RHODES UNIVERSITY

An Investigation into the State-of-Practice of Information Security within Zambian Copper Mines – A Case Study

A thesis submitted in fulfilment of the requirements for the Degree of

MASTER OF SCIENCE

of

RHODES UNIVERSITY

by

CHISHALA LUKWESA

November, 2010

Abstract

Zambian copper mines have embraced the use of information technologies for strategic operations and competitive advantage. This dependence on these technologies has not only been seen in the physical aspects of business operations but also in the use of information systems such as Enterprise Resource Planning Systems (ERPs) for strategic decision making and increased usage of Industrial Control Systems (ICS') that are meant to enhance operational efficiency in production areas.

A survey was conducted to explore leadership perceptions on information security practices in Zambian copper mines and an ISO/IEC 27002 Audit Tool was administered to middle management in a particular mine for an in-depth analysis of their information security practices.

Results revealed that although information security controls may have been put in place in these organisations, there are still areas that require attention. Senior management and middle management have different perceptions as to the extent to which information security practices are conducted in these copper mines. This implies that management may not be fully involved in certain aspects of these organisations' information security practices. The results concluded that management needs to be fully involved and provide support for information security programs. Furthermore, these information security programs should be standardised so as to effectively protect these organisations' information assets. This should also include the involvement of personnel as key players in the information security process.

Dedication

To my late father, Grenson Hector Lukwesa Mpandamabula. I have fulfilled one of your last wishes. I am sure the other one is on its way.

Acknowledgements

I would like to thank the following for their support and contribution towards the success of this research:

My supervisor Chris Upfold - I could not have asked for a better supervisor. Your enthusiasm towards this research made me even more eager to keep going and get the results. You are indeed a “model” supervisor.

My family - for your incessant love and support through each day of my life.

The Beit Trust Trustees – without your financial and moral support, this would not have been possible. Thank you.

All respondents from the Zambian copper mines for your valuable feedback.

Patrick Mkandawire - your invaluable mentorship will forever go a long way.

Veronica Aulelyo Chitoloma - your cibobo, kept me going every day, day and night. I can never thank you enough.

To all my friends, colleagues, who in every special and unique way contributed to my research, I am truly grateful for your support. Tafadzwa, Bridget, Rirhandzu and Pimani, I cannot thank you enough for being there for me.

My LORD – as promised, I found your “footprints in the sand”.

Declaration

I acknowledge that all references are accurately recorded and that, unless otherwise stated, all work herein is my own.

C. Lukwesa

Table of Contents

List of Tables

List of Figures

Chapter 1

Research Introduction

This chapter introduces the research problem. This is achieved by describing the research area and showing how it relates to the research problem on a general level. This chapter also presents a summary of the results and explains the organisation of this thesis.

1.1 Introduction

Information possessed by an organisation is used by a variety of people who include the employees, customers and stakeholders (Botha and von Solms, 2004). As a result of this, in order for the organisation to maintain its image, competitive advantage and high operational levels, information has to be readily available, kept confidential, possess a high level of integrity and not find itself in the wrong hands especially when outsiders also need to have access to it (Dhillon, 2001: 1). For this to happen, an information security program which provides the broader picture of the information security process in an organisation has to be put in place. Information security policies form the cornerstone of the program (Peltier *et al.,* 2005: 55). According to Whitman and Mattord (2009: 174), these policies are strengthened by information security standards. This in turn ensures effective security of information, information systems and all the media and facilities that process and maintain information vital to the organisation's operations (Rittinghouse and Rittinghouse, 2005: 193).

1.2 Research Context

Copper mining companies in Zambia whose history can be traced from as far back as the early 1900s (Yachir, 1988: 9), have mostly had their corporate energy directed towards copper production in an attempt to ensure that production is ongoing as far as possible, day and night, the whole year round. This intensive process implied that technological efficiencies had to be evolved to sustain and provide for a more competitive landscape. The adoption of technology has led to increased efficiency and greater reliance on the use of information for strategic operations (World Stonex, 2006).

According to Porter (2008: 78), most of industrial history's technological progress principally affected the physical component of what businesses do. However, information technology capabilities have been advancing faster than technologies for physical processing (Davenport, 1993: 73). This means information processing boundaries have also expanded (Porter 2008: 78). Hence the mining industry has also found itself in that position. The industry has since evolved and business has become multifaceted and information rich (Parak, 2008). Indeed, according to Knights and Daneshmend (1998: 4), there has been increasing need for ready access to consolidated historical databases to make informed decisions as mining information originates from various data sources.

Mining operations are driven by high standards that often lead to Safety, Health, Environment and Quality (SHEQ) certifications, as well as the need to comply with regulatory frameworks (GRZ, 2000). It is critical that information required for these operations is accurate, reliable and accessible to those who need it. This forms the basis for information security. A case study conducted by Akaner (2003: 29), on the application of ISO 9000 and OHSAS 18000 in the mining industry, revealed that the three primary goals of information security (confidentiality, integrity and availability) that form the information security triad, are required to make informed decisions.

Effective information protection requires a comprehensive approach that takes into consideration a variety of areas within and outside the Information Technology (IT) area (Chang and Yeh, 2006). According to Peltier *et al.* (2005: 4), the information security process must move beyond the narrow scope of IT and address issues of enterprise-wide information protection in order for it to be effective. The fundamental element of this enterprise-wide program is an information security policy that is part of the corporate policies and does not come from IT (Peltier, 2002: 3).

Several organisations already have security blueprints in place which form the basis for the design, selection, and implementation of all security policies, education, and training programs, and technological control (Whitman and Mattord, 2009: 186). However, policies alone do not offer the user community the guidance necessary to design and implement them to effectively address threats and meet the organisation's objectives. This support and guidance is provided by standards as they are mandatory activities, actions, rules, or regulations designed to provide policies with the reinforcement required for them to be effective. Therefore, the information security process should be modelled to conform to these standards (Peltier, 2002: 70).

The development of an information security policy should take into account the organisation's objectives, regulatory requirements, key business processes and management priorities (Purser, 2004: 135). The choice of standard(s) to complement the policy, according to Purser (2004: 144), can either be internal or external. External standards include national and international standards, whereas, internal standards are specific to an organisation. The use of international standards in an organisation also enhances confidence in inter-organisational business relationships (von Solms, 1999).

One of the policy priorities of the thirteen (13) pillars of the Zambian National Information and Communication Technology (ICT) policy which was launched on 28th March, 2007, is securing information in all sectors including the public and private sector. The goal is to safeguard national, institutional and individual security concerns in order to support the development, deployment and effective use of ICTs within the Zambian economy and society at large. The National ICT policy is meant to set a framework for Zambia's participation in the global economy and applies to a cross-section of organisations in the country (Ministry of Communication and Transport, 2006: 51).

The main focus in the mining industry is preservation by securing organisational information to ensure continuous operation of the business with little or no disruption or loss of data. Thus, the level of common standards of the information security process implemented in the organisation needs to be stringent as the mining industry requires top standards for qualification, certification and adherence with relation to mine SHEQ in accordance with Zambia's mining regulations and International Organisation (ILO) standards (Starke, 2002).

Furthermore, while information security policies and standards may enhance information security in an organisation, they may not be adequate for achieving the desired level of information security. While standards provide the necessary principles, concepts and components for an information security program, the key factors for the success of this program include senior management commitment and organisation-wide information security awareness (Kajava *et al.*, 2006b; Kolkowska, 2005). This is because the business function has become multifaceted and now involves individual behaviour, and organisational and managerial aspects in addition to technology and information networks which were previously the main focus of information security (Kajava *et al.*, 2006b; Kolkowska, 2005; Anttila, *et al.*, 2004).

Senior management have, however, been known to have an apparent understanding of IT and information security which may lead them to make decisions that may not be suitable for the enhancement of the organisation's level of information security (Kajava *et al.*, 2006b). Their perceptions of information security which may be different from actual practices or information security needs in the organisation may arise from information security not being regarded as a strategic instrument (Lindström and Hägerfors 2009). Cooper (2003) defines perception as "*...the mechanism with which a person evaluates inputs from the external*

environment, which, in turn, determines his/her own behavioral response". Therefore, their level of commitment and contribution to information security will only be as much as their understanding of information security management. A study conducted by Kajava *et al.* (2006a) revealed that although international standards for security management are a significant factor in achieving competitive and strategic advantage, a deep knowledge of modern business environments, sound business management practices, and fundamentals of managing information security are required for this to be achieved.

The ISO/IEC 27002 (also known as ISO 27002) standard will be used in the study as it is non-vendor specific and sector-neutral (Calder, 2006: 53) and covers more aspects of information security than other standards (Bacik, 2008: 40). A number of Zambian mining companies are already ISO accredited (Konkola Copper Mines, 2007; BOPA Daily News, 2001), or working on it, hence, the use of an ISO information security standard for the study will complement the practices that are already in place.

In view of this, this research aims to investigate the state-of-practice of information security in Zambian copper mines taking into account the role that senior management plays in the effective management of information security in these organisations. The research seeks to answer the following questions:

i. Are information security programs in Zambian copper mines effectively implemented?

ii. Do the information security practices and programs found in Zambian copper mines follow a particular standard?

iii. Is senior management actively involved in the information security process in Zambian copper mines?

iv. How does senior management perceive information security in Zambian copper mines?

v. Would the implementation of the ISO/IEC 27002 in Zambian copper mines enhance the effectiveness of information security in these organisations?

vi. What key factors are required to effectively implement information security in Zambian copper mines?

1.3 Goals and Objectives of the Research

The goal of this research is to investigate the use of ISO/IEC 27002 as the foundation of information security in Zambian copper mines. In doing so, the research will:

- Investigate the use and nature of information systems currently used by Zambian Copper Mines
- Identify the risks that may be associated with information systems within these mines
- Explore the perception of information systems security compliance held by both senior management and operational middle management within these organisations
- Explore the extent to which the ISO/IEC 27002 standard addresses information security concerns raised within the literature review
- Identify those information security concerns found within the 11 Domains of the ISO/IEC 27002 standard that require particular attention.

1.4 Research Methodology

The research was conducted by means of an instrumental case study. The case study was used in view of the fact that an intensive study representative of the population in question was required. Multiple sources were employed to gather the data. According to Yin (2003: 7), the case study method is applied when a variety of sources are employed to gain a deeper understanding of the phenomenon in question. It is also applied when a "how" or "why" question is being asked about a contemporary set of events. Interpretive and positivist paradigms were adopted as both qualitative and quantitative analysis methods were employed in the case study. Carter and Presnell (1994: 2) suggest that each paradigm may require the use of different research methods or a combination of methods to meet research goals. Research methods are, therefore, no longer automatically associated with a single paradigm. Quantitative analysis complements the findings from

qualitative analysis. According to Bröring (2006: 127), the overall intention of using both methods is to determine whether the patterns detected in qualitative data can also be found in quantitative data, thereby substantiating findings. This research was limited to copper mining organisation in Zambia.

Research steps:

- Conduct a literature review in order to synthesise information security elements and practices as well as identify the levels of common standards of information security practices in the mining sector. A theoretical framework for identification of appropriate information security standards for the mining sector will also be created as part of the review.
- By means of a survey using questionnaires, explore leadership perceptions surrounding information security practices in Zambian copper mines.
- By means of an ISO/IEC 27002 information security audit, conduct an in-depth review of information security policies and programs in one Zambian copper mine, in order to identify the information security gaps that exist in that organisation.
- Conduct interviews with senior management and personnel in charge of infrastructure in the mine where the audit tool was administered.
- Using the results obtained from the audit, survey, and interviews, propose a framework outlining information security best practices for Zambian copper mines in accordance with the ISO/IEC 27002 standard.

1.5 Summary of Results

The key results of the thesis are summarised as follows:

- Information security is vital to strategic operations and competitive advantage in Zambian copper mining organisations. This can only be achieved by effective implementation of information security programs.

- A successful information security program requires complete management commitment and support. Information security governance should, therefore, be made part of Zambian copper mining organisations' governance structure. Furthermore,

mobile security governance should also be implemented as the use of mobile devices in these organisations has expanded.

- Personnel who include employees, contractors, and third-party users are a critical component of these organisations' information security programs. They either make or break an information security program and should, therefore, be the key players in these programs.
- Standardised information security programs are necessary for effective implementation of information security in Zambian copper mines.
- Risk management is an important aspect of the information security process. A complete and up-to-date inventory of all information assets is, therefore, vital for an effective risk management process.
- Industrial control systems require as much protection as other corporate systems as they are an equally important part of information systems in Zambia copper mines.

1.6 Organisation of Thesis

Chapter 1: Research Introduction

This chapter introduces the research, provides the research context and identifies the goals of the research. The research methodology is also introduced. Furthermore, a summary of the research results is presented.

Chapter 2: Information Systems and the Mining Sector

This chapter introduces information systems and the mining industry. The use of information systems in the mining industry is also discussed.

Chapter 3: Information Security

Threats that emerge as a result of the use of information systems are identified. These threats are further narrowed down to those that affect the mining industry.

Chapter 4: Risk Management

The process of managing threats identified in chapter 3 is discussed. The information security risk management process in the mining industry is also described.

Chapter 5: Contingency Planning

This chapter discusses contingency strategies that are put in place to minimise interruptions to business operations and enable full restoration of critical business processes as quickly as possible. Contingency strategies in the mining industry are also discussed.

Chapter 6: Information Security Governance

This chapter discusses information security governance and how the mining industry handles information security governance issues.

Chapter 7: Information Security Standards and Models

This chapter provides a description of information security standards and models. It further discusses the applicability of these standards and models to the mining industry.

Chapter 8: Information Security in the Mining Industry and ISO/IEC 27002

Information security concerns that are highlighted in the literature review are reviewed and mapped to the information security controls and domains of the ISO/IEC 27002 standard.

Chapter 9: Design of Experiment

This chapter discusses the research design and describes the administration of the processes of data collection and analysis.

Chapter 10: Analysis and Results

This chapter discusses the results that were obtained from the data collection process outlined in chapter 9 and provides an analysis of the results obtained, thereof.

Chapter 11: Recommendations

Recommendations meant to bridge information security gaps identified in chapter 10 are provided from the findings of the results discussed in chapter 10.

Chapter 12: Conclusion

This chapter concludes the research and lists the contributions the research has made. Areas of future research are also indicated.

Appendix A: Leadership Perception Questionnaire Part – A

The Leadership Perception Questionnaire administered to senior management in Zambian copper mines is provided.

Appendix B: Leadership Perception Questionnaire Part – B

The Leadership Perception Questionnaire administered to Heads of Information Technology in Zambian copper mines is provided.

Appendix C: Praxiom ISO IEC 27002 Information Security Audit Tool Questionnaire 1

Questionnaire 1 of 11 of the Praxiom ISO IEC 27002 Information Security Audit Tool is provided.

Chapter 2

Information Systems and the Mining Sector

This chapter introduces information systems, the mining sector, as well as the integration of information systems into mining operations. Building blocks of information systems are also discussed. It also describes the benefits that are derived out of well implemented and maintained information systems bearing in mind the risks that arise from the usage of such systems.

