RISK MANAGEMENT VS. THE MANAGEMENT OF RISK: DOES IT MATTER TO THE BOARD?

Shaun Posthumus[1], **Rossouw von Solms** [2]

[1],[2]Department of Business Information Systems, Port Elizabeth Technikon, South Africa

[1]sposthumus@petech.ac.za, +27 83 6744006, Private Bag X6011, Port Elizabeth, 6000
[2]rossouw@petech.ac.za, +27 41 5043604, Private Bag X6011, Port Elizabeth, 6000

ABSTRACT

The protection of information assets has become of paramount importance today. Currently, various risk management efforts are implemented to deal with the risks that affect an organization's information assets. According to the King Report [3] on Corporate Governance, it is ultimately the responsibility of the Board of Directors to oversee how all risks are analyzed and managed in an organization. From an information protection perspective, the term risk management is used interchangeably to describe both how the IT discipline deals with the risks to information and how the Board of Directors deals with all information related risks. This paper argues that these concepts imply different meanings. Therefore the term risk management should be used to describe merely how risks to information technology infrastructure are dealt with. Additionally, the term "management of risk" is more suited to describe how the Board deals with all risks from an information protection perspective.

KEYWORDS

Risk Management, Management of risk, Corporate Governance

RISK MANAGEMENT VS. THE MANAGEMENT OF RISK: DOES IT MATTER TO THE BOARD?

1 INTRODUCTION

No matter what type of activity or manner of service an organization provides, there is bound to be some form of risk involved. This is especially true when one considers the vast integration of IT systems into most organizations today. IT systems play a significant role in managing valuable information assets and facilitating various business operations. Any risks resulting from the dependence on information technology may have the potential to negatively impact on an organization's business value should these risks go undetected or underestimated [1]. For this reason it is necessary to identify and manage these potentially harmful risks through some form of risk management activity.

Risk management is, or should be an essential part of any organization's corporate responsibilities, but what exactly does this process entail? Furthermore, does risk management produce comprehensive information regarding the protection process of all information related risks? The King Report on Corporate Governance [3] states that the Board of Directors is ultimately responsible for risk management, which should enable them to successfully manage all the risks affecting their organization's information assets. It is noted however, that there is a difference between what is termed risk management and the management of risk. According to literature these two terms are distinct. It is the objective of this paper to attempt to put some perspective on the interchangeable usage of these terms in the information and IT environments, with relation to the King Report [3]. This should clearly spell out in information protection terms, what risk management actually means in various disciplines where it is apparend.

2 RISK MANAGEMENT - ORIGIN AND OBJECTIVE

2.1 The Origin of Risk Management

According to Terry Simister [2], Chairman of the Institute of Risk Management (IRM), the term risk management was coined as far back as the early 1950's when insurance managers began to identify themselves as risk managers and began practicing what they called risk management activities. Simister [2] further illustrates that the term risk management became the latest buzzword gaining immense popularity. Soon risk management activities were being widely utilized largely by insurance underwriting and broking disciplines to deal primarily with any associated financial risks. Over time, more disciplines, not excluding information technology (IT), began to realize the benefits of applying various risk management practices to their day-to-day business activities. This saw the expansion of risk management into a formally accepted and renowned discipline of its own [2]. Since risk management is no longer used purely in the financial sense, it is necessary to define what this process generally entails, as many disciplines may have their own understanding of what it actually means to them. This is most definitely the case according to Simister [2].

2.2 The Objective of Risk Management

The King Report [3] on Corporate Governance states that: ”The risk management process entails the planning, arranging and controlling of activities and resources to minimize the impacts of all risks to levels that can be tolerated by shareowners and other stakeholders whom the board has identified as relevant to the business of the company.”. These activities as described by the King Report [3], tend to have a specific focus i.e. they follow a particular risk management strategy. These strategies include risk avoidance, risk mitigation, risk acceptance and risk transference [4]. A risk avoidance strategy focuses on implementing means to stay away from risks, whereas a risk mitigation strategy focuses on implementing means to reduce the potential of risks to cause harm through diminishing either their impact or likelihood of occurrence. A risk transference strategy, however, focuses on shifting the responsibility of the risk, should it result in an unwanted situation, onto an external body, such as an insurance firm. In contrast, a risk acceptance strategy leaves the responsibility of the risk with the organization who attempts to absorb the consequences of such a risk without implementing any means to transfer, avoid or reduce the risks. A risk acceptance strategy may be implemented if the risks involved are to such an extent that an organization considers them of negligible consequence. This may depend on the risk appetite of an organization [4], which is the amount of risk an organization is willing to tolerate without these risks having a detrimental effect on such an organization.

