The current issue and full text archive of this journal is available at
www.emeraldinsight.com/1741-0398.htm

Mastering the art of corroboration

A conceptual analysis of information assurance and corporate strategy alignment

Jean-Noël Ezingeard, Elspeth McFadzean and David Birchall
Centre for Business in the Digital Economy, Henley Management College, Henley-on-Thames, UK

Abstract

Purpose – The paper seeks to investigate how the information assurance (IA) efforts of organisations should be aligned with their business strategy. From this analysis, a conceptual model of alignment is presented. This framework shows several organisational factors that can influence alignment.

Design/methodology/approach – A number of published works on alignment are discussed in order to develop a conceptual model of IA fit. In addition, Venkatraman's six perspectives of alignment are used as a framework to suggest future research in this area.

Findings – The paper presents a definition of information assurance and proposes various reasons why IA is a strategic issue and should be aligned with both IT and corporate strategy. From the literature, a conceptual model illustrating the variables that can influence alignment is presented.

Research limitations/implications – A clear conceptualisation of alignment is needed. Six potential research models and associated research questions are proposed.

Practical implications – The paper concludes with a number of management and research implications. In looking at the implications for managers, it is argued that any alignment framework should include adequate metrics for checking the strategic fit on a continuous basis.

Originality/value – This paper is an initial attempt to fulfil an identified gap in the literature, namely the lack of research undertaken on IA and corporate strategy alignment. It offers practical help for management so that they can improve the fit between IA and business strategy. It also offers several avenues of potential future research using Venkatraman's six perspectives of fit.

Keywords Information control, Strategic alignment, Corporate strategy, Data security

Paper type Conceptual paper

Introduction

Today, many organisations are realising that information is one of their most valuable assets (Armstrong *et al.*, 2002). As businesses become increasingly reliant on their information, the responsibility for protecting what is now often referred to as information assets becomes more important (Austin and Darby, 2003; Dutta and McCrohan, 2002). This growing awareness is driving greater thought about the role of information guardians within organisations. The broadening of this responsibility is the reason why information assurance (IA) seems to be emerging as the preferred terminology for the range of activities involved in the role. IA is not just about protecting the systems that carry information, but also requires consideration of the information content itself. Information assets are at least as important to success as physical assets. Indeed, Kovacich (2001) suggests that the roles of the corporate security officer and the information systems security officer should merge to create a new senior position called the Corporate Information Assurance Officer. His or her role would be to "develop, implement, maintain, manage and administer a corporate-wide

Journal of Enterprise Information Management
Vol. 20 No. 1, 2007
pp. 96-118

1741-0398
DOI 10.1108/17410390710717165

information assurance programme to include all plans, policies, procedures, processes, assessments and authorisations" (Kovacich, 2001, p. 303).

The growing responsibility for ensuring information plays its part in corporate success, however, is not always being matched by an increased strategic approach to IA. In many organisations there is a lack of alignment between information assurance policies and corporate strategy (Deloitte Touche Tohmatsu, 2003). Board members and information systems specialists lack a common understanding, resulting in limited dialogue and inadequate definitions of what comprises successful performance for information assurance issues (Birchall *et al.*, 2003).

This paper examines the key areas of information assurance and presents a conceptual model illustrating how IA strategy can be aligned with corporate strategy. The first two sections will discuss the importance of information assurance to organisations and the value of aligning IA policies with corporate strategy. From these two sections, it can be concluded that establishing and measuring the extent of alignment between organisational strategy and information assurance policies should be an urgent priority for many organisations. This leads us to a new conceptual model of IA alignment. Lastly, we present some implications for managers and researchers derived from the analysis.

Why information assurance is strategic

Defining information assurance

Unfortunately, there is no universally accepted definition of what constitutes information assurance as a distinct entity from information security. The term is growing in acceptance and usage, notably amongst an increasing number of government and international agencies (Wolf, 2003). Information security generally includes the following three elements (Whitman, 2004):

(1) *confidentiality* – ensuring information is accessible on a need-to-know basis and unauthorised access is prevented;

(2) *integrity* – data are not deleted or corrupted either accidentally or deliberately; and

(3) *availability* – ensuring that information is available when it is required and that it is able to support the organisation's ability to operate and accomplish its objectives.

Landwehr (2001) and Koved *et al.* (2001) add identification and authentication to this list. The distinction emphasises a necessary separation between the acts of recording who has carried out an interaction with an information asset from the acts of determining their authority to do so. Separating these concepts in information architecture can identify instances of password security breaches. A further component is non-repudiation, introduced as far back as 1989 (International Organization for Standardization, 1989). Defined as a basic security service, non-repudiation ensures organisations can prove that transactions actually took place and that they were correctly recorded (Wright, 2001). This expanded scope of the activity associated with managing the defence, preservation, provenance and surety of information now forms the basis of the definition of IA used in many countries. For instance, in the UK, the Information Assurance Advisory Council (2003, p. 11) defines IA as[1]:

> . . . the certainty that the information within an organisation is reliable, secure and private. IA encompasses both the accuracy of the information and its protection, and includes disciplines such as security management, risk management and business continuity management.

The IAAC uses the terms "reliability", "security" and "privacy" because they suggest that although information security professionals may use terms such as "availability", "integrity", "authentication", "confidentiality" and "non-repudiation", these terms mean very little to directors and senior managers.

Despite this widening of scope, information assurance is still frequently used as a synonym for security, where little is added to the mindset of defence (Boyce and Jennings, 2002). However, it can be argued that those responsible for implementing information security can make a greater contribution to the organisation through a changing perspective, which focuses on enhancing competitive advantage rather than simply defending existing systems (Dhillon, 2004).

Security considerations typically focus on the need to protect systems from internal and external attack, environmental threats and accidental damage (Whitman, 2004). This is undoubtedly a core element of information assurance, but can lead to a "fixed state" approach, predicated on the (dangerous) assumption that all threats can be accurately predicted. Strengthening systems to meet the security needs of today can create a rigidity that reduces the flexibility to adapt quickly. System changes may even be seen as a temporary transition between static states, breeding a tolerance of a reduced state of security during a transition period.

Information assurance could be said to represent a migration from a *preventative* approach to an *enabling* approach. Information systems can represent a source of competitive advantage through their structural integrity as much as through the information content they deliver (Keng, 2003). The reliability and resilience of systems can enable more consistent operational and customer service performance, thus reducing costs and increasing the ability to adapt quickly to changing market circumstances. Table I compares the key elements of a traditional information security method to a more pioneering information assurance approach.

A comprehensive vision for information assurance ensures that the information systems serve the organisation's transactional needs – such as operational capability, customer service and financial systems – as well as its transformational needs including knowledge management, innovation and rapid adaptation.

Taking such a forward-looking view requires an examination of the business's direction as well as its current needs and systems. Information assurance practitioners must understand how the value is created in the business and what will influence future strategic decisions (Ezingeard *et al.*, 2003).

Consequently, combining all these ideals, information assurance strategy can be defined as:

> The reliability, accuracy, security and availability of a company's information assets. This will typically define how these assets – data and/or information both within the tangible and the virtual bounds of the organisation – should be secured to provide maximum benefit. This should be developed and aligned with corporate strategy.