2.1 Introduction

Information systems form an integral part of any organisation as they play a critical role in business operations and management activities at a tactical and strategic level (Cano, 2002: 2). The effectiveness of an information system is measured by the quality of information it produces. Information, therefore, needs to be accurate, relevant, up to date, complete, timely, well-presented and cost-effective (Wessels *et al*., 2007: 169). Organisations are now increasingly integrating information systems into their operations, but benefits are only realised if these systems are strategically integrated into operations (Tusubira and Mulira, 2004; Szymanski *et al.*, 1995: 20). Currently, most organisations are making use of information technologies and information systems in one way or the other. The mining industry has also seen a shift from traditional operations to more information-oriented mining operations (Parak, 2008).

2.2 Information Systems

Information systems have now become part of every day use both in homes and organisations such that users sometimes do not actually realise the extent of their dependence on them. A dishwasher in a home makes use of an information system just like the use of an Automated Teller Machine (ATM) to withdraw money makes use of the same. The role of information systems and IT in organisations has dramatically changed over the years as the industry-based economy has also experienced a shift to an information and knowledge-based economy. This has over the years changed the manner in which organisations conduct business. (Cano, 2002: 2).

According to Montana and Charnov (2000: 453), the latter half of the 20th century is most likely to be regarded as the information age as it has seen a major transformation in the manner in which information is being used in organisations. Information is now seen as an asset of great value which is now used to make strategic decisions and provide competitive advantage. IT alone is not useful to an organisation until it becomes part of the information system as these systems are not only concerned with equipment but also people and their actions (Heeks, 2001: 15).

In order to better appreciate information systems, it is important to understand what data and information are, as well as what makes up a system. Stair *et al*. (2008: 5) define data as *"raw*

facts". They further define information as *"a collection of facts organised in such a way that they have additional value beyond the value of these facts themselves".* A system is a set of components that are linked together and impact each other in some manner (Li, 2005: 69). An information system, therefore, as defined by Laudon and Laudon (2005: 8) is *"a set of interrelated components that collect (or retrieve), process, store and distribute information to support decision making and control in an organisation".*

Lehtinen *et al. (*2006: 99) discuss the different types of information that exist in organisations. These include personnel records, corporate records and national defense information. The criticality of information in a particular organisation depends on the value that is accorded to it as it varies from organisation to organisation due to different industry types.

2.2.1 Components of Information Systems

Computer-based information systems are made up of various components. These include computer hardware and software, databases, telecommunication systems, human resources, data, and procedures (Szymanski *et al*., 1995:17; Encyclopaedia Britannica, 2009). Information system components in an organisation can, therefore, be broken down as follows:

- **Data:** This is the initial object of input into an information system for the purpose of processing. (Shim and Siegel, 2005: 3). Although data is a critical resource in organisations, it is not useful until it is processed into information. (Thuraisingham, 1997: 1).

- **Computer Software:** These are the computer programs that are used for information processing. System software provides a means of communication between the hardware and application software while application software caters for users' individual data processing needs (Shim and Siegel, 2005: 3; Wessels *et al*., 2007: 33).

- **Computer Hardware:** This is a set of devices such as processors, keyboards, monitors and printers which accept data, process it, display it for the user's benefit and also provide storage for data and information in the form of databases (Rainer *et al*., 2007: 6; Wang and Taratorin, 1999: 11).

- **Databases:** As data and information in an organisation are synthesised from various sources, databases are required to organise data and information into a form that is useful for future forecasts and planning (Ward and Dafoulas, 2006: 2).

- **Telecommunications Systems and Networks:** Telecommunications help people communicate using various methods such as electronic mail and voice mail and enable an organisation's users to access the Internet (Laudon and Laudon, 2005: 266).

- **Human Resources:** These are the most important component of an information system as they are users of the data, information and information systems (Peterson *et al*., 2001: xviii). These users who range from top executives to people in operations need to be trained and made aware of the risks and threats associated with information systems in order for them to effectively use them and achieve the desired results. (Laudon and Laudon, 1995: 10).

- **Procedures:** These are rules, policies, methods and strategies by which users of information systems abide. Procedures are part of an organisation's information security program and tell users how to operate and use an information system (Szymanski *et al*., 1995: 17).

2.2.2 Business value of Information Systems

Information systems provide the organisation with the capability to store, process, and transmit data in order to provide support and improve efficiency of operations. They also help organisations produce information more reliably and quickly enough for them to make accurate strategic decisions (Galliers and Leidner, 2003: 1). Firms need to be concerned about their ability to compete with other firms in order for them to stay in business. Efficiency of labour and capital employed in the business is increased through improvement and sometimes the creation of new business processes brought about by information systems (Laudon and Laudon, 2005: 486).

Porter (2008: 74) describes how the information revolution has changed the way organisations conduct business. This change gives them competitive advantage as benefits towards operational objectives are derived out of information systems. These benefits include cost efficiency, product quality, human talent and profitability (Montana and Charnov, 2000: 138). An airline reservation system available on the Internet for any potential passenger to

make a booking, from anywhere in the world, at anytime of the day, takes advantage of global trading opportunities, reduces processing time and enhances competitive advantage (Netmedia, 2008).

2.3 The Mining Sector

There are two types of copper mines in existence. These are underground mines and surface mines (Polar Inertia: 2003). The method of mining typically depends on the distance of the ore body from the surface. Mining operations range from exploration to ore-processing to sale of the processed ore.

Copper mining in Zambia contributes largely to the country's economy. Zambia prides itself in being Africa's top copper producer (Mining Weekly, 2009) and one of the highest copper producers in the world (CRI English, 2009). For more than half a century, Zambia's economic backbone has been the copper mining sector (Ministry of Mines and Minerals Development, 2009). Hence, a lot of emphasis is placed on the smooth operations of the mines. To this effect, several regulatory measures such as the Mining Regulations of 1973 and the Mines and Minerals Act of 1995 (GRZ, 2000) have been put in place.

2.4 Information Systems in the Mining Sector

Mining is the process of exploration (location of the ore-body), extraction (removal from the ground) and processing (isolating the ore) (Dodgson and Vandermark, 2000). The finished product in the mining process is then marketed and sold. Mining is a strategic industry which contributes to both local and international economies (Teseleanu *et al*., 2006). The industry has often been considered a low-tech, low innovation industry hence information technologies have not been well appreciated (Upstill and Hill, 2007). The industry is, however, best understood as a scale-intensive innovative industry with its own characteristics (Pavitt, 1984). Although argued to be slow-changing and somewhat traditional, the face of the industry has been seen to change and this change has been seen in the timing of mining information which is becoming indispensable to sound policy making, strategy and forecasts for future changes (Sawada, 2004).

In their article on data management in the minerals industry, Pincock Perspectives consultants (2005a; 2005b) discuss the extent to which information management has become a large part of mining operations. Data is collected in many forms, from many systems in

various operations within the mines. The sources and types of data come in three (3) different forms, namely:

i. **Unstructured data**, representing the majority of data in the organisation, typically identified as emails, personal knowledge and notes.

ii. **Structured data**, organised in a known form such as a table in a database.

iii. **Metadata**, though often neglected, describes the properties or characteristics of other data to makes it more understandable. Cost accounts in an accounting system are a good example of metadata.

According to Knights and Daneshmend (1998: 3), software used in the mining industry includes both generic industry applications as well as applications specific to mining. Generic applications include Computer Aided Design (CAD) systems, Geographic Information Systems (GIS), Accounting, Payroll and Human Resource Management Systems, spreadsheets, databases, word processors, inventory and purchasing, project management systems, and process control applications. Specialised systems include mine planning, mine dispatch, production control, geotechnical and geological modelling systems (Knights and Daneshmend, 1998: 3).

The ability to carry out data conversion functions such as collection, processing, transmission, and display have been made possible by the computer (Atkinson, 1992: 1360). Computer techniques have become part of everyday mine design, planning and operation and these processes have been altered further by computer technology. High resolution graphics and powerful processors have led to the optimisation of mine planning (Zhang *et al*., 2001: 333-334). In surface mining, for example, there are few areas if any that can be identified as not making use of microcomputers (Atkinson, 1992: 1361).

In view of harsh operating environments in most areas of mines, the quality of hardware is as important as that of software (Atkinson, 1992: 1360-1361; Falco *et al*., 2002). Therefore, use of hardware specifically built for the mining industry is preferred. The usage of microcomputers in most mining operations has increased and their processing power has also become significant due to the increased capacities of the software used in the industry. According to Kizil (2003), these advances in hardware and software have also enhanced the

adoption of Virtual Reality (VR) in the minerals industry for the benefit of data visualisation, accident reconstructions, simulation applications, risk analysis, hazard awareness and training.

Atkinson (1992: 1360) attributes enhanced processing ability of mining equipment for intelligent decision making to improvements in telecommunications and networking. Furthermore, radio network links and radiowave communication are being used for both voice and data transmission in underground and surface mines (Atkinson, 1992: 1360). This data can be used for real-time scheduling, production monitoring and maintenance. The use of the Internet and email for communication has also been as widely adopted in the mining industry as in other industries (Denby and Schofield, 1999: 636).

Mining companies use a variety of information in their everyday operations. Due to a large number of sections both operational and production, different kinds of information and information systems are used within these various sections of the organisation. Information in mines is used by people both internal and external to the organisation. Wessels *et al.* (2007: 170) describe the users of information in an organisation as internal (within the organisation) and external (outside the organisation). Christmann *et al.* (2006) give a detailed view of the various stakeholders in the mines who either directly or indirectly use information found in the mine as shown in figure 2.1 below.

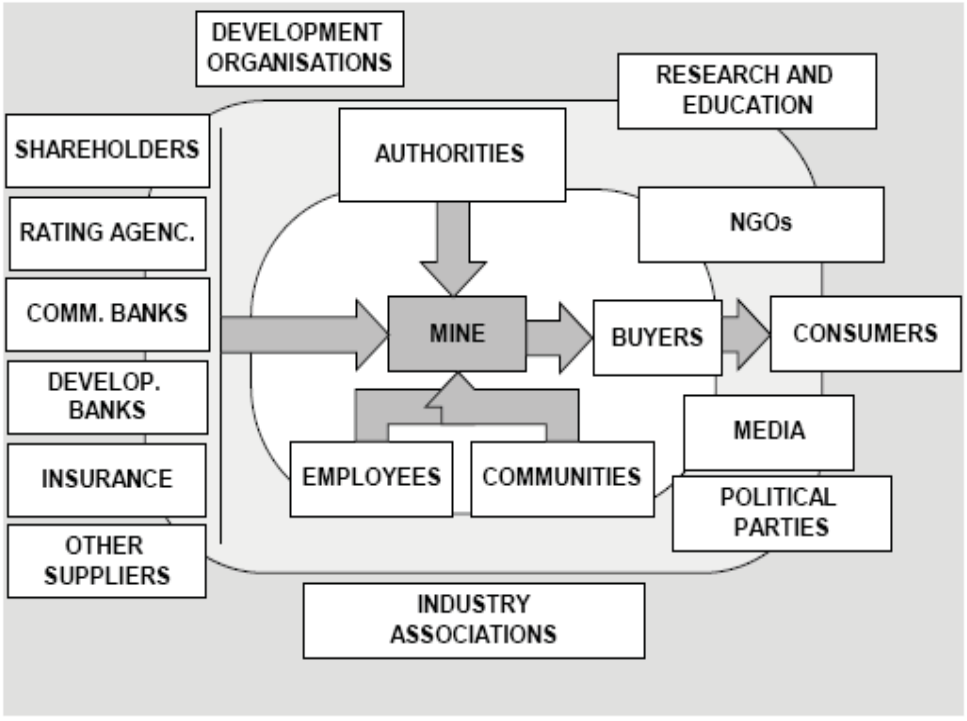

Figure 2.1: Mining Stakeholders (Christmann *et al.*, 2006)

- **Internal users:**
    - Employees, who are the end-users, application and system administrators as well as application programmers of the various systems. Information enables them to carry out their tasks more effectively.
- **External users:**
    - Shareholders, who require information about the organisation's performance and financial position for decision making purposes.
    - Government, which mandates that every organisation supplies it with certain information such as employee taxes, environmental reports, labour returns, production figures and statistical data on safety (GRZ, 1973: 111, 139, 140).
    - Financial institutions, who require certain information to be able to determine the organisation's financial capacity.

- Customers, who require information about the products sold by the organisation.
- Suppliers, who provide the necessary raw materials and services to the organisation.

Every copper mine in Zambia is in private hands (Rakner, 2003: 78), hence, it is inevitable that information is accessible to both internal and external users.

Mining operations run day and night (Hustrulid and Bullock, 2001: 51), hence, information critical to operations should always be available. Different operations and functions use different kinds of information and information systems for various purposes (Copans, 2007). The diversity of this information means each operation treats different kinds of information in different ways. According to NIST SP800-82 (NIST, 2008), typical IT information systems and their components are local and easy to access, whereas control systems which are found in the plant area are in most cases isolated and may require extensive physical effort to gain access to them. All these systems solve different organisational problems at different levels. Laudon and Laudon, (2005: 50) outline the different functional information systems that exist in organisations:

- Finance and accounting use information systems to manage financial resources, determine the best sources of funds, forecast revenues and business activity, perform audits, and ensure all financial reports and documents are accurate (Stair and Reynolds, 2008: 31).
- Sales and marketing information systems facilitate movement of goods from producers to customers and collect, process and make available marketing operations data to decision makers (Kroon, 1995: 477; Lucey, 2005: 267).
- Manufacturing information systems also known as production planning and control systems are used to coordinate the manufacturing process, monitor product quality, control inventory levels and develop production schedules (Stair and Reynolds, 2008: 31).

- Information systems are also used in human resources management for recruitment, job analysis and design, compensation, training and career development decisions (Davenport and Harris, 2007: 77).

- Legal information systems are used to develop reports and legal documents as well as analyse product warranties and liabilities (Stair and Reynolds, 2008: 31).

- Geographic Information Systems (GIS) are used in the mining industry for recording, analysing and visualising data that is spatially referenced (Mining News Premium, 2007). This spatial information is useful for mineral exploration, mine planning and production as well as environmental reclamation (Thorley and Blackwell, 2009). Examples of GIS include Gemcom® (Gemcom Software, 2009) and ARCView® (Esri, 2009).

Mining organisations usually integrate different information systems through the use of ERPs. These systems aid in the consolidation of mine data and information as data and information is usually dispersed in various computer systems. They also provide the necessary governance to a mining company's operations as ERPs specific to the mining industry exist (Copans, 2007).

Consolidation of information systems in ERPs is achieved by integrating information systems in major functional areas of the organisation into modules which include inventory control, product distribution, order tracking, accounting, finance, human resources, product planning, parts and material purchasing, finance and marketing (Sysoptima, 2005). Implementation of modules depends on an organisation's view of the modules' technical and economic feasibility. ERPs help reduce operating costs, support strategic planning and facilitate efficient day to day management (Monk and Wagner, 2008: 33).

