDICATES THAT THE BANK SHOULD AUDIT
PERSONNEL (OPERATOR TRAINING, PROGRAMMER
INTEGRITY) RATHER THAN FIRE OR FILE PROTECTION.
```

Conclusion

Computer crimes are growing at an accelerated rate as computer applications proliferate. Information managers face a much more complex problem than in the past and auditors of computer-based information systems are in urgent need of new, innovative audit tools.

The KRA, a computer-based audit system into which are encapsulated the power of Risk Management and Expert Systems, is perceived to provide an innovative approach that can assist information managers and auditors. The model has been illustrated in this article through a simulated case study in the banking environment in Hong Kong. The outcome of the case study indicates that :

(1) The prototype is cyclic and iterative in practice. Depending on the circumstances, forward and backward tracking at each step of the prototype is possible.

(2) The computed result of the ALE, although quantitative, incorporates a qualitative element. This is demonstrated in the assignment of probabilities of occurrence and the assessment of damage where the auditor is under the subjective influences of personal preference, organisational history, and corporate culture.

(3) The simulated case exercise incorporates the risk management framework: endorsement by senior management, establishment of a steering committee, discovery/identification of the risk factors (vulnerabilities that caused audit attention), computation of ALE using estimated probabilities of damage, and associated management report.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission. www.ma

The quality assurance of the prototype has yet to be ascertained. However, when fully constructed, a dynamic KRA will have to undergo an expert systems evaluation (O' Leary, 1987). It is envisaged that the system will then be able to react to other scenarios – that is, in organisational areas other than the computer centre and in industries other than banks. The prototype can also be extended to include a self-learning element, to accumulate real experience, and deductive reasoning capability.

References

AICPA (American Institute of Certified Public Accountants), "The auditor's consideration of an entity's ability to continue as a going concern", statements on auditing standards, No 59, 1988.

Andersen R E, "EDP auditing in the 1980's or the vanishing paper trail", *Security Audit and Control Review*, 1 (1), pp 6-15, 1982.

Anderson R G, *Information & Knowledge-based Systems: An Introduction*, Prentice-Hall, 1992.

Ansell J and Wharton F (eds), *Risk: Analysis, Assessment, Management*, Wiley, (1992).

Arens A A and Loebbecke J K, *Auditing: An Integrated Approach (6th ed)*, Prentice-Hall, 1994.

Australian Public Service Board, *Risk Management in Automatic Data Processing*, Government Publishing Service, Canberra, 1981.

Bailey Jr A D, Duke G L, Gerlach J, Ko Chen-en, Meservy R D and Whinston A B, "TICOM and the analysis of internal controls", *The Accounting Review*, LX(2), pp 186-201, 1985.

Bariff M L, "Increasing responsibility and professionalism for EDP auditing in the 1980's", *Security Audit and Control Review*, 1(1), pp 16-19, 25, 1982.

Blanton J E and Rosenberger J, "Determining your information system's vulnerability to viruses", *Journal of Systems Management*, pp 10-12, 24-27, May 1991.

Bobrow D G, Mittal S and Stefik M, "Expert systems: perils and promise", *Communications of the ACM*, 29 (9), pp 880-894, September 1986.

Bock D B and Schrage J F, "Computer viruses: over 300 threats to micro-computing ... and still growing", *Journal of Systems Management*, pp 8-13, February 1993.

Boehm B W, *Software Risk Management*, IEEE Computer Society Press, 1989.

Buchanan B G and Duda R O, "Principles of rules-based expert systems", *Advances in Computers*, 22, pp 163-216, 1983.

Campbell R P and Sands G A, "A modular approach to computer security risk management", Proceedings of National Computer Conference, pp 293-303, 1979.

Cash Jr J I, Bailey Jr A D and Whinston A B, "A survey of techniques for auditing EDP-based accounting information systems", *The Accounting Review*, LII (4), pp 813-832, 1977.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission. www

Cerullo M J and Corless J C, "Auditing computer systems", *The CPA Journal*, LIV(7), pp 18-33, 1984.

Chen W and Lee W W, "EDP auditing in China", Proceedings of EDPAA 5th Annual Asia Pacific Conference on Information Systems Control, Hong Kong, August 1989.

Chu G T, "Expert systems in computer based auditing", *The EDP Auditor Journal*, Vol. 1, pp 25-33, 1989.

Courtney R H, "Computer security risk assessment", Proceedings of the Conference on Computer Security and the Data Encription Standard, Maryland, pp 15-17, 15 February 1977.

Cox I J, "Expert systems", *Electronics & Power*, pp 237-240, March 1984.

Davis G B and Weber R, "The impact of advanced computer systems on controls and audit procedures: a theory and an empirical test", *Auditing: A Journal of Practice and Theory*, 5(2), pp 35-49, 1986.

Debenham J K, *Knowledge Systems Design*, Prentice-Hall, 1989.

Dillard J F and Mutchler J F, "A knowledge-based system for audit opinion decisions: A project report", Ohio State University, 1986.

Dorfman M S, *Introduction to Risk Management and Insurance* (4th ed), Prentice-Hall, 1991.