	Information security	Information assurance
Confidentiality	Need-to-know only and protection from unauthorised access	How can ongoing compliance be ensured against regulatory changes or regional variations? What would be the impact on reputation of a breach in confidentiality?
Integrity	Preventing accidental or malicious alteration, corruption or deletion	Can users compare relative levels of reliability if data are conflicting? How does the organisation reduce costs incurred through errors?
Availability	Disaster recovery and business continuity to ensure ongoing operation of existing systems	How can we develop systems that will not be restrictive as the organisation grows, enters new alliances or develops new businesses?
Identification and authentication	Password access control	Do users keep their passwords secret and regularly changed because they are told to or because they understand the importance of password safety? How can we develop better identification and authentication methods for our stakeholders?
Non-repudiation	Fraud prevention	How can security reduce the organisation's transaction costs? Can transactions be simplified for our customers to increase their value gained from dealing with us, without compromising security?

Table I.
Comparing information security with information assurance

Information assurance as a strategic imperative

Breaches in security heighten awareness of just how dependent organisations have become on their information systems – and how high the price for failing to safeguard them is in terms of reputation damage, loss of business and valuation loss on stock markets (Ettredge and Richardson, 2002). It is vital, therefore, that organisations develop an effective information assurance strategy to help them defend against these violations. Despite these dangers, information assurance is not a prime shaper of corporate strategy. Companies do not establish revenue generation plans and budgets after considering information assurance policies (with the few exceptions of those whose primary business is secure transmission or storage of information). Nonetheless, information assurance is a strategic issue – in the sense defined by McFarlan (1984) and Ward (1988) of potential impact on the rest of the business – and should support corporate strategy because the consequences of IA strategy decisions can affect the entire business. For instance, an information system's failure could cause damage to an organisation's reputation and may inhibit the firm's ability to operate. In addition, ill-considered policies may also restrict information flow, causing poor customer service and resulting in loss of business over time. Finally, the cost of the incident may

be prohibitively high and the organisation may not survive the disruption (Logan and Logan, 2003). The results of poor information assurance are summarised in Table II.

There is also a decreasing tolerance by customers for publicised security breaches (Department of Trade and Industry, 2004; Treanor, 2000). Hence, Dutta and McCrohan (2002) strongly suggest information security concerns should rise to the highest levels of the organisation. If customers migrate because of the inconvenience or risk of failing computer systems, stability and reliability become competitive drivers. The advent in the USA of the Sarbanes-Oxley Act, which holds executives personally liable for the accuracy of financial results, could potentially pave the way to similar liability for all compliance issues – particularly in the light of growing consumer concern for information privacy (Culnan and Armstrong, 1999; Swartz, 2003; Tweney, 1998).

In addition to information assurance being important strategically because of its potential impact on the rest of the business, IA is linked to corporate governance making it *de facto* a strategic issue. Research has shown that there is a strong correlation between companies that admit to breaches occurring within their confidential information systems and a reduction in their stock market price (Campbell *et al.*, 2003; Ettredge and Richardson, 2003). Thus, information assurance must become a concern from a corporate governance perspective (Ezingeard and Birchall, 2004; National Association of Corporate Directors, 2001; Von Solms, 2001). A number of government reports have been produced over the past decade to encourage boards to ensure that adequate control mechanisms are put in place within their organisations in order to reduce or promote a better understanding of financial risk (for example, the Sarbanes-Oxley Act in the USA, the Higgs report in the UK, the King report in South Africa, le Rapport Bouton in France). Whereas security was once the sole domain of the IS department, organisations are increasingly tasking audit and compliance committees with monitoring and overseeing IA processes. Parker (2001) suggests that auditors should "fully understand" information assurance issues as a key part of future responsibility. Information assurance and corporate governance are therefore becoming increasingly linked (IT Governance Institute, 2003).

So far we have shown that information assurance can be construed as a "strategic" issue for many organisations. IA decisions will therefore have an impact on business strategy development or its execution. However, despite increasing acknowledgement of IA as a strategic imperative, decisions about information assurance may reside at a

Consequences	Theorists
Loss of value on stock markets	Campbell *et al.* (2003), Ettredge and Richardson (2002, 2003)
Reduction in reputation	Birchall *et al.* (2003)
Inhibits the firm's ability to operate	Logan and Logan (2003)
Restricts information flow causing poor customer service	Birchall *et al.* (2003)
Cost of a security breach can prove to be prohibitively high	Logan and Logan (2003), Sauer *et al.* (1997)
Increases decline in tolerance by customers for publicised security breaches	Department of Trade and Industry (2004), Treanor (2000)
Poor IA compliance can lead to legal problems such as privacy and data protection	Culnan and Armstrong (1999), Tweney (1998), Swartz (2003)

Table II.
The consequences of poor information assurance

tactical level within the organisation. In 2003, over a third of organisations surveyed by Ernst & Young said that their information assurance spending could be better aligned with their corporate strategy (Ernst & Young, 2003). Furthermore, management decisions about information assurance are often reactive, confirming the lack of a strategic approach (Ezingeard *et al.*, 2004). This potentially makes the alignment between IA strategy and business strategy difficult. In order to examine how this may be the case, the next section discusses the concept of strategic alignment.

The concept of strategic alignment

The importance of strategic alignment

The notion of strategic alignment is crucial in many other areas of business. The idea has been discussed in the field of IS (Henderson and Venkatraman, 1993), operations and supply chain management (e.g. Evans and Danks, 1998) and marketing (e.g. Kotler *et al.*, 2001). It has its origins in the concept of strategic fit, popularised by Tom Peters in the 1980s, who argued that congruence among seven elements – strategy, structure, systems, style, staff, shared values and skills – is necessary for success (Peters and Waterman, 1982). The idea is linked to Miller's view that it was how the "whole" was organised that leads to success (Miller, 1981) – a school of thinking later called the Configuration School (Miller, 1987). Strategic fit is therefore important, because it leads to superior performance (Gietzmann and Selby, 1994).

Defining fit is difficult, however, because fit is not only about knowing what needs to be aligned but also how the alignment should be achieved. This led Venkatraman and Camillus (1984) to define fit as *process* (how to achieve fit) and *content* (what fit looks like). Later, Venkatraman (1989) argued that it was necessary for researchers to define clearly what they mean by fit, proposing six perspectives – moderation, mediation, matching, gestalts, deviation and covariation.

The conceptualisation of fit and alignment used in recent studies in the IS field take different forms, but most confirm that alignment is important to business success (Bergeron *et al.*, 2004) and IT success (Sabherwal and Kirs, 1994) (see Table III). For instance, using a moderation and a matching model, Chan *et al.* (1997) demonstrate a link between the alignment of IS strategy and business strategy to be a component of business performance. The same research also discovered that alignment between IS strategy and business strategy was a better indicator of business performance than IS strategic orientation itself – implying that "best practice" applied indiscriminately of business needs is not automatically beneficial to results. Henderson and Venkatraman (1993) take an approach akin to a Gestalt view of alignment by arguing that the configuration of four fundamental domains – business strategy, organisational infrastructure, IT strategy and IT infrastructure – can lead to business success. Other studies, taking an approach akin to Venkatraman's "matching" have proven that lack of alignment could result in significant (and costly) failures (Sauer *et al.*, 1997). Not all studies confirm that alignment is an antecedent of superior performance in all business environments, however, and Sabherwal and Chan (2001) showed – using a deviation conceptualisation of alignment – that alignment was not significant in organisations operating in stable, predictable, niche environments.