The different ERP products applicable to the mining industry are shown in table 2.1 below:

Table 2.1: ERP Systems for Mining Companies (Satenstein, 2008)

Company	ERP Product	ERP Product Description
SAP	SAP ERP	Major ERP software for multinational operations
Mincom	Mincom Eclipse	ERP geared to mining industry
Microsoft	Dynamics-GP	Finance emphasis (mining industry customizations)
Epicor	Vantage ERP	Business performance management; customer relationship management; customer service management; financial management; planning and scheduling; product data management; production management; sales management; supply chain management
SAMSSA	SAMSSA	ERP for *small to medium enterprise* (SME) mining companies
Oracle	Oracle E-Business ERP	Generalized ERP system for manufacturing and mining

Coupled with ERPs, information diversity has also brought about Business Intelligence (BI) and data warehousing in an effort to bring together information from different repositories. This in turn helps organisations make quicker and more reliable decisions for competitive advantage (Davis, 2007; Mottola *et al.*, 2001).

The advancement of Information and Communication Technologies (ICTs) has brought about an increase in the use of technologies in operations such as remote control of dangerous activities and environmental monitoring. All these operations are benefiting from the use of information systems, thereby, making mining processes more effective (Dodgson and Vandermark, 2000).

With the passage of time, the industry has been presented with a number of technological challenges including the need to discover new mineral deposits to replace depleted ones, safer and efficient mining and processing methods, and step-change environmental impact process improvements (Wagner and Fettweis, 2001; Hitzman, 2002). The human factor has become equally important as they are required to be multi-disciplinary skilled to take advantage of emerging technologies and take more control over the equipment they are accessing (Peterson *et al*., 2001: xviii).

In as much as information systems have improved organisational productivity and efficiencies, they, like any other systems have their flaws. Information systems are liable to risk, vulnerability and threats especially with organisations growing dependence on them

(Hawker, 2000: 17). Threats range from technical, environmental and organisational factors coupled with poor management decisions (Laudon and Laudon, 2005: 522). There are several intentional threats to information systems such as virus attacks, Denial of Service (DoS) attacks and information manipulation by disgruntled employees. However, unintentional threats such as human error, computer system failures and environmental hazards also exist and can result in devastating consequences for an organisation. These threats can originate from both within and outside the organisation (Piccoli, 2008: 431). Hence, an organisation needs to put controls in place to protect all components of the information. Knowing potential information system threats is as important as understanding ways of defending the systems against these threats (Turban *et al*., 2002: 674).

Mining organisations deal with sensitive information such as water level records in the underground mine which must always be readily available and accurate enough for the organisation to make informed decisions. A study carried out by Tanser (2003) revealed how the effective use of a Slope Stability Radar (SSR) in an opencast mine can mean the difference between loss of lives and unplanned downtime due to the collapsing of a rock wall and saving lives and planning for downtime because the system was able to detect it on time. Controls such as policies and procedures minimise the risk of information being manipulated so that it can still add value to the business (Butler, 1998: 7).

2.5 Conclusion

Organisations are becoming more dependent on information systems for effective day-to-day operations at all levels of the organisation. The mining sector is no exception as it makes use of various information systems in its daily operations. All information systems in use in the mines contribute towards the mining process, from the exploration to the sale of the finished product which in the case of Zambian mines is copper. Information is an integral component of an organisation's strategic initiatives for survival (Deans *et al.*, 1994: 24). To this effect, management and control measures need to be put in place to ensure that data input is accurate, information systems reliable, and the information produced is accurate, timely, relevant, well-presented, cost effective, and complete. Only then will the organisation benefit fully from the use of information systems for effective and efficient operations.

Chapter 3

Information Security

Chapter 2 introduced the use of information systems in organisations and the mining sector in particular. It also discussed the growing dependence of organisations on information systems. This chapter looks at threats to information systems used in organisations and the need to secure these systems, narrowing down to the mining sector in particular.

3.1 Introduction

Information systems and the data they process enable the creation and movement of goods and services in an organisation. An organisation without data has no ability to record or trace its transactions and/or its ability to deliver value to its customers. It is, therefore, important to protect data that is in the process of being transmitted as well as data in storage (Whitman and Mattord, 2009: 40). Organisations usually implement and use information systems to enhance efficiencies without considering the effects of their usage which include threats. There is, therefore, a need to identify threats that arise and to devise ways of minimising or eliminating them. All information system components are vulnerable to threats (Pfleeger, 2003: 4).

3.2 Information Security

Wessels *et al.* (2007: 233) define security as *"freedom from danger or the condition of safety"*. According to Whitman and Mattord (2009: 8), information security is the protection of information and its critical elements, including the systems and hardware that use, store and transmit that information. ISO/IEC 27002 (2005) also defines information security as the preservation of confidentiality, integrity and availability of information. It further mentions the involvement of other properties such as authenticity, accountability, non-repudiation and reliability. Stanton (2006: 39) outlines three fundamental information security problems:

i. How to securely store, transmit and receive information.

ii. How to prevent unauthorised individuals from modifying information.

iii. How to keep information services available to those who are legitimately allowed to use them.

These three problems collectively refer to the three characteristics of information, namely, confidentiality, integrity and availability, otherwise known as security principles or security objectives (Stewart *et al*., 2008: 180; Flegel, 2007: 26). These characteristics combine to form the ***CIA Triad*** as shown in figure 3.1.

Figure 3.1: CIA Triad (Endorf, 2006: 23)

The characteristics mentioned above can overlap, be mutually exclusive or be independent of each other (Pfleeger, 2003: 10), as shown in figure 3.2. Information security should provide a balance amongst these three characteristics. The level of confidentiality, integrity and availability is dependent on an organisation's goals, objectives and requirements (McMillan, 2007: 110). An organisation will, therefore, have to prioritise which characteristics are more critical for the type of industry. A financial institution for example, focuses more on accuracy and integrity of information than confidentiality (McMillan 2007: 110).

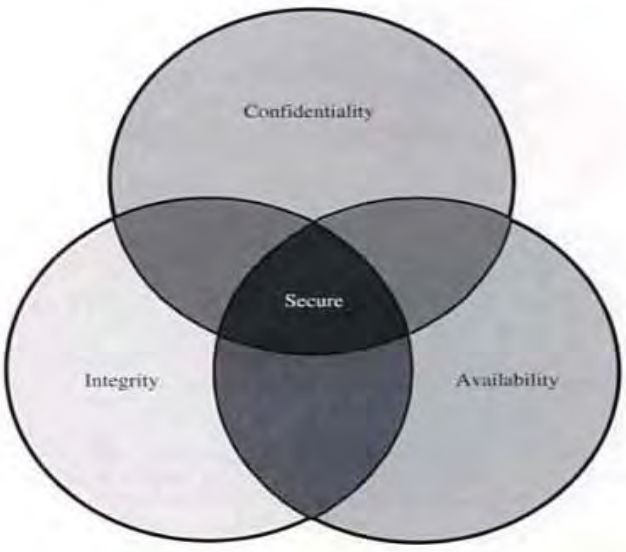

Figure 3.2: CIA inter-relationships (Pfleeger, 2003: 11)

Whitman and Mattord (2009: 8) argue, however, that the CIA triad by itself no longer adequately addresses the environment of the constantly changing computer industry and add

four (4) more characteristics to the three (3) tenets of the CIA triad. These are accuracy, authenticity, possession and utility. Stanton (2006: 39) further adds non-repudiation as another characteristic of information and information systems, turning the CIA Triad into CIA +NR.

Endorf (2006: 23) classifies business data as proprietary data used to gain competitive advantage, private data which refers to personal information, and privileged data which is issued to conform to legal requirements. Data classification depends on the owner of the information.

3.2.1 Information Security Objectives

Research conducted by Ma *et al.* (2008), revealed that six information security objectives were amongst the most cited across industries. These were confidentiality, integrity, availability, accountability, non-repudiation and authenticity as described below.

- **Confidentiality:** deals with non-disclosure or non-exposure of information to unauthorised individuals by restricting information that is in storage, being transferred or being utilised (Whitman and Mattord, 2009: 10; Carpenter and Barrett, 2007: 467). An organisation's security policy provides a guide as to which data or information is confidential (Johnson, 2007: 88).

- **Integrity:** Concerned with modification of information assets by authorised persons through the use of authorised methods (Pfleeger, 2003: 10). According to NIST 800-30 (NIST, 2002), loss of integrity reduces the assurance of an IT system as it could result in inaccuracy, fraud and incorrect decisions and may be the first step in an attack against the systems confidentiality or availability.
- **Availability:** concerned with system reliability, connectivity and stability as delayed recovery of a system from failure makes it susceptible to attackers and can result in loss of monies for the business (McMillan, 2007: 111).

- **Accuracy:** Information is accurate if it is free from errors or mistakes and provides the end user with the expected value (Whitman and Mattord, 2009: 10).

- **Authenticity/Authentication:** Information is authentic if it remains the same information that was originally created, placed, stored or transferred (Whitman and Mattord, 2009: 10). Users should also be authenticated before access to resources is given (Carpenter and Barrett, 2007: 468).

- **Utility:** This is the quality or state of having value in order to serve some purpose or end (Whitman and Mattord, 2009: 12).

- **Possession:** Possession involves having ownership or control of information. Removal of a copy of a backup tape by an employee who has quit his job for the purpose of selling customer records to competitors as an example of a breach of possession (Whitman and Mattord, 2009: 13).

- **Non-Repudiation:** Non-repudiation as described by Stanton (2006: 39) is a record of a transaction.

- **Accountability:** Deals with the ability to hold people responsible for their actions (NIST, 1995: 12).

- **Privacy:** Concerned with the control of sensitive information about stakeholders of an organisation. Organisations require a good information security program in order to protect the privacy of stakeholders who include the employees and customers (Stanton, 2006: 10).

Selection and prioritisation of security objectives, however, differ for each organisation. Table 3.1 provides an overview of the most common security objectives taken from various sources:

Table 3.1: Common Information Security Objectives

Security Objective	Sources						
	Whitman and Mattord (2009)	**Stanton (2006)**	**Ma et al., (2008)**	**ISO 1779:2005**	**NIST Handbook**	**ISF**	**GASSP**
Confidentiality	X	X	X	X	X	X	X
Integrity	X	X	X	X	X	X	X
Availability	X	X	X	X	X	X	X
Privacy		X					
Non-Repudiation		X	X	X		X	
Accountability			X	X	X	X	X
Possession	X						
Utility	X						
Accuracy	X						
Authenticity	X		X	X	X		
Reliability				X			

Findings from various sources reveal that the most common information security objectives are confidentiality, integrity, availability and accountability. This is in line with Ma *et al*.'s (2008) research findings. However, non-repudiation and authentication do not seem to be as highly prioritised as the other four security objectives. Privacy, though often emphasised is not one of the highly prioritised objectives.

3.3 Vulnerabilities and Threats to Information Systems

Threats of attacks on information systems have become so pervasive in organisations and institutions that they are now being accepted as part of doing business in the digital age (Conte, 2003). They can exist in different forms and target a variety of security issues (Conklin, 2009: 418). In order to apply appropriate controls to an environment, it is necessary to understand what the threats are and the consequences that would arise if those threats are to be realised (Tudor, 2006: 11).

With organisations' increased dependency on information technology, the consequences of information security breaches are quite high. In addition to losing money, an organisation may also suffer damage in the form of disruption of internal processes and communications,

negative impacts on reputation, goodwill and trust, loss of potential sales as well as loss of competitive advantage (Ma *et al.,* 2008).

According to Wessels *et al.* (2007: 233), vulnerability is a condition or a weakness in a system that could allow unauthorised access or damage to the system once it is exploited. Vulnerabilities exist in people, processes and technologies (Dattatreya, 2008). The level of vulnerability is impacted by factors such as the level of morale amongst employees, backup procedures, company profiles, types of information, level of employee proficiency, and history of prosecution (Peltier, 2001: 15). A threat is described by Wessels *et al.* (2007: 233) as a condition where vulnerabilities existing in a system could be exploited or result in damage or loss of information. A threat can also cause damage to a system and create a loss of confidentiality, integrity and availability if realised (Krutz and Vines, 2003: 321). As illustrated in figure 3.3, threats can be internal or external to the organisation. Both internal and external threats can either be intentional or unintentional.

Internal threats can be the most difficult to monitor and defend against as they usually come from users who have legitimate access to network resources. In the same way, external threats are more difficult to protect against when the company has provided access and is connected to the Internet (Newman, 2003: 11).

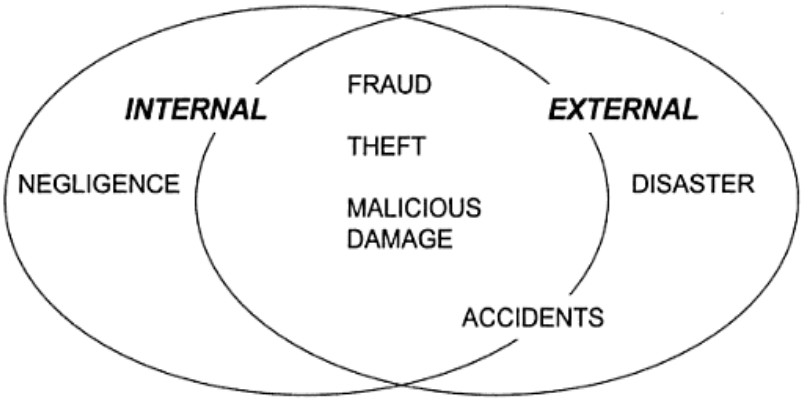

Figure 3.3: Internal and External Threats (Hawker, 2000: 29)

Due to an increased awareness of information threats, organisations have still continued to invest in information security even during times of economic pressures. A global survey conducted by Ernst & Young in 2008 revealed that 50% of respondents were increasing their

investment in information security as part of total organisational expenditure and only 5% were planning on reducing their investment (Ernst & Young, 2008).

3.3.1 Categories of Threats

Whitman and Mattord (2009: 42) refer to twelve (12) categories of threats, citing examples of each threat as shown in table 3.2. They suggest these threats present a clear and present danger to an organisation's systems, people and information. They further go on to say that categorisation of threats depends on the security level at which the organisation operates and the exposure to its assets.

Table 3.2: Categories and examples of threats (Whitman and Mattord. 2009: 42)

Categories of Threat	Examples
1. Acts of human error or failure	Accidents, employee mistakes
2. Compromises to intellectual property	Piracy, copyright infringement
3. Deliberate acts of trespass	Unauthorized access and/or data collection
4. Deliberate acts of information extortion	Blackmail or information disclosure
5. Deliberate acts of sabotage or vandalism	Destruction of systems or information
6. Deliberate acts of theft	Illegal confiscation of equipment or information
7. Deliberate software attacks	Viruses, worms, macros, denial-of-service
8. Forces of nature	Fire, flood, earthquake, lightning
9. Deviations in quality of service	ISP, power, or WAN service issues from service providers
10. Technical hardware failures or errors	Equipment failure
11. Technical software failures or errors	Bugs, code problems, unknown loopholes
12. Technological obsolescence	Antiquated or outdated technologies

Krutz and Vines (2003: 321) further suggest three (3) categories of threats; these are accidental loss, inappropriate activities and illegal computer operations, and external attacks.