Dungan W and Chandler J S, "Auditor: A microcomputer-based expert system to support auditors in the field", *Expert Systems*, 2(4), pp 210-221, 1985.

Forcht K A, *Computer Security Management*, Boyd and Fraser, 1994.

Forsyth A (ed), *Expert Systems: Principles and Case Studies*, Chapman and Hall, 1984.

Gal G F, "Using auditor knowledge to formulate data model constraints: An expert system for internal control evaluation", PhD dissertation, Dept of Accounting, Michigan State University, 1985.

Garner B J and Pinnis J, "Modelling as an auditing technique", *The Australian Computer Journal*, 16(2), pp 48-53, 1984.

Gilmore J F and Howard C, "Expert system tools for practitioners", Proceedings of the First Australian Artificial Intelligence Conference, Melbourne, November 1986.

Gonzalez A J and Dankel D D, *The Engineering of Knowledge-based systems: Theory and Practice*, Prentice-Hall, 1993.

Grobstein M and Craig P W, "A risk analysis approach to auditing", *Auditing: A Journal of Practice and Theory*, 3(2), pp 1-16, 1984.

Grobstein M, Leob S E, and Neary R D, *Auditing: A Risk Analysis Approach*, Irwin, 1985.

Hafner K and Markoff J, *Cyberpunk: Outlaws and Hackers on the Computer Frontier*, Simon and Schuster, 1991.

Hansen J V and Messier Jr W F, "Expert systems for decision support in EDP auditing", *International Journal of Computer and Information Sciences*, 11(5), pp 357-379, 1982.

Hansen J V and Messier Jr W F, "A preliminary test of EDP-XPERT", ARC Working Paper 85-5, University of Florida, 1985.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission. www.ma

Hayes-Roth F, Waterman D A and Lenat D B (eds), *Building Expert Systems*, Addison-Wesley, 1983.

Hayes-Roth F, "The knowledge-based expert system: a tutorial", *IEEE Computer*, 17(9), pp 11-28, September 1984.

Hertz D B, "Risk analysis in capital investment", *Harvard Business Review*, 42, pp 95-106, 1964.

Heuer S, Koch U and Cryer C, "INVEST: An expert system for financial investment", in Andriole, S J and Hopple, G W (eds), *Applied Artificial Intelligence: A Sourcebook*, McGraw-Hill, pp 368-377, 1992.

Jancura E G and Beger A H, "Auditing EDP - by computer", in Jancura E G and Berger A H (eds), *Computer: Auditing and Control*, Auerback, p 329, 1973.

Johnson T and Khan R A, "Risk management - A tool for financial analysis", *The Accountant*, 46, pp 8-10, 13-15, January/February, 1976.

Keyes J, "The Citibank pension expert", in Andriole SJ and Hopple G W (eds), *Applied Artificial Intelligence: A Sourcebook*, McGraw-Hill, pp 363-367, 1992.

Lee W W, "Risk management of computer-based information systems", MBA dissertation, Australian Graduate School of Management, University of New South Wales, 1980.

Lee W W, "The case for data protection", *Business News*, SCM Post, 19 September 1983a (press interview).

Lee W W, "Risks, control and audit of computer-based information systems", *The Hong Kong Computer Society Year Book*, pp 71-76, 1983b.

Lee W W, "Computer laws", *Sing Tao Zao Po*, 15 September 1984a (press interview).

Lee W W, "Risk and risk management of computerisation", Proceedings of the International Computer Symposium, Taipei, pp 1355-1361, 1984b.

Lee W W, "Legislation is needed to deal with computer crimes", *Wah Kui Yat Po*, 30 October 1985a (press interview).

Lee W W, "Design of man-machine decision systems: An approach to risk management", Proceedings of the First Pan Pacific Computer Conference, Melbourne, pp 1310-1324, September 1985b.

Lee W W, "Knowledge-based audit: Expert systems for internal control evaluation", Proceedings of the First Australian Artificial Intelligence Congress, Melbourne, November 1986.

Lee W W, " Automation of internal control evaluation", in Caelli WJ (ed), *Computer Security in the Age of Information*, Elsevier Science Publishers, pp 391-406, 1988.

Lee W W, Construction of a knowledge-based risk analysis model, a R&D project funded by a Lingnan Research Grant, 1994.

Lee W W, "Knowledge-based risk-analytic audit: A conceptual framework for a deterrent to computer crime", an integrated paper presented to the DBA programme, Henely Management College, UK, January 1995.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission. www.m

Loch K D, Carr H H and Warkentin M E, "Threats to information systems: today's reality, yesterday's understanding", *MIS Quarterly*, pp 137-186, June 1992.

Luconi F L, Malone T W and Scott Morton M S, "Expert systems: The next challenge for managers", *Sloan Management Review*, pp 3-14, Summer 1986.

Mastromano F M, "The changing nature of the EDP audit", *Management Accounting*, pp 27-34, July 1980.

McDermatt J, "R1: The formative years", *AI Magazine*, 2(2), 1981.