Clearly, the amount of coverage dedicated to alignment in the IS literature indicates that it is an area regarded as important by researchers; but alignment is also a priority concern for practitioners. The topic is always prominent in surveys of IS "issues"

Research	Type of fit	Findings
Bergeron and Raymond (1995)	Mediation and moderation	Alignment between the strategic orientation of IT management and business strategy found to have a positive effect on business performance
Bergeron *et al.* (2004)	Gestalts	Conflicting co-alignment patterns between business strategy, business structure, IT strategy and IT structure were found in low-performing firms
Chan *et al.* (1997)	Moderation and matching	Fit between IS strategy and business strategy found to be a function of business performance Alignment between IS strategy and business strategy found to be a better indicator of business performance than IS strategic orientation itself
Croteau *et al.* (2001)	Covariation	The fit between organisational and IT infrastructures was found to be a positive influence on performance
Henderson and Venkatraman (1993)	Gestalts	The configuration of four fundamental domains – business strategy, organisational infrastructure, IT strategy and IT infrastructure – was found to improve business success
Palmer and Markus (2000)	Matching	No relationship found between the alignment of corporate and IT strategy and business performance
Sabherwal and Chan (2001)	Deviation	Alignment was found to be insignificant for organisations operating in stable, predictable, niche environments
Sauer (1997)	Matching	Lack of alignment was found to create significant (and costly) failures. It was determined that lack of fit encourages conflicting motivations and uncertainty and inhibits the development of better alternatives, which can cause an increase in failures
Teo and King (1996)	Mediation	The alignment of corporate strategy and IT strategy had a positive influence on business performance

Table III.
Previous research into alignment and business performance

around the world for CIOs (Gottschalk, 2000; Lai, 2001), although the issue seems less important for CEOs (Pervan, 1998), who may not be aware of the degree of deviance between strategic intent and operational practice within their organisation.

How alignment can be achieved

If alignment is important, what, then, will ensure that alignment is achieved? According to Reich and Benbasat (1996), two aspects need to be considered. Firstly the strategic planning process itself (how IT and IS strategies are put together, and how they influence business strategy) needs to be considered. Secondly, social relationships in the organisation need to be examined.

When investigating the IS strategic planning process, most authors contend that a multi-perspective view should be taken. For instance, Earl (1995) argues for a separate examination of IS strategy, IT strategy and information management (IM) strategy. A similar call is made by Henderson and Venkatraman (1993) in their strategic alignment model to distinguish between developing a strategy for the IT domain and one for the IS domain. Alignment has also been shown to be a positive feedback process, where

greater benefits are achieved if IS strategy is influenced by business strategy on one hand, but also if business strategy is influenced by IS strategy on the other hand (Teo and King, 1996). Moreover, Birchall *et al.* (2004) suggest that other stakeholders' views should be considered. For instance, their research found one financial institution that was prepared to accept the cost of a small percentage of fraud rather than investing large sums of money to eliminate all fraud as well as the possibility of alienating customers due to stringent security controls.

The need for IS strategy to influence business strategy can be linked to the idea that the alignment process is a continuous one. It needs to ensure that fit is maintained over time and should be capable of reacting to changes in the environment (Burn, 1996). In order for this to happen, many experts recommend that regular reviews of IS performance should be conducted (Chan, 2002). This points to the need for metrics. Such metrics, as well as auditing and reporting procedures, may also be helpful to ensure board focus (Hodges, 2002). In addition, Birchall *et al.* (2003) suggest that continuous alignment can be developed by discussing, resolving and reviewing the tensions that can occur between corporate and information assurance procedures. This may involve trade-offs being made between the two groups. For instance, corporate goals may demand the necessity for information sharing and creativity whilst the information assurance strategy stipulates tight control over information access. Thus, these types of tensions need to be resolved in order to improve alignment.

Alignment is also a social process. Consequently, good communication between line-of-business and IT executives is often quoted as necessary for alignment to be achieved (Chandler-Wilde and McFadzean, 2004; Reich and Benbasat, 1996, 2000). Moreover, alignment is thought to be easier to achieve if line executives have a good knowledge of IT (Hussin *et al.*, 2002), though this is obviously not always a practicable accomplishment. Alignment can also be enhanced if senior managers are generally committed to IT projects or if the IT function is given high visibility, such as when the CIO reports directly to the CEO of the organisation, or if an exchange is maintained between IT and the business via informal structures, close working relationships and mutual respect (Chan, 2002; Chandler-Wilde and McFadzean, 2004). A summary of these elements is shown in Table IV.

A conceptual model showing the above factors is presented in Figure 1. This framework illustrates the hierarchical process of corporate and information assurance strategy ranging from a top-level vision to metrics and benchmarking at the functional levels. In addition, the model suggests that a continuous information assurance alignment processes can be greatly enhanced by:

- resolving strategic tensions by dealing with the trade-offs;
- undertaking a multi-perspective strategic planning process;
- communicating using both formal and informal procedures;
- understanding the requirements of each group and valuing their projects; and
- recognising continuous change

The success of corporate and information assurance strategy can also be enhanced by educating and informing staff of changes in strategy. Furthermore, explicit roles and responsibilities regarding information assurance procedures should be allocated to all employees. This is important because, as Birchall *et al.* (2004, p. 47) suggest, "by

Analyse the strategic planning process and investigate how the IT and IS strategies are put together and how they influence business strategy	Reich and Benbasat (1996)
Examine IS strategy, IT strategy and Information Management (IM) strategy separately	Earl (1995), Henderson and Venkatraman (1993)
Ensure that the alignment is maintained over time and that it is capable of reacting to changes in the environment	Burn (1996)
Develop appropriate metrics and regularly review IS performance	Chan (2002), Hodges (2002)
Improve communication and reporting routes between line-of-business managers, IT executives and the board	Chandler-Wilde and McFadzean (2004), Reich and Benbasat (1996, 2000)
Enhance line executives' knowledge of IT	Hussin *et al.* (2002)
Encourage senior managers' commitment towards IT projects and/or provide the IT function with high visibility by allowing the CIO to report directly to the CEO and/or maintain effective collaboration between IT and the business via informal structures, close working relationships and mutual respect	Chandler-Wilde and McFadzean (2004), Chan (2002)