Coupled with the CIA triad, another approach beneficial to the identification and categorisation of threats in information security is the STRIDE model which was also used by Microsoft for categorising threats (Casteele, 2005: 22). Schumacher (2006: 123) breaks down the acronym **STRIDE** into Spoofing Identity, Tampering of Data, Repudiation, Information Disclosure, Denial-of-Service and Elevation of Privilege. The STRIDE model categorises threats based on goals and purposes of the attacks.

- **Spoofing:** occurs when a user attempts to become another user or assume some attributes of another user (Ashbaugh, 2008: 76).

- **Tampering of Data:** occurs when users change information provided to them by an application for the purpose of disrupting normal routines (Schumacher, 2006: 123; Sodiya *et al.*, 2007: 54).

- **Repudiation:** occurs when a subject denies performing an action, causing an event or sending a message when records prove otherwise (Stewart *et al*., 2005: 159).

- **Information Disclosure:** involves disclosure of information to a user who does not have access to it (Sodiya *et al*., 2007: 54).

- **Denial-of-Service (DoS):** this is when an attacker sends a large volume of connections or information requests to a target. These requests overwhelm the system such that it fails to handle even legitimate requests (Whitman and Mattord, 2009: 66). Distributed Denial-of-Service (DDoS) equally sends large volumes of requests but these requests come from multiple computers at a time such that it is difficult to block the attacks (Newman and Tittel, 2003: 13).

- **Elevation of Privilege:** this is when a user gains more privileges on the computer than they are entitled to (Gollman, 2005: 11).

3.4 Need for Information Security in the Mining Sector

As described in Chapter 2, information in the mines is used by a variety of people, both internal and external to the organisation. Accurate information, therefore, needs to be accessed by the appropriate stakeholders. As such, information meant for shareholders should only be accessible to them just as that meant for financial institutions should only be made available to those institutions. This information should be available when needed and should be accurate enough for sound decision making (Avramenko and Thomas, 2000: 317).

Chapter 2 also discussed the various information systems and sources of data in the mining industry. All these are subject to vulnerability and need to be protected. Whitman and Mattord (2009: 39) list the four important functions which information security performs in an organisation:

i. The organisation's ability to function is protected.

ii. It enables the safe operation of applications which have been implemented on the organisation's IT systems.

iii. It safeguards the technology assets which are in use in the organisation.

iv. The data that the organisation collects and uses is protected.

A global survey carried out by Deloitte Touche Tohmatsu (DTT) in 2008 revealed that the biggest threat to industrial control systems in the energy and resource industry, which includes the mining sector, was accidents caused by authorised personnel. This threat totalled 40% of the outlined threats. The human factor has not only been seen to be the greatest threat in the energy and resource industry but also in other industries. The survey further confirmed that as in previous years, human error had also remained the highest cause of information system failures, making up 86% of the total figure. This finding shows that in as much as people are an organisation's greatest asset, they may also be the weakest link. This will be more prominent during the economic crisis where the number of disgruntled employees will be on the increase and stress levels will be high (Manduca, 2009). The survey also revealed that the number of both internal and external information security breaches remains high with external threats being higher than internal threats. Top of the list of external threats was social engineering where users are hoaxed into disclosing confidential information online (DTT, 2008).

3.5 Information Security in the Mining Sector

According to ISO/IEC 27002 (2005), the amount of information security required in an organisation, including mining organisations is normally derived from three sources:

i. Assessment of the information risks that the organisation faces.

ii. Regulatory, legal, statutory, and contractual obligations that must be satisfied by the organisation, trading partners, contractors and service providers.

iii. The requirements, objectives and set of principles for information processing that the organisation has set to support its operations.

The mining industry is a continuous operational industry. Among the top priorities of information security, therefore, should be the high availability of information. With this, should be the high reliability of the hardware and software that are used to produce this information. According to the Mining, Minerals and Sustainable Development Project (MMSD) (2002: 296), access to information has been identified as one of the challenges faced by the mining sector. The quality of information, its production, use, flow, accessibility and credibility were described as key to developing trust and cooperation amongst stakeholders. The MMSD (2002: 296) further suggest that sustainable development in the sector requires increased openness and greater transparency in information production and dissemination throughout the mineral life cycle. This enhances effective decision making. Weaknesses were identified in the areas of information quality in terms of disclosure, timeliness, reliability and targeting the right people.

A survey carried out in 2008 by Ernst and Young on the mining and metals industry identified the major threats being faced in the industry as derived from the current business drivers. Macro threats emerge from the geopolitical and macroeconomic environment. Sector threats emerge from trends or uncertainties being faced by the industry, and operational threats emerge from organisational operations and may impact strategic performance of an organisation (Ernst & Young, 2008). These threats are illustrated in figure 3.4:

Figure 3.4: Macro, Operational and Sector threats faced by the Mining and Metals Industry (Ernst & Young, 2008)

As with any other organisation, mining information systems are vulnerable to deliberate and accidental damage (Tomlinson, 2007: 173). Information systems are often built without adequate security measures, thereby posing a security risk to the business (Dobelis, 2007: 46). Systems such as GIS' are also vulnerable to human error, incorrect data input, or incorrect use of programs and or measuring devices (Tomlinson, 2007: 12)

As ERPs integrate various functions and handle a variety of organisational information including human resources data, financial information, production planning and sales data, the security of this information is vital (von Solms and Hertenberger, 2005: 79). Von Solms and Hertenberger (2005: 79) further add that the security administrator of a system becomes a bottleneck as he has to handle several functional areas as well as business areas which make his work prone to errors and omissions. As information in an ERP is stored in a central repository, hackers have easier access to various kinds of information which may be susceptible to abuse by improperly assigned users of the system (van Holsbeck and Johnson, 2004; Kairab, 2004: 7).

A lot of communication is now done through emails which are increasingly used for formal and informal information. Research conducted by Ferris Research (2009) revealed that there were over 700 million business email users globally in 2006 with the number expected to go up to 934.8 million in 2010. Common email threats include viruses, spam and phishing (Cocca, 2004). A global security survey conducted by Deloitte Touche Tohmatsu in 2008 revealed that email attacks are still prevalent in the energy and resources industry (DTT, 2008).

Industrial Control Systems such as Programmable Logic Controllers (PLCs), Supervisory Control and Data Acquisition (SCADA), and Distributed Control Systems (DCS), used in production areas are currently facing increasing threats. Welander (2007) cites among others, inadequate policies, procedures and culture governing control system security, inadequately scrutinised control system software and inadequately secured wireless communication as some of the threats being faced by such control systems. Whereas IT systems that are part of the corporate network are governed by corporate policies and security, information systems used in the plant area are usually isolated and geographically dispersed and, therefore, do not receive as much security enforcement as typical IT systems (NIST, 2008; Falco *et al*., 2002). This is partly due to the fact that they were not meant to be connected to the enterprise network. However, these systems are now being interconnected with other networks and the Internet, and managers also require real-time data from these systems for decision making (Cárdenas *et al.*, 2008; Hentea, 2008).

3.6 Conclusion

In order for an organisation to fully appreciate and implement information security, there is a need to assess the risks faced by information systems in the organisation. Only when information security threats and their consequences posed to the organisation are understood and their corresponding risks evaluated, can appropriate controls be implemented. The security of data is only at risk because it has value and that is what attracts attackers to steal, sabotage and corrupt it (Whitman and Mattord, 2009: 38). As suggested by McMillan (2007: 109), an evolving, continuous risk management process supported by management is, therefore, essential in the protection of data and information in an organisation.

Chapter 4

Risk Management

Chapter 3 described the vulnerabilities and threats that organisations face through the use of information systems and information. This chapter discusses the process of managing the issues that were identified in chapter 3. It also looks at how the mining industry handles these risks as well as the mitigating factors that are put in place to reduce or eliminate risks to organisational information.

4.1 Introduction

Information threats and vulnerabilities exist in all organisations irrespective of whether or not these systems are connected to the outside world. It is, therefore, vital to assess the risks these threats and vulnerabilities pose to the continuous operation and wellbeing of the organisation. Once the risks are understood, controls can be put in place to mitigate, reduce or transfer the risk (Tudor, 2006: 11). Any kind of operation in any organisation always involves a certain amount of risk (Whitman and Mattord, 2009: 117; Vellani, 2006: 110). According to Gerber and von Solms (2005), traditional risk management focused more on infrastructure than information, although this has now been seen to change with the advent of the information age. As a result, organisations are now including information management in their standard business practices (Broderick, 2001).

4.2 Risk Management

A risk as defined by Wessels *et al.* (2007: 233) is the likelihood that a threat will exploit vulnerabilities. A risk is made up of a threat, a probability and an impact (Purser, 2004: 27). Organisational risks need to be managed in order for threats and vulnerabilities to be contained. Risk management is the process used to identify, control and minimise the impact of uncertain events. Through risk management, business managers are able to create a balance between operational and economic costs while protecting assets and achieving organisational objectives (Peltier *et al.*, 2005: 7). Risk management is a management process and according to NIST SP800-30 (NIST, 2002), should, therefore, involve senior management, the Chief Information Officer (CIO), Information Security managers and personnel, system and information owners, business and functional managers, and security awareness trainers. According to Peltier *et al.* (2005: 7) and Whitman and Mattord (2009: 117), risk management is made up of four distinct processes, namely; risk identification, risk assessment, risk mitigation and vulnerability assessment and, controls valuation as shown in figure 4.1.

Figure 4.1: Components of Risk Management (Whitman and Mattord, 2009: 117)

4.3 Risk Identification

Chinese General Sun Tzu's observation made over 2400 years ago is still relevant to today's philosophy of information security. Sun Tzu recommended that in order for an organisation to reduce risk, it must know itself and know its enemy (Whitman and Mattord, 2009: 118). According to Whitman and Mattord (2009: 119), good risk management begins with managers understanding how information is processed, transmitted and stored as they are the key players in risk management. Risk identification should be a continuous process as new risks keep emerging (Tchankova, 2002; Broderick, 2001).

Risk can be identified by the basic elements; sources of risks, perils, hazard factors and exposures to risk (Tchankova, 2002). The first step in the risk identification process is the identification of information assets. These include people, procedures, data, information, software, hardware and networking. Risk identification also involves the identification of specific elements of the three components of risk which are threats, vulnerabilities and assets (Shelly and Rosenblatt, 2009: 577) as shown in figure 4.2.

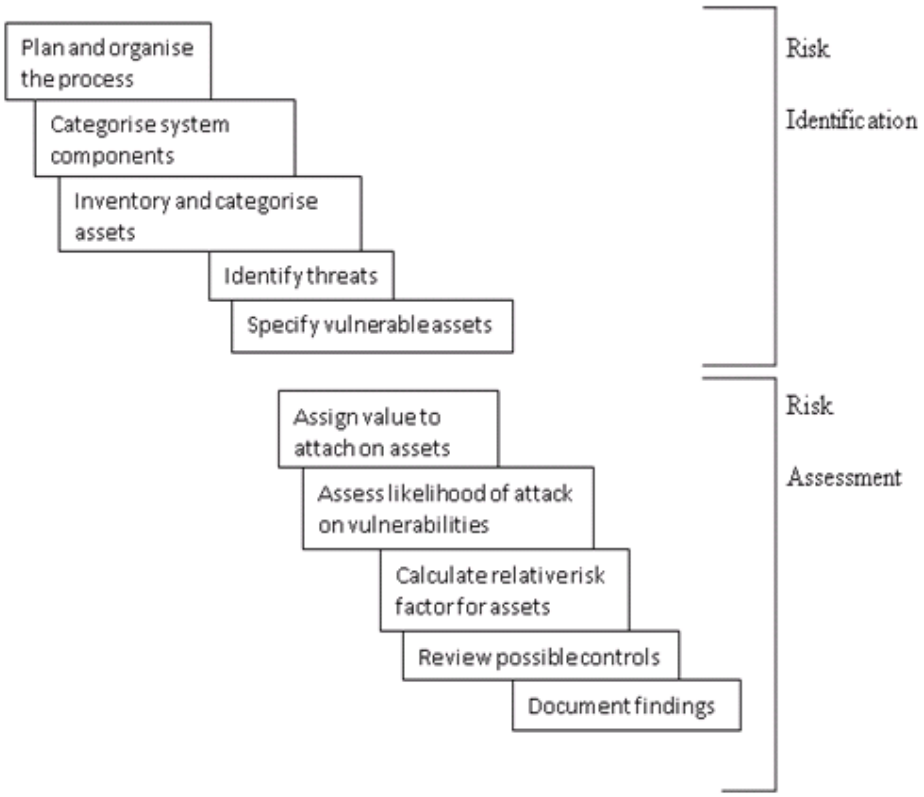

Figure 4.2: Components of Risk Identification and Risk Assessment (Whitman and Mattord, 2009: 120)

Coyle (2004: 12) and Williams *et al.* (1998) in Tchankova (2002) cite the environments in which risks can occur. These include physical, legal, social, political, cognitive, and operational environments.

4.3.1 Asset Identification and Valuation

Before any risk management process can take place, the assets that are at risk need to be identified so that their risk levels can be determined. In order to appropriately determine the level of security required in an organisation, assets needs to be inventoried, responsibility assigned, and a value attached to each existing asset. The value of the asset can be in the form of quantity (related to its cost) or quality (its relative importance) (Honan, 2009: 48). Information gathering can be done using questionnaires, on-site interviews, document reviews, brainstorming, Delphi techniques (group input by a team of experts in that particular area), SWOT (Strengths, Weaknesses, Opportunities and Threats) analysis and scanning tools (Peltier *et al.,* 2005: 187; Schwalbe, 2009: 434-435). This identification will help the risk

management team determine what resources are required to support these assets and the impact these assets have on business processes.

Ownership of assets may be allocated to a business process, a defined set of activities, an application or a defined set of data. The asset inventory according to ISO/IEC 27002 (2005) should include the asset type, format, backup information, business value, license information and location of the asset. This inventory may also be required for safety, health, insurance or financial purposes. ISO/IEC 27002 (2005) also suggests that the types of assets for inventory should include information, software and physical assets, people and their qualifications, skills and experience, computing and communications services, general utilities, such as heating, lighting, power and air conditioning, and intangibles.

Organisations use a variety of information classification schemes. Whitman and Mattord (2009: 131) suggest a general classification scheme that could be adopted by organisations:

- Public: this information can be disseminated to the general public and includes advertisements, and public and press releases.
- For Official Use Only: although not very sensitive, this information is not for public release. Internal communications may fall under this category.
- Sensitive: this information is relatively important to the business and may cause loss of market share or destroy the reputation of an organisation if revealed.
- Classified: this is information of utmost importance to the business and may have devastating consequences if revealed.