Regardless of the risk management strategy an organization chooses, the ultimate goal of these strategies is the same. Heemstra and Kusters [5] describe this goal as ”identifying and responding to potential problems with sufficient time to avoid crisis situations.” More completely though, with all of the above in mind, the objective of risk management can be described as the process of recognizing and reacting to potentially harmful risks through a risk management strategy which incorporates the planning, arranging and controlling of various activities and resources. This serves to dissipate the criticality of risks to a level that satisfies an organization’s risk appetite.

The process of risk management is usually preceded by an exercise known as risk analysis [6]. Generally, risk analysis involves identifying and assessing which risks an organization needs to consider. Thus, enabling such an organization to manage these risks through a particular risk management activity. The financial sector for example, employs financial risk analysis techniques (also known as investment appraisal techniques) to help managers choose the best investment for their company’s capital resources. These techniques are aimed at establishing an expected outcome for each proposed future investment so that any potentially unprofitable ventures may be avoided. Standard deviation and sensitivity analysis are examples of such techniques. Usually, once an investment decision has been reached, assisted by the results of a risk analysis exercise, any risks associated with the chosen investment may be managed through efforts such as a hedging scheme in the form of forward contracts or options [7]. These hedging schemes would be chosen and implemented as part of some financial risk management activity.

Most organizations today however, face more than merely financial risks. The use of information technology, to manage information assets and facilitate business operations, in these organizations has brought about the realization of an even wider spectrum of risks. These risks most definitely require consideration. The IT discipline does indeed employ risk management practices to deal with risks, but how exactly is risk management in the IT discipline implemented? The next section deals with this.

3 RISK MANAGEMENT FROM AN IT PERSPECTIVE

As far as the IT discipline is concerned, the concept of risk is understood to comprise three core components. These components are assets, threats and vulnerabilities [8]. An asset is anything that an organization considers valuable, and it is something that contributes towards the business value of an organization. Assets could include things like hardware, business processes, people and information. Threats are anything that has the potential to cause damage to, or destroy assets, thereby decreasing the business value of an organization. Threats could include people like hackers for example, weather phenomena or even computer hardware or software failures. A vulnerability is a means by which a threat is allowed to have an influence on an asset like a weakness or loophole in a computer system, for example. The process of risk management in IT ultimately aims to provide protection to an organization's assets by reducing the impact on the asset, the probability of the threat and/or vulnerabilities and thereby reducing any risks. The business environment is, however, constantly changing and evolving due to technological innovation and greater dependence on such technology. This may only serve increase the number of risks that can have an affect on an organization's assets [9]. This may be clearly illustrated by looking at the evolution of the IT environment, describing just how the risk management practices employed here have had to adapt to cope with any new risks arising from technological innovation and dependence on such technology.

3.1 Some History on Risk Management

The stages of evolution in the IT environment can be categorized into three distinct eras [8]. In the first era, computers had very limited capabilities. They were large mainframes and their purpose was to process the data from various other departments within an organization. These computers were located in a centralized computer department from which all the data processing commenced. Access to this facility was restricted to those responsible for operating the computers. Risks were managed by means of simple physical security controls. Burglar alarms, burglar bars, security guards, surveillance cameras and locked doors are examples of such physical controls [10]. The identification of controls was based on the use of security control checklists listing all possible security controls available. Some examples of the checklists previously in use are the SAFE checklist, the Computer Security Handbook and the AFIPS checklist [11].

The second era in the evolutionary process saw the introduction of advances such as multiprocessing and high-speed communications. These advances instigated the progression to distributed computing systems. Distributed systems make hardware and software resources more easily accessible to computer users in remote locations. This enables them to log onto disparate sites and work with the programs and files located at these sites [12]. With these new developments came new risks and subsequently it became necessary to identify and cater for these risks. The process of risk management had to incorporate new means to address these various new risks that had now become apparent. Technical controls were thus introduced to mitigate the consequences of potential risks. These technical controls included mechanisms such as access control, user authentication and data encryption [8].