Table IV.
Achieving alignment

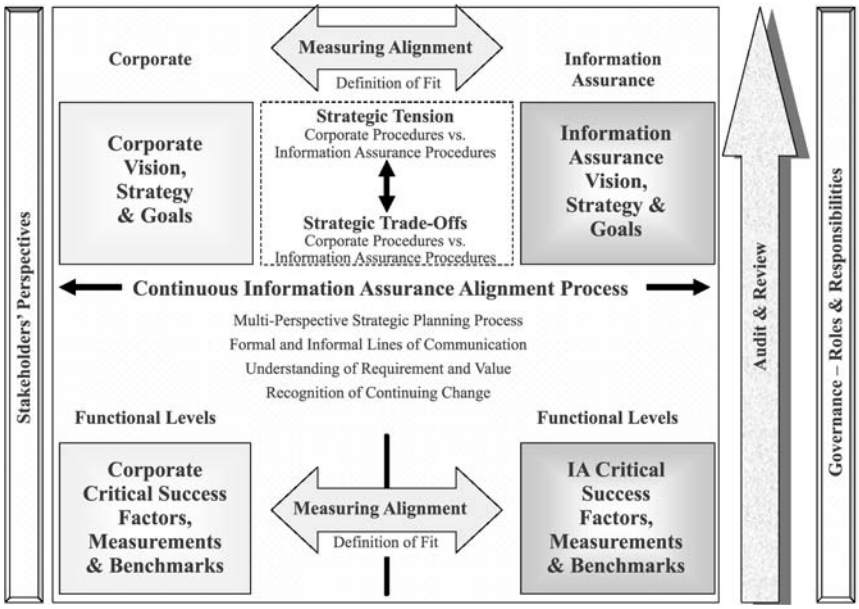


Figure 1.
A conceptual model of IA alignment

assigning responsibility to an individual or group to manage all relevant inputs and decide on appropriate action, the board is showing that these representatives are empowered to act".

There has been little research on the measurement of IA alignment to corporate strategy. However, theorists have posited a number of methods for measuring alignment between other functional areas and business strategy (Chan, 2002; Kaplan,

2002; Safizadeh *et al.*, 1996). Venkatraman (1989, p. 423) suggests, "Although it is common for theorists to postulate relationships using phrases and words such as matched with, contingent upon, consistent with, fit, congruence, and co-alignment, precise guidelines for translating these verbal statements to the analytical level are seldom provided". He therefore proposed six different perspectives of fit that have subsequently been used by other theorists to measure alignment (see Table V).

Hoffman *et al.* (1992) favoured the moderation model after they compared this alternative perspective with matching. They found that the former was much less ambiguous and more widely applicable than the latter. Chan *et al.* (1997) also found that their results supported moderation rather than matching. On the other hand, Bergeron *et al.* (2001) compared all six perspectives in their study of alignment on IT management, the organisational environment, strategy and structure and their impact on performance. They found that the mediation and covariation methods showed that the strength of the strategy-technology alignment influenced performance. Likewise, the moderation and matching approaches confirmed the same for the structure-technology pair. They also determined that "both the profile deviation and gestalts perspectives confirm the existence of specific configurations of strategic IT management, strategic orientation, structural complexity, and environmental

Alternative perspectives	Definition of fit	Potential methods for measuring fit	Theorists
Moderation	How a combination of variables affect performance	Multiple regression Multiplying business and IT strategy ratings	Hoffman *et al.* (1992), Hussin *et al.* (2002)
Mediation	How a combination of one variable plus and intervening mechanism indirectly affects performance	Regression analysis	Birkinshaw and Gibson (2004)
Matching	How a conjectured convergence or divergence in a structure/context fit affects performance	Deviation score model Residual approach Configurational theory	Hoffman *et al.* (1992), Sauer *et al.* (1997)
Gestalt	How the coherence between a set of variables affects performance	Balanced scorecard Assessment through indicators Rating alignment categories	Kaplan and Norton (2004a, b), Keeble *et al.* (2003), Luftman (2003a, b), Sledgianowski and Luftman (2005)
Covariation	How the consistency within a set of interdependent variables affects performance	Confirmatory factor analysis Model fit measures	Segars and Grover (1998), Beal (2000)
Deviation	How the degree of deviation from a specific profile affects performance	Euclidean distance between actual strategy attributes and ideal strategy attributes	Sabherwal and Chan (2001)

Table V.
Venkatraman's (1989) alternative perspectives of fit

uncertainty that are more effective than others" (Bergeron *et al.*, 2001, p. 137). In fact, Bergeron *et al.* (2004) suggest that the Gestalt perspective is useful for describing, predicting and explaining the performance of IT.

In their *Dictionary of the Social Sciences*, Gould and Kolb (1964) have defined Gestalt as "an organized entity or whole in which the parts, though distinguishable, are independent; they have certain characteristics produced by their inclusion in the whole, and the whole has some characteristics belonging to none of the parts". A number of theorists have developed alignment measures based on the Gestalt approach. For example, Luftman (2003a, b) developed the Strategic Alignment Maturity (SAM) assessment, which includes:

- *communications maturity* – the degree to which ideas are exchanged between stakeholders as well as the development of a clear understanding of what it takes to be successful by all parties;
- *competency/value measurements maturity* – the extent to which the value of IT and IA can be demonstrated to the business;
- *governance maturity* – the extent to which resources, conflict resolution, risk and responsibility for IT and IA are shared with appropriate stakeholders;
- *partnership maturity* – the degree to which an equal relationship exists between the stakeholders, which is based on mutual trust and the sharing of risks and rewards;
- *technology scope maturity* – the extent to which the technology provides the organisation the opportunity to grow, compete and profit; and
- *skills maturity* – the extent to which the staff have the motivation, knowledge and skills to learn, innovate and change in a dynamic environment.

Others such as Keeble *et al.* (2003), Kaplan and Norton (1996a, 2004a, b) and Kaplan (2001) have also used a Gestalt perspective to develop alignment measures. In addition, the use of the balanced scorecard for developing and measuring IA, IT and business strategy alignment has been discussed by McFadzean *et al.* (2005) and Birchall *et al.* (2004) (see Figure 2).

This model includes the different stakeholder perspectives and illustrates how certain tensions between stakeholder groups may occur. For example, organisations that undertake business through the internet will expose themselves to more risk than companies that are not connected. However, many firms are finding that sharing information and trading with customers over the internet are improving their competitive advantage (Evans and Smith, 2004; Siaw and Yu, 2004; Teo and Pian, 2003). Thus, these organisations may have to make a trade-off between their risk of exposure and their ease of doing business. Alignment can be measured at regular intervals during the strategy development and implementation processes. Unremitting environmental change may result in a modification of strategy, and therefore it is vital that the degree of alignment between IA, IS and corporate strategy is continuously measured.

Implications for research

The literature on information assurance suggests that a strategic approach is needed. IA is vital to achieve good corporate governance, retain customers and generally strive

Source: McFadzean *et al.* (2005) and Birchall *et al.* (2004)

Figure 2.
Venkatraman's (1989) model of fit applied to information assurance and corporate strategy

for competitive advantage. There is evidence, however, that this is not being achieved at three levels:

(1) Boards and senior executive still take little sustained interest in the matter (Dutta and McCrohan, 2002; Information Assurance Advisory Council, 2003).

(2) There is a lack of alignment between business and information assurance strategies (Kovacich, 2001; Von Solms, 2001).

(3) Measuring the success of information assurance in order to ensure its alignment with business strategy is difficult. Few frameworks exist, and there is evidence that those that do are not applied widely (Dutta and McCrohan, 2002; Von Solms, 2001).