4.3.2 Threat Identification and Analysis

A threat is an exploitation of a vulnerability (Peltier *et al.,* 2005: 187). Janczewski and Colarik (2005: 52) list the four steps involved in threat analysis:

i. Definition of the actual threat.
ii. Identification and estimation of possible consequences to the organisation if the threat is realised.
iii. Determination of the probable frequency of a threat.

iv. Assessment and estimation of the probability that a threat will actually materialise.

4.3.3 Vulnerability Assessment

The goal of vulnerability assessment is to determine the vulnerabilities that could be exploited by potential threat sources. NIST SP800-30 (NIST, 2002) recommends development of a security requirements checklist, performance of system security testing and use of vulnerability sources as methods of identifying vulnerabilities.

The end product of risk identification is a list of threats, assets and their vulnerabilities. This list, together with other documents forms the basis for risk assessment (Whitman and Mattord, 2009: 139). Risk identification should be a continuous process as the environment keeps changing (Tchankova, 2002).

4.4 Risk Assessment

Risk assessment involves the identification and evaluation of risks and their impacts. It also includes the recommendation of risk reduction measures (Rittinghouse and Ransome, 2005: 27). Risk assessment further provides a framework for the establishment of policies and identification of appropriate controls and procedures that will consequently be used to protect the organisation's assets (Tregear, 2001). This process should also take into account any services that have been outsourced by the organisation (Broderick, 2001). Figure 4.3 shows the risk estimate model used to assign a risk rating to each information asset.

Risk is
The **likelihood** of the occurrence of a vulnerability
Multiplied by
The **value** of the information asset
Minus
The percentage of the risk mitigated by **current controls**
Plus
The **uncertainty** of current knowledge of the vulnerability

Figure 4.3: Risk Identification Estimate Factors (Whitman and Mattord, 2009: 139)

A risk matrix is also used to determine the level of risk that an asset might be exposed to if a vulnerability materialised. A high risk level means there is a strong need for corrective measures as soon as possible. A medium risk level means there is need for corrective measures but these measures can be incorporated into a risk mitigation plan within a period

of time. A low risk level on the other hand, means the approving authority can decide whether to implement corrective measures or accept the risk and continue operating (NIST, 2002).

Table 4.1: The 3x3 Matrix for Risk Assessment (Adapted from NIST, 2002 and Sadgrove, 2005: 28)

Threat Likelihood	**Impact**		
	Low (10)	**Medium** (50)	**High** (100)
High (1.0)	**Low** 10 x 1.0 = 10	**Medium** 50 x 1.0 = 50	**High** 100 x 1.0 = 100
Medium (0.5)	**Low** 10 x 0.5 = 5	**Medium** 50 x 0.5 = 25	**Medium** 100 x 0.5 = 50
Low (0.1)	**Low** 10 x 0.1 = 1	**Low** 50 x 0.1 = 5	**Low** 100 x 0.1 = 10

Risk Scale: High (>50 to 100); Medium (>10 to 50); Low (1 to 10)

Risk assessment, involves two techniques. Quantitative risk assessment translates risks into numbers, usually financial, using probability theory while qualitative risk assessment attempts to explain risks using descriptive variables (McGaughey *et al*., 1994). Whitman and Mattord (2010: 325), however, further add the OCTAVE approach as a third risk assessment methodology. Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE) approach comprises three phases, namely; building asset based threat profiles, identifying infrastructure vulnerabilities, and developing security strategies and plans (Tregear, 2001; Whitman and Mattord, 2009: 151-155).

Risk assessment brings together all the elements of the risk management process which are identification, analysis and control, and is critical in the development of an effective risk management strategy (Kuempel *et al*, 2007: 119). Information gathered from an initial risk assessment may be used as a baseline for future comparisons (Whitman and Mattord, 2009: 159). Zelkowitz (1997: 31) points out that there is no defined recipe for risk management or analysis. However, choices made during implementation will affect the overall effectiveness of the process.

4.5 Risk Control Strategies

Managing risk requires the introduction of control mechanisms. It is, therefore, important to take into account the fact that these actions may themselves introduce new risks into the organisation (Purser, 2004: 28). Peltier *et al*. (2005: 192), NIST SP800-30 (NIST, 2002), Schwalbe (2009: 447-448) and Whitman and Mattord (2009: 145) suggest four common risk control strategies:

i. Avoidance: this strategy seeks to avoid risk rather than deal with it once it has materialised. This is accomplished through application of policy, training and education, countering threats, and implementation of technical security controls and safeguards.

ii. Transference: this strategy attempts to shift the risk to other assets, processes or organisations. This can be accomplished through purchase of an insurance policy, revision of deployment models, and a rethought of how services are offered.

iii. Mitigation: this approach attempts to reduce the damage caused by the exploitation of a vulnerability by means of planning and preparation. It includes three (3) types of plans namely, Disaster Recovery Plan (DRP), Business Continuity Plan (BCP) and Incident Response Plan (IRP). Mitigation is dependent on the ability to detect and respond to an attack as quickly as possible.

iv. Acceptance: in this approach, the organisation decides to do nothing to protect the information asset but rather accept the outcome from any resulting exploitation. This usually happens when an organisation has concluded that the cost of protecting an asset does not justify the security expenditure. As illustrated in figure 4.4 below, not all threats require a control situation. Implementation of a control to curb those threats may prove to be too restrictive on certain business processes (Kovacich and Halibozek, 2003: 206).

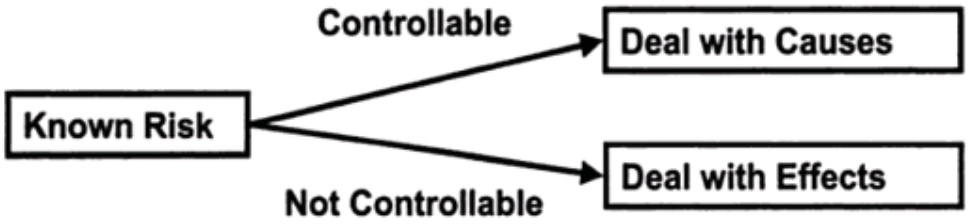

Figure 4.4: Risk management Strategies (Kendrick, 2009: 185)

Hess and Hess (2008: 129) and Culp (2001: 8) argue that risk cannot be completely eliminated. No matter how much investment has been put into a system or environment, it can eventually be compromised. An organisation, therefore, needs to define the quantity and nature of risk that it is willing to accept through evaluation of trade-offs between unlimited accessibility and perfect security. This definition is known as *risk appetite* Some threats such as natural disasters are actually beyond human control and unpredictable (Whitman and Mattord, 2009: 312).

In as much as avoidance is an effective way of managing risk, the main aim of risk management should be reducing risks to a level that is acceptable to an organisation. This is also known as risk mitigation (Kendrick, 2003: 191). Crocker (2003: 13) cites an example of the installation of water sprinklers in a warehouse. This installation does not reduce the chances of a fire breaking out but reduces the damage the fire will cause if it was to break out. The choice of a risk reduction strategy depends on an organisation's environment and the circumstances under which it conducts business.

Before a risk control strategy can be selected, a cost-benefit analysis is carried out to determine the impact of implementing a new or enhanced control and the impact of not implementing the control at all (Peltier *et al.*, 2005: 27). This control should not cost more than the asset itself (Kovacich, and Halibozek, 2003: 206). A benchmark can also be created where an organisation studies the practices of another organisation and compares them with its own (Whitman and Mattord, 2009: 155).

Even after measures have been put in place to manage risk, a certain amount of risk called residual risk still remains. This risk needs to be classified into acceptable or unacceptable risk. Further decisions need to be made to either apply more controls or make the controls more stringent on the unacceptable risks (Gerber and von Solms, 2005).

4.6 Controls

It is the responsibility of senior management to put in place policies and strategies which define how the company develops and makes use of its assets (Sadgrove, 2005: 276). According to Sadgrove (2005: 276), these assets form the basis of an organisation's risks and if the organisation is well managed, there will be systems, audits and controls in place to regulate them and provide feedback.

Controls are the specific technologies, policies and manual procedures that are used to protect assets as well as the accuracy and reliability of information systems (Wessels *et al.*, 2007: 234). They are defense mechanisms that are intended to prevent accidental hazards, deter intentional acts, detect problems as early as possible, enhance damage recovery and correct problems (Turban *et al.,* 2002: 674).

Controls can be implemented as functional controls which include preventive, detective and corrective, or classified by type to include general, application, data communication and security measures (Wessels *et al.*, 2007: 239, 243). According to ISO/IEC 27002 (2005), these controls need to take into account:

i. Organisational objectives.

ii. National and international legislation and regulations.

iii. Operational requirements and constraints.

iv. Balancing of investments in implementation and operation of controls against the harm that is likely to arise from security failures.

v. Cost of implementation and operation in relation to the risks being reduced and remaining proportional to the organisation's requirements and constraints.

4.6.1 Categories of Controls

Controls fall into three (3) categories. These are administrative, technical and physical controls. These categories can further be classified into preventive and detective controls. Preventive controls, according to Hall (2008: 137), attempt to avoid the occurrence of unwanted events while detective controls attempt to identify and expose unwanted events

after they have occurred. Table 4.2 provides examples of both preventive and detective controls per category.

Table 4.2: Examples of information security controls (Adapted from Hall (2008: 137); Tudor (2006: 16); Contesti et al. (2007: 208); Wessels et al. (2007: 240-243))

	Administrative Controls	**Technical Controls**	**Physical Controls**
Preventive Controls	Security awareness and technical training	Access control software	Backup files and documentation
	Separation of duties	Antivirus software	Fences
	Procedures for recruiting and terminating employees	Library control systems	Security Guards
	Security policies and procedures	Passwords	Badge systems
	Supervision	Smart Cards	Locks and keys
	Disaster recovery and contingency plans	Encryption	Backup power
	User registration for computer access	Dial-up access control and call back systems	Biometric access controls
Detective Controls	Security reviews and audits	Audit trails	Motion detectors
	Performance evaluations	Intrusion-detection expert systems	Smoke and fire detectors
	Required vacations		Closed circuit television monitoring
	Background investigations		Sensors and alarms

Slade (2006: 179) and Wessels *et al.* (2007: 243) further add supplementary controls called corrective, deterrent and recovery controls which are considered to be special cases within the physical, technical and administrative controls. They either return conditions to what they were before the violation or remedy the circumstances that allowed the activity to take place.

Whitman and Mattord (2004: 328-329) provide a form of control classification which helps in the selection of controls based on the kind of protection it should provide. Classification of a control can be based on

i. Control function, of which the control can either be preventive or detective.

ii. Architectural layer: controls may be applied depending on which layers they provide protection to.

iii. Strategy layer: this classification depends on the risk control strategy they operate within such as transference or alleviation.

iv. The information security principle they operate within.

4.6.1.1 Administrative Controls

These controls involve guidelines and policies on the steps employees can take when confronted with risky situations at a place of work (Caballero, 2009: 232).

4.6.1.1.1 Asset Management

Management of classified information includes storage, distribution, portability and destruction of information. Classified data in storage must only be made available to authorised individuals through such methods as locking of file cabinets and safes and should be inconspicuous when in transit (Whitman and Mattord, 2009: 124, 132).

A *clean desk policy* may be enforced to mandate employees to secure all information in appropriate storage containers and destroy any information that is no longer of value to the organisation. Care should be taken when disposing of information as dumpster divers search for information in trash and recycling areas. Information should only be disposed of after appropriate authorisation (Whitman and Mattord, 2009: 132).

4.6.1.1.2 Change Management

Once a system has been properly secured, there is a need to manage and to keep the security intact as any changes made to it may introduce new vulnerabilities. Stewart *et al.* (2005: 455) suggest that the only way to maintain security in the face of change is to manage change. Change management involves extensive logging, auditing and monitoring of activities related

to security controls and mechanisms. They also identify five (5) stages involved in the change management process:

i. Applying to introduce a change.

ii. Cataloguing the intended change.

iii. Scheduling the change.

iv. Implementing the change.

v. Reporting the implemented change to the appropriate authorities.

Change management involves technical changes affecting implemented technologies and non-technical changes affecting people and procedures (Whitman and Mattord, 2004: 56).

4.6.1.2 Technical Controls

Technical controls when properly implemented enhance the confidentiality, integrity and availability of information which is in storage, being transmitted, and that which is being processed (Whitman and Mattord, 2004: 363). These controls also known as logical controls restrict access to systems and provide for protection of information (Krutz and Vines, 2003: 45). The controls are able to work without human intervention once implemented (Tudor, 2006: 15).

4.6.1.3 Physical Controls

Physical controls deal with physical access to an organisation's resources (Whitman and Mattord, 2009: 402). They incorporate guards and building security in general such as locking of doors, securing of server rooms or laptops and backing up of files (Krutz and Vines, 2003: 45). Section 4.6.1.4 discusses physical access controls. Physical controls also deal with physical interception of data. Data interception is usually done through direct observation, interception of data transmission and electromagnetic interception. Mobile and portable devices are fitted with tracking devices and software, and encrypted so as to preserve sensitive information (Whitman and Mattord, 2009: 424-426).

4.6.1.4 Access Control

While Wessels *et al.* (2007: 240), Whitman and Mattord (2005: 199), and NIST (1995) suggest that logical access control falls under technical controls, Harris (2007: 155) and Stewart et al. (2005: 2) point out that there are other access control processes that also fall into the administrative and physical categories, hence access control falls into all three categories. Access control involves admission of a user into a trusted area of the organisation and encompasses four security objectives; authentication, accountability, auditability and authorisation (Hill and Alvarado, 2003: 9). These areas include information systems, physically restricted areas such as computer rooms, and the organisation as a whole (Whitman and Mattord, 2005: 135). Effective access control requires a formal implementation of an access control policy which determines how access rights are granted to the appropriate individuals, groups and entities.

Whitman and Mattord (2009, 338), Peltier *et al.* (2005: 150), and Wessels *et al.* (2007: 240), list four types of authentication mechanisms:

- *Something you know,* which includes passwords, PINs and passphrases.
- *Something you have*, which includes smart cards, magnetic cards and cryptographic tokens.
- *Something you are,* which includes retina scans, hand geometry and fingerprints.
- *Something you produce*, which includes voice and signature pattern recognition.

Authorisation deals with an authenticated entity. It can be an authenticated user, members of a group, and multiple systems where a central authentication authority grants a set of credentials also called an authorisation ticket or *single sign-on*.

Access control can be mandatory, non-discretionary and discretionary (Whitman and Mattord, 2009: 141). Mandatory access controls give users and data owners limited control over access to information resources. When the owner of a file or resource can decide what rights or privileges the users will have to that file or resource based on their identity or groups to which they belong, this is called discretionary access control (Lehtinen *et al*., 2006: 266). Non-discretionary access controls, on the other hand, are managed by a central authority and granting of access can be based on an individual's role (Whitman and Mattord, 2009: 142).

According to Hawker (2000: 58), with good controls in place to eliminate or minimise risks, an organisation will attain competitive advantage, produce accurate information, maintain good controls over information, and improve the quality of decisions.