In the third era information technology began to facilitate an organization's business processes and services to clients and customers. The Internet enabled many

organizations to conduct business with their customers and other organizations more conveniently through electronic commerce. Information technology had, by this stage, come to play an integral role in the daily operations of most organizations. Moreover, the effective use of information began to play a significant role in sustaining these organizations and consequently ensuring the protection of this information was paramount. Therefore there was a shift in the emphasis of what needed protection. While it was still important to protect the IT infrastructure it had become even more important to ensure the protection of an organization's information assets [8]. In order to help protect information assets more effectively, various operational security controls were introduced in the form of policies, standards and procedures [8]. Operational controls attempt to enforce the adherence to certain codes of conduct, as well as common security practices by users, when they use information systems to do their work. ISO/IEC TR 13335[15] and BS 7799[13] are examples of such standards [8].

The requirements for the security of an organization's information assets had by this stage become based on three distinct criteria and not merely the IT infrastructure [13]. These criteria include firstly, requirements to protect the IT infrastructure; secondly, legal, regulatory and statutory requirements and thirdly, requirements for information integrity, confidentiality and availability as identified by an organization.

3.2 Addressing Security Requirements

In order to attempt to comply with the stipulated security requirements, the IT discipline also relies on a risk analysis exercise, which precedes risk management. However, there seems to be some difference in opinion presented in the literature as to whether risk analysis forms part of the process of risk management or not. Frosdick [6] suggests that risk analysis is a separate process which precedes risk management, and includes activities such as risk identification, risk estimation and risk evaluation, each of which will be discussed in more detail later in this paper. BS 7799 [13] however, describes risk management as the "process of identifying, controlling and minimizing or eliminating security risks that may affect information systems, for an acceptable cost". This definition of risk management includes the identification of risks, which Frosdick [6] suggests forms part of risk analysis. Hence it can be said that according to BS 7799 [13] risk analysis forms part of the process of risk management. This paper will however, adopt the idea that risk analysis precedes the process of risk management as it is understood and stated by Frosdick [6].

Risk analysis is said to provide meaningful information concerning risks so that the necessary controls can be chosen and implemented through IT risk management [6] and hence attempt to satisfy an organization's security requirements. According to BS 7799[13], risk analysis in IT is defined as the "assessment of threats to, impacts on and vulnerabilities of information and information processing facilities and the likelihood of their occurrence". Frosdick [6] suggests that the assessment of risks, which from an IT perspective comprise threats, vulnerabilities and assets involves three core phases, these are: risk identification, risk estimation and risk evaluation. During the risk identification phase any possible risks are considered by identifying all assets and all possible threats and vulnerabilities. The risk estimation phase commences next and is concerned with determining the probability of occurrence and level of impact of each potential risk through either quantitative or qualitative means or even a combination of both. Once the

severity of each of the identified risks has been determined, the risk evaluation phase commences. During this phase, risks are prioritized according to their severity in order to identify the most critical of these. This is so that each risk receives an appropriate level of attention, and that the most important security controls are selected and implemented. Once these risks have been prioritized the process of risk management is initiated.

The King Report [3] states that: ”The risk management process entails the planning, arranging and controlling of activities and resources...”. Risk management, which involves the controlling and minimizing of risks, can be conducted by means of various approaches in the IT discipline. ISO/IEC TR 13335[15] describes some of these approaches as the baseline approach, the informal approach, the detailed approach and the combined approach.

During implementation of the baseline approach to risk management in IT, controls are selected from a security checklist, a baseline control manual or a security code of practice. These sources ensure that an organization achieves an adequate level of security that is sufficient enough to guarantee the basic security of their assets. BS 7799 [13] would be an example of such a code of practice.

The informal approach is a time and cost effective means to risk management. Experts, such as well-established security analysts or consultants, apply their skills and knowledge in an unstructured, simple and practical manner to deal with the risks that an organization may face. The chance that some risks may be disregarded due to the subjective opinions and perceptions of these experts is, however, a sincere possibility [15].

The detailed approach to risk management is one which follows a formal risk analysis exercise, which incorporates the three phases of risk identification, risk estimation and risk evaluation [6]. The process of selecting and implementing security controls, amongst other things that make up the process of risk management, follows once the risk analysis exercise is completed. Hence this approach is a much more structured and organized exercise but can be quite resource intensive and time consuming.

The final approach, the combined approach, entails a combination of the baseline approach used to cater for risks that are not of critical importance, and the detailed approach used to cater for the more critical risks faced by an organization. This approach ensures that resources are allocated where they are most needed.

Despite whichever approach to risk management is chosen, the end result is the same i.e. security controls are selected and implemented in order to deal with the risks faced by an organization. It is suggested that security controls should only be implemented if the severity of the loss incurred as a result of the occurrence of an unwanted incident is greater than the cost of implementing the named security control [13].