The first step in addressing why this may be the case is to define what exactly "alignment" would mean in the context of information assurance. To our knowledge, no study has considered the alignment of information assurance with business strategy explicitly, or what form alignment or fit should take. Figure 3 illustrates, using Venkatraman's (1989) classification, what each definition of "fit" would mean in an information assurance context. Many of the potential research models that are illustrated in Figure 3 are inspired by the work of Bergeron *et al.* (2001). In addition, Figure 3 presents some potential research questions on each area of fit as it relates to IA. In Figure 3 we have deliberately used the word "performance" as a more "vague" dependent variable than "business performance", which is the dependent variable traditionally used in the IS alignment literature. This is because we can conceive circumstances where a more focused measure of performance is needed (e.g. customer service performance, or user acceptance).

Some of the verbalisations of alignment in the context of information assurance given in Figure 3 indicate the need to profile an organisation's information assurance state. Birchall *et al.* (2003) discovered five key strategic trade-offs inherent in information assurance strategy decisions:

(1) *procedural controls versus creativity* – the need to maintain secure processes within the organisation versus the need to develop novel and innovative ideas;

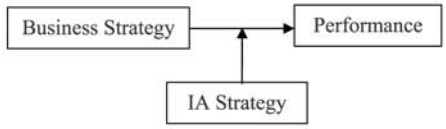
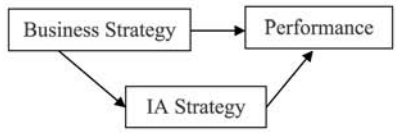
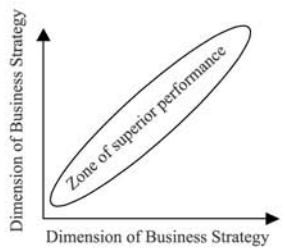
(2) *top-down control versus trust* – the need to control information sharing versus the need to trust employees with sensitive information;

(3) *exposure versus ease of doing business* – the need to reduce the exposure to security incidents versus the need to allow stakeholders (customers and suppliers) to undertake business with ease and without restriction;

(4) *insourcing versus outsourcing* – the need to undertake information security in-house versus the need to outsource it to another organisation; and

(5) *reputation versus the bottom line* – to ensure that the company maintains a reputation for security and ease of doing business versus the need to reduce cost and increase revenue.

By considering how each trade-off is affected by business strategy, a clearly defined vision of requirements can be communicated to IA practitioners. This should allow IA policies to be established that do not restrict the ability of the organisation to implement the overall corporate strategy (see Figure 4).

Perspective:	
Moderation	
Application to information assurance:	The interaction between business strategy and a moderator, such as information assurance, will influence performance.
Example research questions:	In what ways will the interaction between IA and business strategy determine performance? How can this interaction be changed in order to improve performance?
Potential research model:	
Mediation	
Application to information assurance:	The interaction between business strategy and an intervening mechanism, such as information assurance, will *indirectly* determine the success of organisational performance.
Example research questions:	What is the role of IA in supporting strategy implementation? How can this interaction be changed in order to improve organisational performance?
Potential research model:	
Matching	
Application to information assurance:	There should be a match between two variables for superior performance to be achieved.
Example research questions:	How should IA practices differ between organisations that use technology for competitive advantage and those that don't?
Potential research model:	

(Continued)

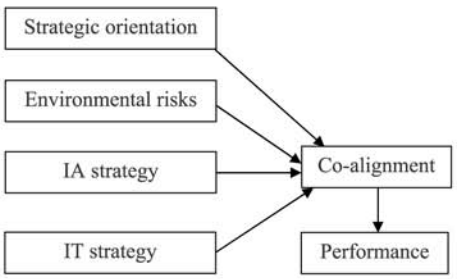
Figure 3.
Using the balanced scorecard to develop and measure alignment

Gestalts

Application to information assurance:	The coherence between a set of attributes – such as information assurance, employee motivation and training, the sharing of information between stakeholders, the use of technology and corporate strategy – and how this influences performance.
Example research questions:	How will the coherence between the need for creativity and information sharing, employee awareness, internal business processes and information assurance procedures influence the success of the organisation? How can this coherence be enhanced? How will the relationship between IA strategy, IT strategy and corporate strategy shape the success of the organisation? In what ways can this alignment be improved?
Potential research model:	

	IA Characteristic 1	IA Characteristic 2	IA Characteristic 3	IA Characteristic 4	IA Characteristic 5	IA Characteristic n
Company 1		x		x		x
Company 2	x			x	x	
Company 3	x		x	x	x	
Company 4	x		x	x	x	x
Company 5		x	x		x	
Company n			x			x

Covariation

Application to information assurance:	Fit relates to a consistency within a set of interdependent variables
Example research questions:	What are the variables that need to be taken into account when putting together an IA strategy that is supportive of business strategy? How can a firm ensure that its IA strategy is consistent with its business and IT strategy?
Potential research model:	

(Continued)

Figure 3.

Deviation	
Application to information assurance:	The degree of adherence to a specific profile (for instance, IA strategy, business strategy, environmental variables) will be a predictor of business performance. On the other hand, if there is *deviation* from this ideal pattern, a reduction in performance will result.
Example research questions:	What would be the result if there is a deviation from either the specified corporate strategy or the specified IA strategy?
Potential research model:	

	High Performance Group	Company X	Deviation
IA strategy dimension 1	i1	x1	i1-x1
IA strategy dimension 2	i2	x2	i2-x2
IA strategy dimension 3	i3	x3	i3-x3
IA strategy dimension 4	i4	x4	i4-x4
IA strategy dimension 5	i5	x5	i5-x5
IA strategy dimension n	in	xn	in-xn

Source: Adapted from McFadzean *et al.* (2005) and Birchall *et al.* (2004)

Figure 3.

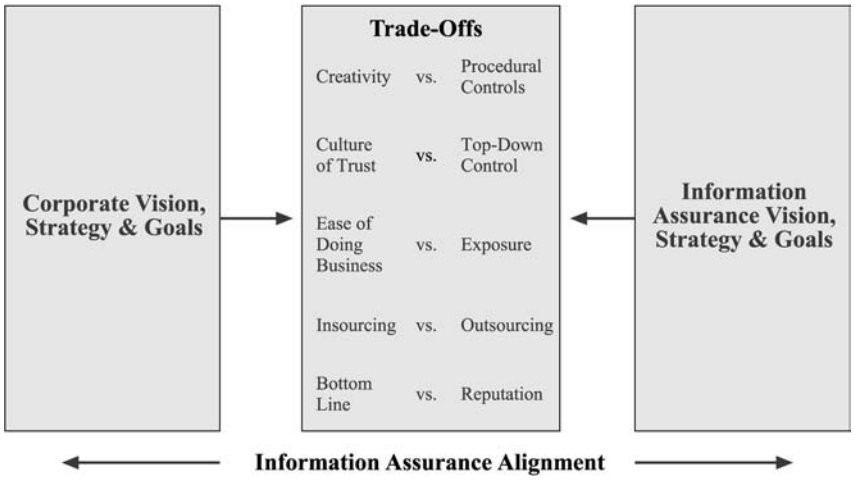


Figure 4.
Aligning information assurance with corporate strategy

We can therefore suggest that there is scope for further research at two levels:

(1) While there is theoretical and practitioner support for the idea that information assurance should be aligned with business strategy, we need to understand what model of alignment is most appropriate. Because no studies have been undertaken around the topic, this could start with an investigation of alignment

dynamics. What do practitioners think of the alignment between information assurance and business strategy? What impact do they see IA alignment having on organisational performance? How do they think it is achieved in their organisation, and how could the process be improved?