4.7 Risk Management in the Mining Industry

Gerber and von Solms (2005) suggest that although a lot of research has been conducted, there is no ideal method for risk analysis or risk management. Each organisation has its own unique characteristics which need to be taken into consideration when addressing information security requirements. The mining industry has its own risk management model(s), an example of which is shown in figure 4.5:

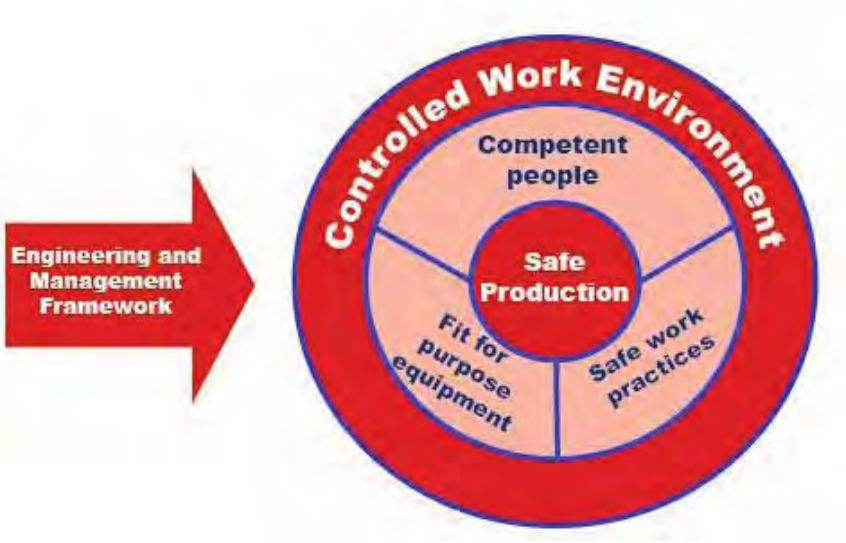

Figure 4.5: Minerals Industry Risk Management Model (DPI, 2005)

Risk management in the mining industry has been solely concentrated on safety, occupational health, and quality management. With the advent of the information age, the risk management process has been extended to include physical IT assets. Information that is stored, transmitted and processed within the same IT infrastructure has, however, not yet been well covered (Pironti, 2008). In view of this, in as much as risk management in the mining industry requires information for it to be carried out effectively, information risk management itself has not been one of the high priority risk areas in this industry. An integrated or enterprise risk management approach, however, which aims to identify, evaluate and manage major corporate risks in an integrated framework, is now being adopted by the

mining industry. This is in order to encompass all risk areas and not just focus on safety, environmental, occupational health and quality areas (Fagg, 2009; Olson and Wu, 2008: 3).

The use of Industrial Control Systems such as Supervisory Control and Data Acquisition (SCADA) and Distributed Control Systems (DCS) put control data in the organisation at a higher risk than that of typical IT systems, as they were not designed to accommodate any additional functions and were, therefore, operating in an isolated environment requiring extensive physical effort to gain access to them (Lowe *et al.,* 2007; NIST, 2008c). This meant certain system management functions such as patch management, anti-virus updates and enterprise backups could not be performed. Security incidents in these systems could have health, safety, environmental and reputation implications (Lowe *et al.,* 2007). Manufacturers of industry systems and applications are taking into consideration the interconnectivity of these systems with other systems as well as supporting remote connectivity to them. As a result, system hardening measures are being put in place to address security issues (Bartels, 2005; Rockwell, 2009; SAP, 2009) According to Krutz (2005: 97), implementation of login restrictions, cryptography, audits, intrusion detection systems and patch management are now being introduced.

Maintaining and upgrading legacy systems is a challenge constantly faced by managers as technologies are constantly changing. Maintenance of these systems usually takes up to 80% of the total IT budget and these systems often lack the agility to support critical competitive efforts (Shelton, 2009; Lawrence, 2007; Welander, 2009). Modern information systems are built with latest technologies which are often efficient enough to handle business processes and security requirements whilst legacy systems still run on old technologies. Despite the availability of these modern systems, 80% of IT systems still in use are legacy systems (Zoufaly, 2009). Some mining organisations are, however, adopting a Service Oriented Architecture (SOA) and Legacy IT Modernisation (LIM) to transform legacy systems and make them part of a flexible and fast IT architecture (Citect, 2008; Lawrence, 2007; Shelton, 2009).

Cultural clashes between IT staff and control engineers on securing control systems while meeting organisational security goals often occur as they sometimes do not understand each other's needs (Bartels, 2005). Current IT staff have been trained on modern systems creating a skills gap for the support of legacy systems (Shelton, 2009).

As mines have diverse information sources, assets need to be properly identified and valued for the risk management process to be effective. All information systems in an organisation and the information they produce need to be identified and the criticality of the information defined. A survey on the global state of information security in energy and mining industries which was conducted by PricewaterhouseCoopers in 2008, revealed that only 35% of energy and mining organisations had an accurate inventory of customer and employee data being collected, transmitted and stored (PricewaterhouseCoopers, 2008). As discussed in chapter 2, mining companies deal with a variety of stakeholders, hence information classification is vital if the right information is to be disseminated to the right people.

According to the PricewaterhouseCoopers survey conducted in 2008, the mining and energy industry has seen an increase in the implementation of access control software from 47% in 2007 to 64% in 2008 (PricewaterhouseCoopers, 2008). Bartels (2005) and Bajpai and Gupta (2005) describe the security measures that are put in place in processing industries which include the mines. These include physical and electronic access to the plant area and IT environment controls which range from intruder prevention and detection systems, anti-virus software, timely patch implementation, regular audits of systems, and employee awareness on policies and procedures. Bartels (2005) goes on to say that loss of security in such industries could result in serious safety and economic implications beyond that of loss of production.

As mining is a continuous operation industry, a disruption in operation must be quickly returned to normal state. Security in these industries is not just a business or manufacturing issue but one of national security as well. Such regulations as mining regulation 2103 (GRZ, 1973: 137) preventing entry of unauthorised persons into any part of the mining area require an organisation to put in place measures to comply with the regulation.

Change management is equally important in the mines as employees can either intentionally or unintentionally change processes. Rahesh Mody, chief architect of open standards, says well intentioned insiders can be just as harmful as outsiders (Bartels, 2005).

Bajpai and Gupta (2005) suggest the implementation of clear procedures such as access control, CCTV, background checks of potential employees as well as effective emergency response plans to enhance security.

With email use as a workflow and collaborative tool in an organisation, the confidentiality of sensitive information cannot easily be guaranteed (Bradley, 2008). In a survey conducted by eMedia in 2008, 94% of executives felt they had no control over the flow of information into and out of the organisation. Real-time proactive controls are required as part of strategic risk management as not having the necessary controls in place may trigger a regulatory violation or expose sensitive company information. This can be achieved through archiving, implementation of policies and audits (Bradley, 2008).

Implementation and use of an ERP system may also prove risky if the risk assessment process is not undertaken properly. This is because an ERP system is integrative in nature and affects a number of business processes and functional areas (Aloini *et al*., 2007). As ERP systems are high investment systems, they thus require adequate planning, time and controls, if an organisation is to derive benefits from its implementation (Motwani *et al*., 2005; Berchet and Habchi, 2005).

4.8 Conclusion

Carrying out risk assessment does not necessarily mean controls have to be implemented to mitigate the current risks. Risk management involves creating an awareness of the level of risk existing in the organisation and finding ways of handling those risks. Coupled with this, is the correct identification of organisational assets and their classification in order for the right controls to be put in place. As controls cannot completely protect an organisation's assets, they need to be monitored and improved upon for them to continue being efficient and effective (IRM, 2002). This also helps in the implementation of contingency measures. As the mining industry increasingly recognises the importance of information assets, information risk management is being integrated into daily operations (Fagg, 2009).

Chapter 5

Contingency Planning

This chapter is an extension of risk mitigation strategies discussed in chapter four which are part of the risk management process. It describes the contingency strategies that organisations need to put in place to restore and maintain business operations in case of a disaster.

5.1 Introduction

A successful risk assessment process does not end with identification and implementation of controls. Managers are still tasked with strategic planning to ensure the continuous availability of information systems. Causes of business interruptions range from natural disasters such as fires to computer viruses (Hawkins *et al.*, 2000). A Gartner report identified the 24/7 business delivery model, increasing operational risk and globalisation of business operations as the main factors which are currently driving the growth of Business Continuity Management (BCM) (Gartner, 2009). Events such as the terrorist attacks of 11th September, 2001, the 'millennium bug' and the Severe Acute Respiratory Syndrome (SARS) outbreak of 2003 provided a wake-up call for "must have" contingency plans as organisations realised the criticality of such plans (Savage, 2002; Honour, 2007: xvii). Historically, financial industries were amongst the few industries that were best prepared in the recovery of data and critical business units. However, industries such as manufacturing, service and public administration are now increasingly aware of the reality of risks (Tilley, 1995).

5.2 Contingency Planning

Contingency planning helps organisations anticipate, react to and recover from events that threaten the security of information and information assets in the organisation and subsequently the restoration of the organisation to normal business operations (Whitman and Mattord, 2009: 209). Fischer *et al*. (2008: 248) define a contingency as a possible but uncertain occurrence of an event that can cause significant disruption to the organisation's activities. Contingency planning involves carrying out a Business Impact Analysis (BIA), incident response planning, disaster recovery planning and business continuity planning (Caballero, 2009: 233). An IRP focuses on immediate response but the process may move on to disaster recovery and/or a business continuity process if the attack escalates or is disastrous (Whitman and Mattord, 2009: 209). While the concept of business continuity and disaster recovery may be the same, business continuity deals with measures that are or have been put in place to switch over operations to a backup facility within 24 hours. Disaster recovery on the other hand, deals with reconstruction and retrieval of information if a primary facility is damaged or has been destroyed (Elrod, 2005: 2). Figure 5.1 outlines the inter-relationship amongst the contingency plans:

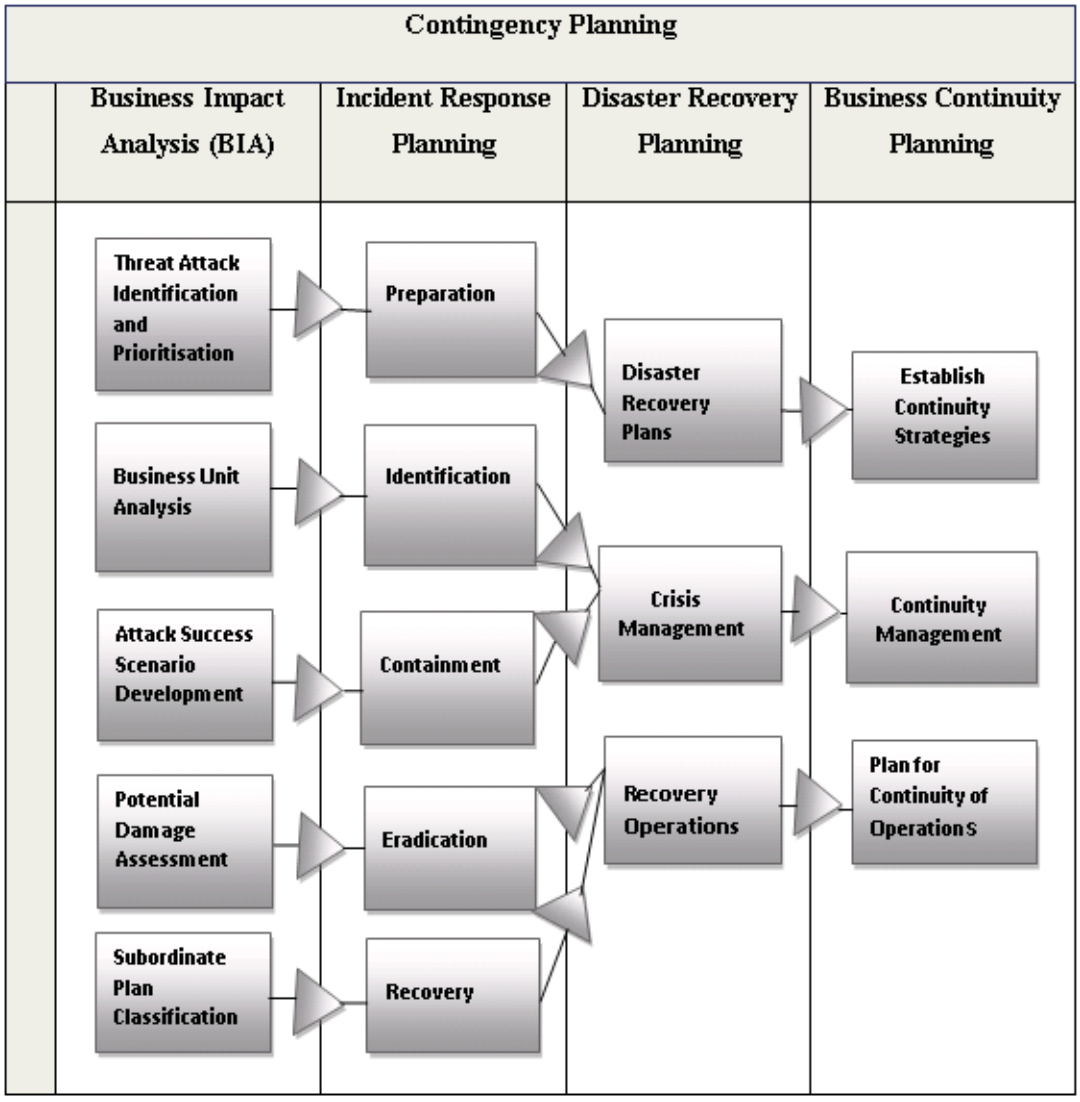

Figure 5.1: The relationship amongst the four types of contingency plans (Caballero, 2009: 235)

5.3 Business Impact Analysis

Rittinghouse and Ransome (2005: 69) define Business Impact Analysis (BIA) as a process of identifying critical business processes and the effects of loss on these processes in order to determine recovery strategies for the business. Results obtained from a BIA must be incorporated into an organisation's BCP, Business Recovery Plan (BRP) and Continuity of Operations Plan (COOP). A BIA will help the organisation identify the dependencies of core business processes (Doughty, 2007: 1549). Whitman and Mattord (2009: 212-214) outline the five (5) stages of the BIA process:

i. **Threat identification and prioritisation:** An organisation which has already conducted a risk assessment need only add a threat profile which gives a detailed description of activities that occur during an attack. Threat identification and risk assessment were discussed in chapter 4.

ii. **Business Unit Analysis:** This involves carrying out an evaluation of business functions within business units and determining which functions are vital to the continual operation of the business.

iii. **Development of successful attack scenarios:** Scenarios depicting a series of successful attacks from each threat are created. The outcomes which are added to the attack profile describe the best, worst or most likely case that could result from an attack on that particular business functional area. This helps them address each business function at a time.

iv. **Assessment of potential damage:** The BIA planning team estimate the cost of the best, worst and most likely cases identified during the scenarios to determine what must be done to recover from a disaster or an incident. This results in an attack scenario end case.

v. **Classification of subordinate plans:** A subordinate plan is developed or identified from amongst existing plans. These plans take into account identification of, reaction to and recovery from each scenario. An attack scenario end case can either be disastrous or non-disastrous. A non-disastrous end case falls under incident response whereas a disastrous one is addressed in a DRP.