After the implementation of selected security controls, several other activities may commence. These activities involve the maintenance of the security controls in place in order to sustain their effectiveness as risk reducing mechanisms. A further point of consideration includes scrutinizing the efficiency of the security platform in place by constantly amending asset registers and reassessing the likelihood of additional threats and vulnerabilities that may arise [4]. As such it can be said that activities such as control maintenance and risk monitoring have a role to play in managing risks. The King Report

[3] agrees, but in addition they add that the documentation of risks is another important aspect that needs consideration when risks are to be managed.

Risk analysis and risk management have thus far been described as having a significant role to play in addressing the security requirements of an organization. However, risk analysis and risk management from an information protection perspective do not seem to cover the full scope of the requirements, as enumerated in BS 7799 [13], needed to effectively protect information. They only seem to focus on one of these aspects i.e. the protection of the IT infrastructure. Additionally, they apparently disregard the other aspects such as legal, regulatory and statutory requirements and requirements for information integrity, confidentiality and availability. The implications of this will be addressed in subsequent sections.

The next issue that needs to be addressed, however, is whose responsibility it is to ensure that an organization's security requirements are satisfied. According to King [3] this ultimate responsibility rests with the Executive Management and the Board of Directors. As a result they need to ensure that the process of risk management within their organizations is effective. How though, do they know if their risk management endeavors are actually effective? In order to address this issue a discussion about the risk management responsibilities of the Board is in order.

4 CORPORATE GOVERNANCE AND RISK MANAGEMENT - WHAT IS THE BOARD RESPONSIBLE FOR?

The King Report on Corporate Governance clearly stipulates the responsibilities of the Board in terms of risk management. The Board of Directors must decide on an organization's strategic direction, constantly maintain complete control over an organization, adhere to laws and regulations and identify and monitor important risks, including any non-financial elements [3].

The Board can be considered the supreme authority in an organization and therefore they need to know about risks in all areas in order for them to make calculated decisions affecting the future of the organization. The King Report [3], therefore, states that the Board should be responsible for the total overall process of risk management addressing all aspects of risk that should be considered. In order to achieve this through risk management i.e. addressing all aspects of risk, the King Report [3] highlights several key considerations that the Board should contemplate with regard to their risk management activities. These include ensuring that organizational activities commence in an acceptable manner, ensuring the protection of all organizational assets, maintaining adherence to laws and regulations. They also include ensuring that there are measures in place that will promote accurate reporting of all risks and to be in no doubt that the organization is resilient to any potentially harmful risks.

Risk management should not be a once off exercise if an organization's Board of Directors is to ensure that these considerations have been taken into account. The King Report [3] emphasizes that it is the Board's duty to ensure that all risk management efforts are conducted on a regular basis. This helps to ascertain whether all risks have been dealt with successfully, including any new risks that may arise. Furthermore it is important for the Board to know how they are going to deal with the risks they have identified as being unacceptable. Consequently, according to King [3], it should also be the responsibility of the Board to decide on the appropriate risk strategy that their

organization should follow. These strategies include risk acceptance, risk avoidance, risk transference and risk mitigation, as discussed earlier.

The chosen risk strategy should satisfy the risk appetite of the organization. It is the responsibility of the Board to decide on this risk appetite i.e. the amount of risk an organization is willing tolerate [3]. Once the Board has decided on an organization's risk appetite and an appropriate risk management strategy has been chosen to deal with its risks, the Board then has the responsibility of creating policies and procedures that complement the chosen risk management strategy, which should be communicated to all employees within their organization [3].

The King Report [3] further explains that the application of these policies and procedures needs to be monitored by the Board in order to elucidate their utility with respect to managing existing risks as well as exposing any new risks that may arise. In order for the Board to become aware of all risks in an organization, the King Report[3] points out that the Board needs to receive reports on their organization's risk management efforts. This is made possible through conducting an annual risk analysis exercise, which has been said to inform the process of risk management [6].

By implementing a regular risk analysis activity, an organization's risk management endeavors will be synchronized and up to date with its current risk environment. When an organization's risk management practices are sound and produce value, this will generate competitive advantage, making such an organization more attractive as a potential investment opportunity [3].