(2) In order to test the impact of alignment, we need to understand how the success of information assurance can be best measured and communicated at a strategic level in organisations. Different stakeholders in a business will have different requirements from information assurance. The success of alignment will therefore need to be explored from different perspectives. In practice this points towards the need for research into what drives perceptions of success in information assurance and how this success is measured.

Implications for managers

The literature reviewed suggests that there is a need for a comprehensive framework to help managers align information assurance with business strategy. As with all frameworks of this kind – for instance Kaplan and Norton's (1996b) balanced scorecard – it is necessary to start from a shared understanding of the goals of the organisation and how they are reflected in the needs of its stakeholders.

Working from this shared platform of understanding, specific IA goals could be developed and tested to ensure that they are fully aligned to the organisation's corporate vision. Research has shown that alignment can be encouraged and improved by developing both formal and informal lines of communication between IA and business functionaries (Chan, 2002; Chandler-Wilde and McFadzean, 2004). In addition, both the business and IA personnel must develop an understanding of each other's requirements as well as recognising that each party has important and valuable goals. Studies have shown that a lack of understanding about requirements and the importance of the other group's needs can lead to a breakdown in communication and a misalignment of goals (Chandler-Wilde and McFadzean, 2004; Luftman and Brier, 1999). Finally, the two groups must recognise that both the business and security environments are constantly changing and therefore the goals for each area will need to be reviewed on a continuous basis (these factors are illustrated in the conceptual model presented in Figure 1).

After the IA/business alignment has been agreed both the IA function and the business function can define the critical success factors (CSFs) that would indicate attainment of their goals. Appropriate operational metrics to measure progress towards those CSFs could then be determined. The metrics themselves may overlap from one goal to another, or they may include non-technical measures. However, this process would ensure an important transition towards a focus on measuring what is important to the business, rather than what can easily be measured. From the model shown in Figure 1, appropriate roles and responsibilities can be given to all the organisation's stakeholders. This includes encouraging employees, suppliers and customers to remain vigilant with their passwords or other security devices and to be aware of potential security risks.

Conclusion

> We can understand the very notion of alignment only thanks to our (tacit) knowledge of the messy world (Ciborra, 2002, p. 23).

Although few of the papers we have reviewed as part of this paper would be as blunt as describing information assurance as "messy", it is clear that the topic is still in its infancy. This means that few practitioners or academics understand fully the strategic consequences of IA, let alone the impact of poor alignment between IA strategy and business strategy. It is, however, clear that information assurance is an important function within organisations. Unfortunately, much of the IA literature focuses on the operational level where researchers generally explore IA metrics, privacy issues, new methods for counteracting threats, risk analysis and trust amongst others.

Nonetheless, it is not sufficient to show that there is theoretical and practitioner support for the idea that IA should be aligned with business strategy. We also need to understand what model of alignment is most appropriate. All the six models of fit proposed by Venkatraman have face validity when applied to corporate and IA strategy. We suggest that in order to ascertain which would be most appropriate, researchers should start by an investigation of alignment dynamics: What do practitioners think of the alignment between IA and business strategy, how do they think it is achieved in their organisation, and how could the process be improved?

Secondly, in order to test the impact of alignment, we need to understand how the success of IA can be best measured and communicated at a strategic level in organisations. Different stakeholders in an organisation will have different requirements from IA. The success of alignment will therefore need to be looked at from different perspectives. In practice this points towards the need for research into what drives perceptions of success in IA, and how success is measured.

Note

1. The IAAC is a UK not-for-profit body comprising corporate leaders, public policy makers, law enforcement and the research community; its aim is to increase awareness of the very real business importance of information assurance and to progress towards better practice and legislation to encourage businesses to adapt sound IA practice.

References

Armstrong, J., Rhys-Jones, M. and Rathmell, A. (2002), *Information Assurance & Corporate Governance: What Every Director Must Know*, Information Assurance Advisory Council, Cambridge.

Austin, R.D. and Darby, C.A. (2003), "The myth of secure computing", *Harvard Business Review*, Vol. 81 No. 6, pp. 120-6.

Beal, R.M. (2000), "Competing effectively: environmental scanning, competitive strategy, and organizational performance in small manufacturing firms", *Journal of Small Business Management*, Vol. 38 No. 1, pp. 27-47.

Bergeron, F. and Raymond, L. (1995), "The contribution of IT to the bottom line: a contingency perspective of strategic dimensions", *Proceedings of the 16th International Conference on Information Systems, Amsterdam*, pp. 167-81.

Bergeron, F., Raymond, L. and Rivard, S. (2001), "Fit in strategic information technology management research: an empirical comparison of perspectives", *Omega*, Vol. 29 No. 2, pp. 125-42.

Bergeron, F., Raymond, L. and Rivard, S. (2004), "Ideal patterns of strategic alignment and business performance", *Information and Management*, Vol. 41 No. 8, pp. 1003-20.

Birchall, D., Ezingeard, J.-N. and McFadzean, E.S. (2003), *Information Security: Setting the Boardroom Agenda*, Grist Ltd, London.

Birchall, D., Ezingeard, J.-N., McFadzean, E.S., Howlin, N. and Yoxall, D. (2004), *Information Assurance: Strategic Alignment and Competitive Advantage*, Grist Ltd, London.

Birkinshaw, J. and Gibson, C. (2004), "Building ambidexterity into an organization", *Sloan Management Review*, Vol. 45 No. 4, pp. 47-55.

Boyce, J.G. and Jennings, D.W. (2002), *Information Assurance: Managing Organizational IT Security Risks*, Butterworth-Heinemann, London.

Burn, J.M. (1996), "IS innovation and organizational alignment – a professional juggling act", *Journal of Information Technology*, Vol. 11 No. 1, pp. 3-12.

Campbell, K., Gordon, L.A., Loeb, M.P. and Zhou, L. (2003), "The economic cost of publicly announced information security breaches: empirical evidence from the stock market", *Journal of Computer Security*, Vol. 11 No. 3, pp. 431-48.

Chan, Y.E. (2002), "Why haven't we mastered alignment? The importance of the informal organization structure", *MIS Quarterly Executive*, Vol. 1 No. 2, pp. 97-112.

Chan, Y.E., Huff, S.L., Barclay, D.W. and Copeland, D.G. (1997), "Business strategic orientation, information systems strategic orientation, and strategic alignment", *Information Systems Research*, Vol. 8 No. 2, pp. 125-50.

Chandler-Wilde, R. and McFadzean, E.S. (2004), "Aligning IT with business strategy: a matter of process", paper presented at ISOneWorld Conference, Las Vegas, NV.