5.4 Incident Management

No matter how effective or efficient an information security program is, incidents will still occur (Dodson, 2001). An incident as defined by Dodson (2001) is any adverse event or situation that poses a threat to the confidentiality, integrity and availability of information. This identification helps the organisation reduce disruption to the business as operations are quickly reduced to acceptable levels, hence maximising the availability of IT services (McPhee, 2008: 337). Effective and timely management of major incidents is a significant factor in the preservation of an organisation's reputation and financial standing (Taylor, 2008). Threats that were described in section 3.3 could turn into incidents and threaten the

confidentiality, integrity and availability of information resources if they are directed against information assets and have a realistic chance of success (Whitman and Mattord, 2009: 215).

5.4.1 Incident Response

Incident response is a set of activities that are taken to plan for, detect and correct the impact an incident would have on information assets (Whitman and Mattord, 2009: 215). An incident can range from hardware failure to a concentrated attack on a computer system by an unethical hacker and can go beyond organisational and national boundaries (Miles, 2001; ISO/IEC 27002, 2005). Hence, the need to coordinate and share information with appropriate external parties. In addition to Caballero's model (Caballero, 2009: 235) for incident response planning, Dodson (2001), NIST (2008b), Miles (2001), Mitropoulos *et al.* (2006) and Whitman and Mattord (2009: 215, 224) further suggest that incident response planning should not end at the recovery stage but should also include post-incident activities. They, therefore, sum up the major steps involved in the incident response process to include incident preparation, incident detection or identification, incident reaction and containment, incident eradication, incident recovery and post-incident activity, as shown in figure 5.2. The incident response planning process like other contingency plans should be continuously reviewed and updated (Kovacich *et al.*, 2003: 291).

Figure 5.2: Major Phases of Incident Response: NIST SP800-61 (2008b)

5.4.1.1 Incident Preparation/Planning

Preparation is a critical step in any professional environment (Miles, 2001). This step involves preparation for the occurrence of an incident and includes identification of events that may have a negative impact on the business coupled with a detailed understanding of the scenarios developed for the BIA (Whitman and Mattord, 2009: 216). These events include data backup, preparation for re-installation tools, resource kits, security patches, boot disk and operating system archiving (Mitropoulos *et al.*, 2006).

5.4.1.2 Incident Identification/Detection

This involves identification of the incident and invocation of the IRP and relies on either a human or automated system (Whitman and Mattord, 2009: 218). An organisation may decide to declare an incident a disaster if it is unable to mitigate the impact of an incident or the level of damage is so severe that it is unable to recover quickly.

5.4.1.3 Incident Reaction and Containment

Once an incident has been classified as such, action is taken to stop it, mitigate the impact and provide information relating to recovery from the incident. An alert message describing the incident is sent out to key personnel so that each individual knows which part of the IRP is supposed to be implemented (Whitman and Mattord, 2009: 221). A quick and organised response may mean the difference between a minor incident and a major catastrophe (Bragg *et al*., 2004: 742). Documentation of an incident should start as soon as the incident or disaster is declared so as to record the who, what, when, where, why and the how of the event. This documentation serves as a reference for similar incidents in future and provides evidence from a legal standpoint.

Incident containment strategies involve isolating affected channels, processes, services, or computers and removing the losses or reducing the impact of the loss (Whitman and Mattord, 2009: 223). An organisation should define acceptable risks in dealing with incidents and develop strategies accordingly. For example, the strategy needed to contain an email-borne virus infection is different from that used against a Denial-of-Service (DoS) attack (Vallabhaneni, 2008: 331). In extreme situations, the ultimate containment option is to disconnect all computers and network devices in the organisation (Whitman and Mattord, 2009: 223).

5.4.1.4 Incident Eradication

After an incident has been contained, it is necessary to eliminate components of the incident. This process may also take place during recovery (NIST, 2008b).

5.4.1.5 Incident Recovery

This involves bringing the business and assets involved in the incident back to normal operations and possibly harden systems to prevent similar incidents (Caballero, 2009: 233;

Vallabhaneni, 2008: 331). Recovery may involve restoring systems from backup or rebuilding them afresh, changing passwords and tightening security measures (Vallabhaneni, 2008: 331).

5.4.1.6 Post-incident Activity

After an incident has been handled, a lesson learnt meeting is held to review the incident handling process and any shortcomings that may have arisen during incident handling (Vallabhaneni, 2008: 331; Dodson, 2001). This may involve updating security policies, procedures and guidelines in order to address future attacks of the same type (Mitropoulos *et al.*, 2006).

5.5 Disaster Recovery Planning

Disaster recovery planning identifies all activities that will be performed by personnel involved in disaster recovery to respond to a disaster and recover an organisation's IT infrastructure. Disaster recovery includes the response, recovery, resumption and restoration phases (Stacey, 2006: 1557). These form part of the eight (8) R's discussed in section 5.6. Disaster recovery planning is a subset of business continuity planning which is also a subset of contingency planning. Figure 5.3 illustrates the foundation of the similarity of concepts in disaster recovery and business continuity.

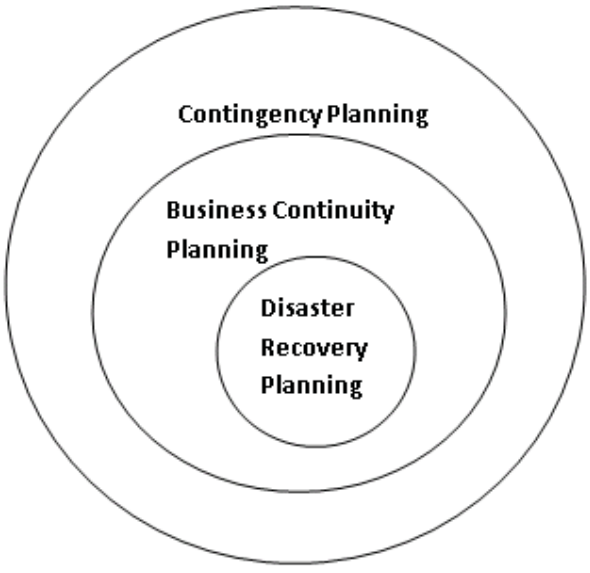

Figure 5.3: Subsets of Contingency Planning (Adapted from Rittinghouse and Ransome, 2005: 2; Eagar, 2009)

Disasters can be classified into acts of nature, external man made events, internal unintentional events, internal intentional events, legal, regulatory, compliance or governance failure, and business failures (Vancoppenolle, 2007: 10). Examples of disasters are shown in Table 5.1.

Table 5.1: Examples of disasters (Adapted from Fulmer, 2004: 4)

Equipment failure	Security incidents	Hazardous material incident
Flooding	Cyber crime	Denied access
Fire	Power failures	Loss of key employees, customers or suppliers
Explosion	Utility failures	Communication failures
Wind and Ice Storms	Arson	Strikes and work stoppages
Severe storms	Pandemics	Terrorism
Civil disturbances	Sabotage	Transportation accident

5.5.1 Backup strategy

Selection of a backup strategy can speed up the process of disaster recovery. There are currently two (2) backup strategies available (Hawkins *et al.*, 2000):

i. In-house backup systems: these guard against theft and loss of an organisation's data as backup servers are strategically located within the organisation. Data can, however, still be lost if the physical site itself is destroyed (Coombs, 2008: 52).

ii. Offsite backup systems with encryption: data is encrypted and backed up to a remote site. Offsite backup will be discussed in section 5.6.2.

5.5.2 The Disaster Recovery Plan

A DRP is a written and tested document which guides the organisation in the event of an interruption in service due to an unexpected or unplanned disaster (Janulaitis, 2007: 9). It does not document tasks but is an action plan that identifies policies, procedures and resources that are used to monitor and maintain corporate IT before, during and after a disaster (Hawkins, *et al.*, 2000). Hawkins *et al.* (2000) further add that a good DRP requires the participation of three functional areas, namely, management, human resources and IT which are involved in employee awareness, data security and safety of computer

technologies. Like other contingency plans, copies of the DRP should be secured and stored off-site in case the entire facility is destroyed (Samuelle, 2008: 348).

Holtsnider and Jaffe (2007: 521-522), Barndt and Schaefer (2003: 145), Rothstein (2007: 24), Samuelle (2008: 348), and Whitman and Mattord (2009: 228) all agree that a DRP should contain:

- Name of department or institution depending on who that particular plan applies to.
- Contact numbers of key personnel, customers and vendors.
- Diagrams and blueprints of the existing environment, maps and floor plans to critical emergency materials. This also includes procedures for declaring a disaster, re-establishing operations in disaster recovery mode, contacting key resources and identifying disaster recovery resources, step-by-step application and restoration, and details of licensing media.
- Location where people will meet during a disaster and an alternative data centre if current location cannot be used.
- Location of offsite facility with an up-to-date set of backups.
- A list of hardware in case it needs replacement. This may include servers, hubs, routers and workstations.
- Identified members of the organisation who can make decisions in the event of an emergency and be able to communicate activities and plans to the rest of the organisation.
- Schedule for testing and updating the plan as organisational needs, people, and technologies keep changing.

5.5.3 Crisis Management

Crisis situations often appear to happen suddenly and an organisation's assets which include people, intellectual property, facilities and reputation need to be protected (Heath, 2008: 51; Rozansky, 2009). In as much as people are core to business recovery, they are core to crisis management as there would be no crisis situations without people (Heath, 2008: 51).

Lerbinger (1997: 4) defines a crisis as an event that brings or has the potential for bringing an organisation into disrepute and endanger its future profitability, growth, and possibly, its survival. Failure to manage a crisis has led to the demise of many organisations. Statistics show that 43% of businesses that suffer a disaster never reopen, which is why crisis management is critical for an organisation (Rozansky, 2009; Cerullo and Cerullo, 2004). According to Heath (2008: 52), four elements indicate the presence of a crisis. These are missing or unreliable information, little time in which to act or respond, a threat to people or resources valuable to people, and resources required to resolve a situation exceeding available resources.

Crisis management involves four sides which according to Heath (2008: 57), include:

i. Managing processes involved in the preparation and development of crisis management.

ii. Dealing with the crisis situation.

iii. Looking after the organisation's stakeholders.

iv. Managing the communication processes involved such as enquiries from the general public and media.

5.5.4 Recovery Operations

There is no defined method for recovery after a disaster. Each organisation has to determine scenarios that are particular to its operations before it can define how to respond. If the physical facility survives after a disaster, the disaster recovery team can start rebuilding the operation to full capability (Whitman and Mattord, 2009: 229). If not, alternative actions should be put in place until a new facility is acquired. In the worst case scenario, if the disaster threatens the survival of the organisation, the transition from disaster recovery to a business continuity process should begin. Furthermore, every event that takes place during the recovery operations process needs to be recorded. (Whitman and Mattord, 2009: 229; Rittinghouse and Ransome, 2005: 165, 228).

5.6 Business Continuity Planning

A business continuity strategy should be in line with an organisation's risk tolerance levels, should be achievable given the manpower and budget allocated to it, and address the interests of the organisation and its shareholders (Garcia, 2008). A recovery strategy should focus on the business process and not the technological components of the process (Koch, 2004).

With the advent of cloud computing, business continuity planning can now be made easier as this method does not require a significant investment in physical infrastructure. Appropriate controls concerning privacy and regulatory requirements still need to be put in place to secure the information (Gatewood, 2009). Virtualisation can also be used to implement a much cheaper disaster recovery and business continuity process and help an organisation extend its recovery plans to services that previously may not have justified the expense of a continuity plan. It provides among other things, reliable failovers, maximised systems availability and streamlined backup processes (Microsoft, 2009; Dell, 2006).

Business continuity is an organisation-wide process and should not be driven by IT. Thus, it is pointless for an IT function to have a BCP in place to enable it to continue operating without the rest of the business to support. In the same way, the business requires a BCP in place to continue operating for the IT function to survive (Thompson, 2006; Musson, 2007: 185). Savage (2002) outlines the activities that should be encompassed in a business continuity planning process:

- Business risk and impact analysis.
- Documentation of activities necessary to prepare the organisation for possible emergencies.
- Identification and authorisation of activities needed for the disaster recovery phase and management of the business recovery process.
- Testing and auditing of the business recovery process.
- Training of staff involved in the business continuity process.
- Implementation of a process to keep the BCP up to date.

Schiesser (2003) suggests that there are eight (8) R's which define key steps in a business continuity process, before, during and after an event has occurred. These steps are outlined in table 5.2.

Table 5.2: Eight Key Steps to Business Continuity (Adapted from Schiesser, 2003; Stacey, 2006: 1557)

	Key Step	Activity
During an Event	**Response**	Initial reaction to an event which involves notification, emergency response and includes initial assessment
	Recovery	Determination of location, time-frame and amount of restoration required at temporary alternate site
	Resources	Deployment of hardware, software and people required for recovery
	Relocation	Movement of the data centre, support services and business staff
	Restoration	Revival of application and database management systems, network connectivity and desktop environment
After an Event	**Resumption**	Redeployment of resources for the resumption process and reverting back to original site or reconciling issues for a new site in production status
	Remediation	Identification of lessons learnt and provision of suggestions for improvement which will help in the transition from a reactive to a proactive environment
Before, During and After an Event	**Relationships**	Maintenance of relationships with internal and external customers and suppliers

A BCP can be written for a specific function or can address all business functions. There is no single recommended BCP. Each organisation has to develop one based on its functionality, processes and situation (Cerullo and Cerullo, 2004: 71). BCPs need to be updated whenever there is a change in personnel, legislation, business strategy, processes, stakeholders, team member contact details, risk, location, facilities and resources (ISO/IEC 27002, 2005). As a comprehensive BCP is large and complex, it may be worth adopting a commercial toolkit or template to act as a checklist and guide and ensure that all the necessary aspects are covered in the plan (Savage, 2002). A BCP should enable the business to resume operations quickly and fulfil its corporate mission (Tilley, 1995). It should also be clear and concise, easily understood at all levels, cover all critical aspects of business

functions with the right detail, kept up to date and tested regularly. Regular testing ensures the BCP retains its effectiveness (Maslen, 1996). Testing procedures and methods are discussed in section 5.8. A BCP is usually activated and executed concurrently with a DRP (Caballero, 2009: 235). Tilley (1995) further describes the development of a BCP to include:

- Identification of individuals, departments, external organisations, and procedures involved in the recovery process.
- Resources required for restoration to normal operations. Emergency telephone numbers, communication equipment and work area recovery. Work area recovery provisions can be made in hotels, homes, and disaster recovery sites (Gartner, 2009).