Clearly the responsibilities of the Board with respect to their risk management endeavors are quite numerous. Such an immense responsibility requires much information and communication on various aspects of risk but correct reporting on the risks affecting information is a challenge. If the Board is to oversee the entire process of risk management, they need something comprehensive to base their decisions on. Reports about various aspects of information related risks need to have sufficient scope to enable the Board to fully understand the entire spectrum of risks they may face in this regard. In most organizations the Board of Directors is accustomed to well formatted financial reports, which inform them of any financial risks that need to be considered. However, the Board needs to consider any non-financial risks that may present a potentially negative outcome. These non-financial risks may refer to risks encountered as a result of a dependence on IT amongst others. Risk management from an IT perspective should be based on fulfilling the three security requirements as enumerated earlier. These security requirements include firstly, requirements to protect the IT infrastructure; secondly, legal, regulatory and statutory requirements and thirdly, requirements for information integrity, confidentiality and availability as identified by an organization. Risk management from an IT perspective should produce sufficient information that can be reported to and considered by the Board. This will ensure that they are fully in control of the total process which constitutes risk management from an information protection perspective. However, do these reports provide the Board with complete information to satisfy the full scope of their responsibilities as far as the process of risk management from an information protection perspective is concerned?

In the next section the responsibilities of the Board with regard to managing information related risks are weighed up against the capabilities of IT risk management.

This aims to ensure the protection of information, in order to clearly spell out in information protection terms, what risk management actually means.

5 THE MANAGEMENT OF RISK

It was mentioned earlier that IT risk management, which should provide protection to an organization's information assets, only seems to deal with the risks facing the IT infrastructure. This statement can be clarified by examining the definitions of risk analysis and risk management. Protecting assets by reducing vulnerabilities to prevent threats from damaging these assets is characteristic of ensuring the security of the IT infrastructure. Moreover Frosdick [6] suggests that risk analysis informs the process of risk management and since risk analysis is only concerned with issues of security for the IT infrastructure, this suggests that risk management merely focuses on the infrastructure. The definition of risk management according to BS 7799 [13] is that it is a "process of identifying, controlling and minimizing or eliminating security risks that may affect information systems, for an acceptable cost". Even though risk identification is considered to be a part of risk management in this instance, the definition clearly suggests that merely the infrastructure is considered, since only risks that affect the information systems seem to be taken into consideration. Could the information produced by such risk management activities really be sufficient for use by an organization's Board of Directors, assisting them in fulfilling their total risk management responsibilities as far as the protection of information is concerned?

The security requirements of an organization include three aspects, not just requirements to protect the IT infrastructure. The other two aspects which include legal, regulatory and statutory requirements, and requirements for information integrity, confidentiality and availability are not necessarily threat driven like the first. This is due to the fact that they are not required because of the affects of some threat that could manifest. They are requirements as stipulated by the law and the organization. Since risk management can be considered to focus only on one aspect of these requirements, how can it be considered effective in dealing with all risks, this being the responsibility of the Board of Directors [3]? The Board of Directors needs to be made aware of any legal risks that may exist with regard to the protection of information, as well as risks resulting from a compromise of information integrity, confidentiality or availability. More than what is termed risk management is thus needed when reports on the issue of risks to information are concerned.

The Board should be responsible for the total process of managing risks. This total process should include legal aspects as well as non-financial aspects. Frosdick [6] terms this total process by which all risks are analyzed and managed as the "management of risk". Therefore it can be said that since the Board is responsible for the total process of managing all risks as stated according to the King Report [3], they are actually concerned with issues regarding the management of risk, and not risk management. IT Risk management does indeed still have a part to play in assisting the Board in managing some of the risks affecting information, but only as a component, since it seems to focus only on the IT infrastructure. The Board needs to address all three aspects of security requirements in order to ensure that all aspects of risk associated with the protection of information are dealt with effectively and that they maintain control over the process of the management of risk.

Figure 1 illustrates an adaptation of the model for the management of risk as defined by Frosdick [14]. This model suggests that the Board is actually concerned with issues regarding the management of risk, since they need to consider all three aspects of security requirements as identified by BS 7799 [13]. Additionally, they must adhere to the stipulations of the King Report [3] if they wish for their organization to remain stable and competitive. Hence it is unsatisfactory where reports to the Board, regarding the protection of information, are concerned.