Ciborra, C. (2002), *The Labyrinths of Information: Challenging the Wisdom of Systems*, Oxford University Press, Oxford.

Croteau, A.-M., Solomon, L., Raymond, L. and Bergeron, F. (2001), "Organizational and technological infrastructures alignment", *Proceedings of the Hawaii International Conference on System Sciences, Maui, HI*, pp. 1-10.

Culnan, M.J. and Armstrong, P.K. (1999), "Information privacy concerns, procedural fairness, and impersonal trust: an empirical investigation", *Organization Science*, Vol. 10 No. 1, pp. 104-15.

Deloitte Touche Tohmatsu (2003), "Global security survey", available at: www.deloitte.com/gfsi (accessed 16 May 2003).

Department of Trade and Industry (2004), "Information security breaches survey", DTI and PriceWaterhouseCoopers, available at: www.pwc.com/images/gx/eng/about/svcs/grms/2004Technical_Report.pdf (accessed 28 April 2004).

Dhillon, G. (2004), "The challenge of managing information security", *International Journal of Information Management*, Vol. 24 No. 1, pp. 3-4.

Dutta, A. and McCrohan, K. (2002), "Management's role in information security in a cyber economy", *California Management Review*, Vol. 45 No. 1, pp. 67-87.

Earl, M. (1995), "Integrating IS and the organisation: a framework of organisational fit", in Earl, M. (Ed.), *Information Management: The Organisational Dimension*, Oxford University Press, Oxford, pp. 485-502.

Ernst & Young (2003), *Global Information Security Survey 2003*, Ernst & Young LLP.

Ettredge, M. and Richardson, V.J. (2002), "Assessing the risk in e-commerce", *Proceedings of the 35th Annual Hawaii International Conference on System Sciences, Maui, HI*.

Ettredge, M. and Richardson, V.J. (2003), "Information transfer among internet firms: the case of hacker attacks", *Journal of Information Systems*, Vol. 17 No. 2, pp. 71-82.

Evans, D.M. and Smith, A.C.T. (2004), "Augmenting the value chain: identifying competitive advantage via the internet", *Journal of Information Technology Theory and Application*, Vol. 6 No. 1, pp. 61-78.

Evans, R. and Danks, A. (1998), "Strategic supply chain management: creating shareholder value by aligning supply chain strategy with business strategy", in Gattorna, J. (Ed.), *Strategic Supply Chain Alignment*, Gower, London.

Ezingeard, J.-N. and Birchall, D. (2004), "Securing information: governance issues", in Crainer, S. and Dearlove, D. (Eds), *Financial Times Handbook of Management*, Pearson Education, Harlow.

Ezingeard, J.-N., Bowen-Schrire, M. and Birchall, D. (2004), "Triggers of change in information security management", paper presented at ISOneWorld Conference, Las Vegas, NV.

Ezingeard, J.-N., McFadzean, E.S. and Birchall, D. (2003), "Board of directors and information security: a perception grid", paper presented at British Academy of Management Conference, Harrogate.

Gietzmann, M.B. and Selby, M.J.P. (1994), "Assessment of innovative software technology: developing an end-user-initiated interface design strategy", *Technology Analysis & Strategic Management*, Vol. 6 No. 4, pp. 473-83.

Gottschalk, P. (2000), "Studies of key issues in IS management around the world", *International Journal of Information Management*, Vol. 20 No. 3, pp. 169-80.

Gould, J.L. and Kolb, W.L. (1964), *A Dictionary of the Social Sciences*, The Free Press, New York, NY.

Henderson, J.C. and Venkatraman, N. (1993), "Strategic alignment: leveraging information technology for transforming organizations", *IBM Systems Journal*, Vol. 32 No. 1, pp. 4-16.

Hodges, J. (2002), "Technology studied from the board's perspective", *Internal Auditor*, Vol. 59 No. 1, pp. 13-14.

Hoffman, J.J., Cullen, J.B., Carter, N.M. and Hofacker, C.F. (1992), "Alternative methods for measuring organizational fit: technology, structure and performance", *Journal of Management*, Vol. 18 No. 1, pp. 45-57.

Hussin, H., King, M. and Cragg, P. (2002), "IT alignment in small firms", *European Journal of Information Systems*, Vol. 11 No. 2, pp. 108-27.

Information Assurance Advisory Council (2003), *Engaging the Board: Corporate Governance & Information Assurance*, Information Assurance Advisory Council, Cambridge.

International Organization for Standardization (1989), *ISO 7498-2:1989 Information Processing Systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture*, International Organization for Standardization, Geneva.

IT Governance Institute (2003), *IT Control Objectives for Sarbanes-Oxley*, IT Governance Institute, Rolling Meadows, IL.

Kaplan, R.S. (2001), "Using strategic themes to achieve organizational alignment", *Balanced Scorecard Report*, Harvard Business School Publishing, Boston, MA.

Kaplan, R.S. (2002), "Using strategic themes to achieve inter-organizational alignment", *Balance Scorecard Report*, Harvard Business School Publishing, Boston, MA.

Kaplan, R.S. and Norton, D.P. (1996a), *The Balanced Scorecard: Translating Strategy into Action*, Harvard Business School Press, Boston, MA.

Kaplan, R.S. and Norton, D.P. (1996b), "Using the balanced scorecard as a strategic management system", *Harvard Business Review*, Vol. 74 No. 1, pp. 75-85.

Kaplan, R.S. and Norton, D.P. (2004a), *Strategy Maps: Converting Intangible Assets into Tangible Outcomes*, Harvard Business School Press, Boston, MA.

Kaplan, R.S. and Norton, D.P. (2004b), "Measuring the strategic readiness of intangible assets", *Harvard Business Review*, Vol. 82 No. 2, pp. 52-63.

Keeble, J.J., Topiol, S. and Berkeley, S. (2003), "Using indicators to measure sustainability performance at a corporate and project level", *Journal of Business Ethics*, Vol. 44 Nos 2/3, pp. 149-58.

Keng, S. (2003), "Interorganizational systems and competitive advantages – lessons from history", *Journal of Computer Information Systems*, Vol. 44 No. 1, pp. 33-9.

Kotler, P., Armstrong, G., Saunders, J. and Wong, V. (2001), *Principles of Marketing*, 3rd European edition, Financial Times Prentice-Hall, Harlow.

Kovacich, G.L. (2001), "The Corporate Information Assurance Officer (CIAO)", *Computers & Security*, Vol. 20 No. 4, pp. 302-7.

Koved, L., Nadalin, A., Nagaratnam, N., Pistoia, M. and Shrader, T. (2001), "Security challenges for Enterprise Java in an e-business environment", *IBM Systems Journal*, Vol. 40 No. 1, pp. 130-52.

Lai, V.S. (2001), "Issues of international information systems management: a perspective of affiliates", *Information and Management*, Vol. 38 No. 4, pp. 253-64.

Landwehr, C.E. (2001), "Computer security", *International Journal of Information Security*, Vol. 1 No. 1, pp. 3-13.

Logan, P.Y. and Logan, S.W. (2003), "Bitten by a bug: a case study in malware infection", *Journal of Information Systems Education*, Vol. 14 No. 3, pp. 301-5.