Mertan A G and Severance D G, "Executive management's perspective on information systems control", in Wyson Jr E M and de Lotto I (eds), *Information Systems Auditing*, Elsevier Science Publishers, pp 1-14, 1983.

Meservy R D, "Auditing internal control: A computational model of the review process", PhD dissertation, University of Minnesota, 1985.

Michaelsen R H, "A knowledge-based system for individual income and tax planning", PhD dissertation (in Accountancy), University of Illinois at Urbana, 1982.

Michie D, "Expert systems", *The Computer Journal*, 23 (4), pp 369-376, 1980.

Milko E M, "Auditing: Through the computer or around?" in Jancura E G and Berger A H (eds), *Computers: Auditing and Control*, Auerback, pp 299-308, 1973.

Mykytyn K, Mykytyn Jr P P and Slinkman C W, "Expert systems: A question of liability?", *MIS Quarterly*, pp 27-42, March 1990.

Munter P and Ratcliffe T A, "Impact of computer processing on financial audits", *The CPA Journal*, LV(1), pp 34-38, 1985.

Neumann P G, *Computer Related Risks*, Addison-Wesley, 1995.

Nissenbaum H, "Computing and accountability", *Communications of the ACM*, 37(1), pp 72-80, January 1994.

O'Leary D E, "Validation of expert systems – with applications to auditing and accounting expert systems", *Decision Science*, 18, pp 468-486, 1987.

Parker D B and Nycum S, "The new criminal", *Datamation*, pp 56-57, January 1974.

Parker D B, "Human factor controls for information security", in Fak VA (ed), *Security*, IFIP/Sec '83, pp 247-252, 1983.

Perry A E, "EFT and risk management", *Computer and Security*, ACM/SIGCS, 12(3), pp 2-5, 1982.

Pfleeger C P, *Security in Computing*, Prentice-Hall, 1989.

Rainer Jr R K, Snyder C A and Carr H H, "Risk analysis for information technology", *Journal of Management Information Systems*, 8(1), pp 129-147, 1991.

Rich E and Knight K, *Artificial Intelligence* (2nd ed), McGraw-Hill, 1991.

Riley J, "Computer fraud on increase", *Technology Post*, *South China Morning Post*, 9 November 1993.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission. www.m

Ross S J, "Risk management and data security - partners in the computer age", *Risk Management*, pp 28-32, August 1979.

Sendrow M, "Impact of rapidly changing computer technology on computer crime", *Security Audit and Control Review*, ACM, 1(2), pp 8-16, 1982.

Sherer S A, *Software Failure Risk: Measurement and Management*, Plenum Press, 1982.

Shortliffe E H, *Computer-based Medical Consultation: MYCIN*, American-Elsevier, 1975.

Sieber U, *The International Handbook on Computer Crime: Computer-related Economic Crime and the Infringement of Privacy*, Wiley, 1986.

Smith H F, "Privacy policies and practices: Inside the organisational maze", *Communications of the ACM*, 36(12), pp 105-122, December 1993.

Socha W J, "Problems in auditing expert system development", *The EDP Audit, Control and Security Newsletter*, March 1988.

Spetzler C S, "The development of a corporate risk policy for capital investment decisions", *Transactions on Systems Science and Cybernetics*, SSC-4, IEEE, pp 279-300, 1968.

Steele A, *Audit Risk and Audit Evidence*, Academic Press, 1992.

Steinbart P J, "The construction of an expert system to materiality judgements", PhD dissertation, Dept of Accountancy, Michigan State University, 1984.

Stettler H F, *Stettler's Systems Based Audit*, Prentice-Hall, 1981.

USDC/NBS (US Dept of Commerce/National Bureau of Standards), "Guidelines for automatic data processing risk analysis", Federal Information Processing Standard Publication 65, Government Printing Office, Washington, DC, 1979.

Varsarhelyi M A, "Automation and changes in the audit process", Research Working Paper No. 532A, Columbia University, 1984.

Varsarhelyi M A, "Audit automation: On-line technology and auditing", *The CPA Journal*, LV(4), pp 10-17, April 1985.

Warren C S, "Audit risk", *The Journal of Accountancy*, pp 66-74, August 1979.

Waterman D A, *A Guide to Expert Systems*, Addison-Wesley, 1986.

Watne D A and Turney P B B, *Auditing EDP Systems* (2nd ed), Prentice-Hall, 1990.

Weber R, *EDP Auditing* (2nd ed), McGraw-Hill, 1988.

Weiss, H, "Computer security: An overview", *Datamation*, pp 42-47, 1974.

Weiss S M and Kulikowski C A, *A Practical Guide to Designing Expert Systems*, Chapman and Hall, 1984.

Williams Jr C A and Heins R M, *Risk Management and Insurance* (6th ed), McGraw-Hill, 1989.

Yager R R, "Explanatory models in expert systems", *International Journal of Man-machine Studies*, 23, pp 539-549, 1985.

Yazandi M (ed), *Artificial Intelligence: Principles and Applications*, Chapman and Hall, 1985.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission. www.