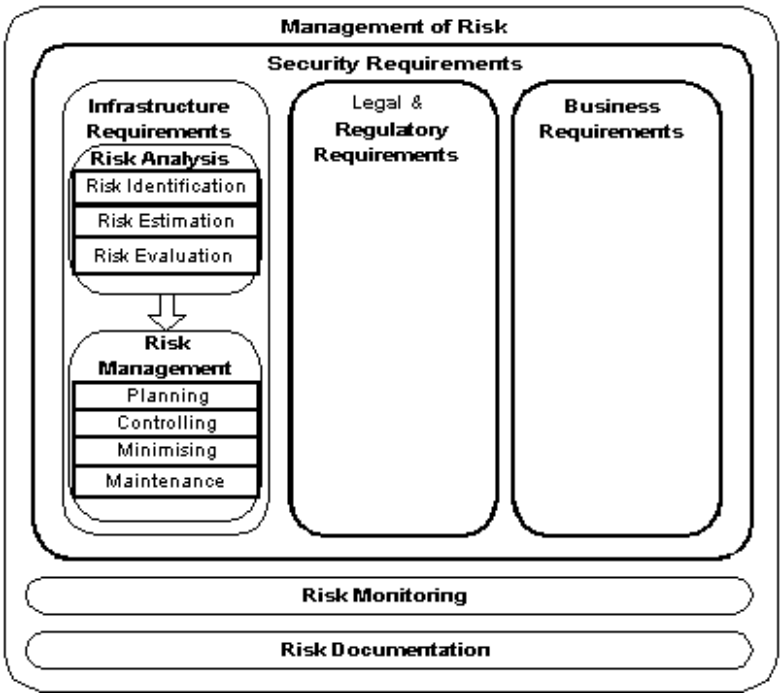

Figure 1: A model depicting the management of risk.

6 CONCLUSION

This paper argued that risk management from an information protection perspective focuses merely on the IT infrastructure, but the Board, who is responsible for managing all information related risks, requires more than this. They need to know about any legal and business risks that may affect their information assets. According to the argument presented in this paper, and presented in figure 1, reporting comprehensively on risk to the Board actually refers to the concept of management of risk. The management of risk refers to the comprehensive, all inclusive process of addressing all risk related areas. Reporting on risk management to the Board, could be interpreted as merely reporting on IT related risks. Though, it is very important that reporting to the Board is extensive enough to indicate all aspects that can possibly pose a risk to organizational information.

Further research would involve identifying what the content of the information that must be reported to the Board should consist of and in what format should it be

presented to the Board in order for them to fulfill their responsibilities in terms of the management of risk.

7 REFERENCES

[1] Bob Blakley, Ellen McDermott, and Dan Geer. Information security is information risk management. In *Proceedings of the 2001 workshop on new security paradigms*, pages 97–104. ACM Press, 2001.

[2] Terry Simister. Risk management: the need to set standards. *Balance Sheet*, 8(4):9 – 10, 2000.

[3] King Report. *The King Report on Corporate Governance*. Institute of Directors, Available from: http://www.iodsa.co.za/IoD

[4] Michael E. Whitman and Herbert J. Mattford. *Principles of Information Security*, chapter 5, pages 153 – 190. Course Technology, 2003.

[5] F. J. Heemstra and R. J. Kusters. Dealing with risk: A practical approach. *Journal of Information Technology*, 11:333 – 346, 1996.

[6] Steve Frosdick. The techniques of risk analysis are insufficient in themsleves. *Disaster Prevention and Management: An International Journal*, 6(3):165–177, 1997.

[7] Paul McKoen and Leo Gough. *The Financial Manual for Non-Financial Managers*. Pitman Publishing, 1997.

[8] Mariana Gerber and Rossouw von Solms. From risk analysis to security requirements. *Computers and Security*, 20(7):577–584, 2001.

[9] Kakoli Bandyopadhyay, Peter P Mykytyn, and Kathleen Mykytyn. A framework for intergrated risk management in information technology. *Management Decision*, 37(5):437–445, 1999.

[10] Gary P. Schneider and James T. Perry. *Electronic Commerce*, chapter 6, pages 193 – 236. Course Technology, second edition, 2001.

[11] Richard Baskerville. Information systems security design methods: implications for information systems development. *ACM Computing Surveys (CSUR)*, 25(4):375–414, 1993.

[12] Ida M. Flynn and Ann McIver McHoes. *Understanding Operating Systems*, chapter 1, pages 3 – 16. PWS Publishing, second edition, 1997.

[13] BS 7799-1. *Information Security Management - Part 1: Code of practice for information security management*. British Standards Institution, 1999.

[14] Steve Frosdick. Practical management of programme risk: the case of the national strategy for police information systems for england and wales. *Information Management and Computer Security*, 4(5), 1996.

[15] ISO/IEC TR 13335-2. Guidelines for the management of IT security (GMITS) - part 2: Managing and planning IT security. Technical report, ISO/IEC, 1997.