Luftman, J. (2003a), "Assessing IT/business alignment", *Information Systems Management*, Vol. 20 No. 4, pp. 9-15.

Luftman, J. (2003b), "Assessing IT/business alignment", *Information Strategy: The Executive's Journal*, Vol. 20 No. 1, pp. 7-14.

Luftman, J. and Brier, T. (1999), "Achieving and sustaining business-IT alignment", *California Management Review*, Vol. 42 No. 1, pp. 109-22.

McFadzean, E.S., Ezingeard, J.-N. and Birchall, D. (2005), "Information security from the perspective of senior executives: the development of a balanced scorecard", Working Paper No. 0503, Henley Management College Working Paper Series, Henley-on-Thames.

McFarlan, F.W. (1984), "Information technology changes the way you compete", *Harvard Business Review*, Vol. 62 No. 3, pp. 98-103.

Miller, D. (1981), "Toward a new contingency approach: the search for organizational gestalts", *Journal of Management Studies*, Vol. 18 No. 1, pp. 1-26.

Miller, D. (1987), "The genesis of configuration", *Academy of Management Review*, Vol. 12 No. 4, pp. 686-701.

National Association of Corporate Directors (2001), *Information Security Oversight: Essential Board Practices*, National Association of Corporate Directors, Washington, DC.

Palmer, J.W. and Markus, M.L. (2000), "The performance impacts of quick response and strategic alignment in specialty retailing", *Information Systems Research*, Vol. 11 No. 3, pp. 241-59.

Parker, X.L. (2001), "Understanding risk", *Internal Auditor*, Vol. 58 No. 1, pp. 61-5.

Pervan, G. (1998), "How chief executive officers in large organizations view the management of their information systems", *Journal of Information Technology*, Vol. 13 No. 2, pp. 95-109.

Peters, T.J. and Waterman, R.H. (1982), *In Search of Excellence: Lessons from America's Best Run Companies*, Harper & Row, New York, NY.

Reich, B.H. and Benbasat, I. (1996), "Measuring the linkage between business and information technology objectives", *MIS Quarterly*, Vol. 20 No. 1, pp. 55-81.

Reich, B.H. and Benbasat, I. (2000), "Factors that influence the social dimension of alignment between business and information technology objectives", *MIS Quarterly*, Vol. 24 No. 1, pp. 81-113.

Sabherwal, R. and Chan, Y.E. (2001), "Alignment between business and IS strategies: a study of prospectors, analyzers, and defenders", *Information Systems Research*, Vol. 12 No. 1, pp. 11-33.

Sabherwal, R. and Kirs, P. (1994), "The alignment between organizational critical success factors and information technology capability in academic institutions", *Decision Sciences*, Vol. 25 No. 2, pp. 301-30.

Safizadeh, M.H., Ritzman, L.P., Sharma, D. and Wood, C. (1996), "An empirical analysis of the product-process matrix", *Management Science*, Vol. 42 No. 11, pp. 1576-91.

Sauer, C., Dampney, C.N.G. and Southon, G. (1997), "Fit, failure, and the house of horrors: toward a configurational theory of IS project failure", *Eighteenth International Conference on Information Systems, Atlanta, GA*, pp. 349-66.

Segars, A.H. and Grover, V. (1998), "Strategic information systems planning success: an investigation of the construct and its measurement", *MIS Quarterly*, Vol. 22 No. 2, pp. 139-63.

Siaw, I. and Yu, A. (2004), "An analysis of the impact of the internet on competition in the banking industry, using Porter's five forces model", *International Journal of Management*, Vol. 21 No. 4, pp. 514-23.

Sledgianowski, D. and Luftman, J. (2005), "IT-business strategic alignment maturity: a case study", *Journal of Cases on Information Technology*, Vol. 7 No. 2, pp. 102-20.

Swartz, N. (2003), "The cost of Sarbanes-Oxley", *Information Management Journal*, Vol. 37 No. 5, p. 8.

Teo, T.S.H. and King, W.R. (1996), "Assessing the impact of integrating business planning and IS planning", *Information and Management*, Vol. 30 No. 6, pp. 309-21.

Teo, T.S.H. and Pian, Y. (2003), "A contingency perspective on internet adoption and competitive advantage", *European Journal of Information Systems*, Vol. 12 No. 2, pp. 78-92.

Treanor, J. (2000), "Security fear shuts online bank", *The Guardian*, August 1, p. 1.

Tweney, D. (1998), "The consumer battle over online information privacy has just begun", *InfoWorld*, Vol. 20 No. 25, p. 66.

Venkatraman, N. (1989), "The concept of fit in strategy research: toward verbal and statistical correspondence", *Academy of Management Review*, Vol. 14 No. 3, pp. 423-44.

Venkatraman, N. and Camillus, J.C. (1984), "Exploring the concept of 'fit' in strategic management", *Academy of Management Review*, Vol. 9 No. 3, pp. 513-25.

Von Solms, B. (2001), "Corporate governance and information security", *Computers & Security*, Vol. 20 No. 3, pp. 215-18.

Ward, J.M. (1988), "Information systems and technology application portfolio management – an assessment of matrix-based analyses", *Journal of Information Technology*, Vol. 3 No. 3, pp. 205-15.

Whitman, M.E. (2004), "In defense of the realm: understanding the threats to information security", *International Journal of Information Management*, Vol. 24 No. 1, pp. 43-57.

Wolf, D.G. (2003), "Statement by NSA's Director of Information Assurance before the House Select Committee on Homeland Security, US House of Representatives", available at: www.nsa.gov/ia/Wolf_SFR_22_July_2003.pdf (accessed 22 July 2003).

Wright, T. (2001), "Secure digital archiving of high-value data", *BT Technology Journal*, Vol. 19 No. 3, pp. 60-6.

About the authors

Jean-Noël Ezingeard is Professor of Processes and Systems Management and Academic Dean at Henley Management College. His first degree was in Engineering Science from Ecole Centrale de Lille, and Engineering Grand Ecole. He later obtained his PhD from Brunel University for research on performance evaluation techniques for information systems. Jean-Noël's current research interests are in the area of technology management, IT security, information assurance and business continuity planning. He has a keen interest in educating engineers for the twenty-first century, and joined Henley in 1998 before becoming a College Professor in 2004. He is also a regular speaker at conferences in the UK and overseas. He is also a Visiting Professor at the Lille Graduate School of Management. Jean-Noël Ezingeard is the corresponding author and can be contacted at: Jean-Noel.Ezingeard@HenleyMC.ac.uk

Elspeth McFadzean is with the Associate Faculty at Henley Management College. She has several research publications in the area of team dynamics, innovation and group learning.

Professor David Birchall teaches and researches aspects of work in the digital economy in the Information and Operations Management Group at Henley Management College. David's research interests are in the areas of innovation practices in organisations and organisational implications of IT. He is a regular speaker on innovation management, knowledge management, IT and learning and new forms of organisation and has designed management development programmes at all levels. He currently directs projects funded by the European Union, UK Government Department and several commercial organisations; moreover, he regularly presents research findings at conferences and seminars worldwide.