Furthermore, production, certification and distribution of a well detailed recovery plan are important components of the business continuity process. A BCP should be considered to be part of a wider process which includes risk management, hazard control, training and awareness, and testing (Maslen, 1996).

A study conducted by AT&T in 2002 to identify a formalised approach for business continuity came up with five (5) business continuity best practices:

- Apart from protection of tangible assets, critical elements of a business continuity process include communication with stakeholders, employee education and alternative work processes.
- The use of lessons learnt from mistakes of past incidents and disasters.
- Using managed third party providers to make use of emerging technologies and continuity needs.
- Testing and updating plans on a regular basis to keep them up to date and effective. An organisation with an untested BCP faces as much risk as that without one.
- Business continuity planning should be viewed as a value adding activity and not merely a cost to an organisation. A well-developed business continuity program is a source of reassurance and a positive element of brand positioning.

With the recurrence of pandemics such as N1H1 and Avian (Bird) flu, organisations also need to consider adding pandemic preparedness to their business continuity planning process (Coombs, 2008: 311; Gartner, 2009). A pandemic brings with it substantial impacts and challenges which range from business continuity disruptions, productivity losses due to absenteeism, personnel losses, disruptions in commodity markets to unusual medical and healthcare costs (Coombs, 2008: 310). An organisation should identify how services such as telecommuting, teleconferencing, videoconferencing, network and systems support, and customer support will be provided in the event of a pandemic. However, risks brought about by the increase in the use of technologies need to be managed as well (WHO, 2009: 17; Chandler, 2007: 117; Kennedy, 2006). Coombs (2008: 311) suggests a shift from the traditional method of addressing the protection of information technologies, data, equipment and buildings to the addition of global pandemics if the recovery plan is to be considered comprehensive and complete.

5.6.1 Continuity Strategies

An organisation can use cost and risk levels to determine its continuity strategy which can either be technical or business oriented (Whitman and Mattord, 2009: 230; Doughty, 2001: xvi). All too often, organisations place more emphasis on cost than the risk associated with the strategy. Before a continuity strategy is selected, a comprehensive risk evaluation and BIA should be carried out in order to identify core business processes and their dependencies. Four (4) continuity strategy options exist: alternate sites, time shares, service bureaus, and mutual agreements (Doughty, 2001: xvi).

5.6.1.1 Alternate sites

An organisation can move to this site in times of a disaster and continue with mission-critical operations (Stewart, 2004: 157). Three levels of alternate sites exist:

i. A hot site, which is a duplicate of the original site and has real-time moment-to-moment data so that business operations can continue without any downtime at all.

ii. A warm site usually includes major computer equipment and servers but not client workstations and requires a few days before it can be fully functional (Whitman and Mattord, 2009: 230).

iii. A cold site is an almost empty room with heating, air-conditioning and electricity where equipment and furniture can be delivered to construct a temporal processing capability (Broder, 2006: 190).

An organisation can also have a contract with a vendor to deliver equipment to the local site or an alternate site within three to five days. This is called *quick shipping* (Hawkins *et al*., 2000).

5.6.1.2 Time shares

A time share is a hot, warm or cold site leased in conjunction with another organisation. One advantage of time shares is that overall costs are reduced although the other organisation may also face a disaster at the same time and this may cause problems if it is a shared arrangement (Whitman and Mattord, 2009: 230).

5.6.1.3 Service Bureaus

A service agency provides the physical facilities in the event of a disaster and possibly off-site data storage at a fee (Whitman and Mattord, 2009: 231).

5.6.1.4 Mutual Agreements

A contract is drawn up by two organisations in which each party agrees to provide the necessary facilities, services and resources in the event of a disaster until the receiving organisation is able to recover (Whitman and Mattord, 2009: 231).

5.6.2 Offsite Disaster Data Storage

Both disaster recovery and business continuity rely on proper backup procedures. Backups must be tested in order to check if they are reliable and useable (Stewart, 2004: 156). According to Whitman and Mattord (2009: 231), an organisation must be able to move data into the new site's system in order to get it up and running after a disaster. Several options can get the new site up and running in a shorter period of time. These include:

- Electronic vaulting: transfer and archiving of data at another facility.
- Remote journaling: transfer of close to real-time online transactions without the data to an off-site facility.

- Data shadowing: storage of duplicate online transaction data and databases at a remote site on a redundant server.

5.7 Continuity Management

As part of the business continuity planning process, continuity management ensures that interruptions to business operations are mitigated and that key business processes required to support essential business functions are not interrupted (Bryson, 2006: 280).

5. 8 Continuity of Operations Plan

A Continuity of Operations Plan (COOP) focuses on restoring an organisation's essential functions at an alternate site for up to about 30 days until the organisation can return to normal operations (NIST, 2010). Although it is an organisation-wide document, a COOP, developed independent of BCPs does not typically include IT operations. With information now identified as a critical organisational asset, however, IT operations may now be included or the plan may have BCPs and DRPs as appendices. (NIST 2010; Rittinghouse and Ransome, 2005: 6). A Gartner survey of 359 information security and risk management professionals conducted in 2008 found that nearly 60% of organisations only plan for a 7-day outage instead of a 30-day outage (Gartner, 2008).

5.9 Consolidated Contingency Plan

Some small and medium sized organisations prefer to place the IRP, DRP and BCP into one document. This approach supports concise planning and encourages them to develop, test and use all the plans (Whitman and Mattord, 2009: 233). A team of AT&T researchers came up with a combined disaster recovery and business continuity framework as shown in table 5.3.

Table 5.3: Integrated Business Continuity and Disaster Recovery Framework (AT&T, 2002)

Team Chartering	Business Analysis	Define DRBC Strategy	Develop Detailed Plan	Implementation	Maintenance
Secure top-level commitment Establish a cross-functional DRBC Steering Committee Establish DRBC Core Team	Understand business objectives Identify business outputs, processes and resources Identify DRBC partners and roles Identify threats and risks Analyze business impacts	Define corporate-level DRBC strategy Define process-level DRBC strategy Define resource-level DRBC strategy Define funding and resources	Define scope of plan Document detailed requirements Design detailed DRBC Plan	Obtain approvals and buy-in Develop awareness and education Develop implementation documentation Assign roles and responsibilities Test implementation	Set up change management process Monitor performance Keep process up-to-date through performance monitoring, simulations, benchmarking and ensuring that new products, processes and acquisitions are added to the plan

5.10 Testing Contingency Plans

Whitman and Mattord (2009: 217) describe an untested plan as no plan at all. Contingency plans, therefore, need to be tested regularly to identify vulnerabilities, faults and inefficient processes. Rothstein (2007: 145-149) and Whitman and Mattord (2009: 217) outline the different strategies that can be used to test these plans:

- Desk Check or checklist: copies of the plan are distributed to individuals who will have been assigned roles for them to go through and create a list of correct and incorrect components.
- Structured walk-through: team members verbally walk though each component of the process as documented in the plans. This is in done as an on-site walk-through or a chalk-and-talk.
- Simulation: each team member works individually and simulates the performance of his own task to identify faults in the procedures. Normal organisational operations are not disrupted.

- Parallel testing: team members perform actual tasks and execute procedures without interrupting normal business operations. Historical transactions such as the previous day's transactions may be processed against the preceding day's backup files at the contingency site.

- Full interruption: The entire disaster recovery plan is activated as service is interrupted, data is restored from backups and appropriate individuals are notified. Unfortunately, this test may be too risky for businesses as it may turn into an incident and should, therefore, be done outside normal operating hours.

5.11 Contingency Planning in the Mining Industry

According to Seldon (2009), organisations are built on similar principles but each has unique characteristics in the way business is conducted and products and services provided. Seldon (2009) suggests there is at least one person, certain technology or information specific business processes and some critical infrastructure components that are critical to business operations. Seldon (2009) further suggests that, in times of disaster, manmade or natural, if their continuity has not been catered for, the business may fail. An organisation should, therefore, identify the critical components that need to be protected.

Contingency planning in the mining industry covers a lot of areas and issues and may involve production, distribution, IT and other functional areas (Musson, 2007: 185). All functional areas and not just IT should be catered for in the business continuity plan as they need to co-exist at any given time. Recovery in such industries also faces challenges which may not be found in other industries. These range from government regulations to certification and re-certification requirements such as ISO 9000 (Musson, 2007: 185; Warner, 2007).

It is vital for industries such as the mining industry to deploy a business continuity process that encompasses all areas of the enterprise including supplier and customer networks. A DRP and/or BCP should provide a solution that will account for and ensure the recovery of all business processes, an alternate workspace environment for employees, facilitate ongoing operations within a consistent timeframe and cover all regulatory requirements (Warner, 2007). Warner (2007) further goes on to say that in many cases, the amount of investment in a DRP or BCP could literally mean the difference between the business and its shareholders sinking or swimming. A Meta Group report in 2000 showed that metal and natural resource

industries can lose an average of $580,588 per hour in downtime costs. However, it is not only money that will be lost but also reputation, current and potential customers, and customer confidence (Hinton and Clements, 2002).

While business continuity planning across industries may have similar objectives, different industries have specific aspects that should be considered. A study on business continuity planning in manufacturing, financial, education, construction, transport, retail, utilities, and other industries was conducted by Pitt and Goyal (2004). This study highlighted the activities that are included in the business continuity planning process across industries. Zambian copper mines are represented by the activities of the manufacturing sector as shown in figure 5.4.

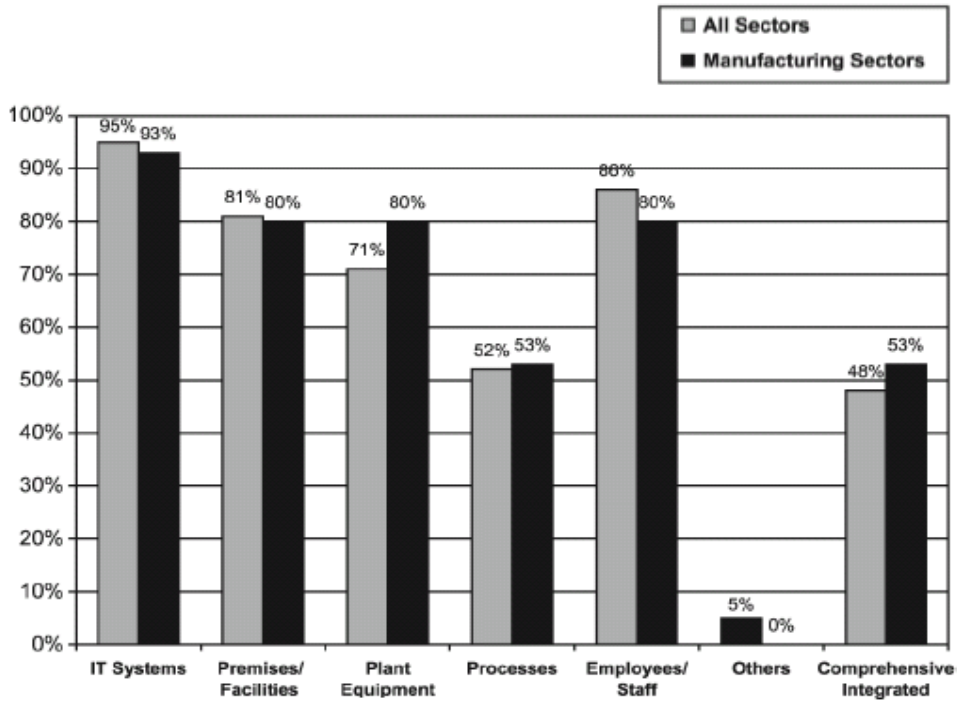

Figure 5.4: Activities included in Business Continuity Planning across Industries (Pitt and Goyal, 2004)

Musson (2007: 186) suggests that a business continuity plan in the mining industry and related industries should consider and accommodate:

- Different areas and functions of the organisation, ranging from manufacturing and related supply/chain and logistics functions, office and work area, to data centre.

- Links between production and business/data processing functions such as ERPs and CAD.
- Multiple strategies to be considered at the time of disaster.
- Lack of actual fixed recovery locations.
- Recovery strategies that are more business related than technologically related.
- Determination of a clear distinction between an every-day emergency and a disaster.
- Dependency on outside sources or services.
- Links between business and data processing functions.

As mining companies face emergencies as part of their daily operations, there is a need to distinguish between an emergency and a disaster. The BCP should outline disaster qualifying criteria (Musson, 2007: 186).

An energy and resources industry survey conducted by Deloitte Touche Tohmatsu in 2008 revealed that in as much as energy and resource industries play a critical role in providing continuity, operation and quality of life in the communities they serve, hence the need for a formal BCP, only 45% have BCPs that will enable them to recover critical systems. As a BCP can quickly lose its usefulness by becoming obsolete and through lack of staff awareness, it has to be regularly tested and updated for the purpose of relevance and appropriateness. However, only 10% of the respondents in the survey indicated that all elements of the BCP are regularly tested. Almost all respondents to the survey said industry-specific control systems are critical to business success yet the majority did not have programmes in place to assess that security (DTT, 2008).

A survey conducted by PricewaterhouseCoopers in 2008 on the global state of information security revealed that business continuity and disaster recovery was the top most reason why organisations have continued investing in information security. This means even though few organisations have formal contingency plans in place, they are working towards developing some (PricewaterhouseCoopers, 2008). Helberger (2009) further recommends the review and testing of pandemic response plans as well as development and testing of an effective

incident response program as two of the ten information security and compliance activities organisations should focus on for 2010.

A Gartner hype cycle report on business continuity management showed that continuous email communication is top priority in most organisations and demand for wireless email services is now increasing as emails are now the most critical mode of communication in organisations (Gartner, 2009). It further identified new technologies that improve disaster recovery management and reduce operational costs. These include server virtualisation, IT-service failover and bare-metal recovery (recovery to a workstation or server that has no previously installed software or operating system) (Gartner, 2009).

Mining is an inherently dangerous business where even the most safety conscious mines should expect a disaster. A crisis communications plan should, therefore, be implemented and regularly tested as it may have to be invoked (ICMM, 2009). Mining organisations also perform incident management using Virtual Reality (VR) systems. These systems are used to simulate scenarios and identify possible hazards in both training and testing modes. This helps in identifying possible incident scenarios before they occur and finding ways of preventing or minimising them (Karmis, 2001: 168).

An Ernst & Young 2008 report on strategic risks faced by the mining and metals industry recommends an annual risk assessment which goes beyond financial and regulatory risk to the strategic environment in which the organisation operates. This includes placing effective controls on mergers and acquisitions, IT effectiveness, business continuity planning and transaction integration (Ernst & Young, 2008).

5.12 Conclusion

Business processes drive today's organisations. These organisations consist of integrated business processes, process participants and infrastructure and the resources supporting them (Vancoppenolle, 2008: 24). Business continuity planning is now, therefore, no longer a luxury for an organisation but is an essential element of the risk management process (Doughty, 2001: xi). Smooth execution of a well-constructed BCP will minimise losses incurred by an organisation as well as the impact on employees and customers and ensure that an organisation maintains its highest operational state under the circumstances (La Fazia, 2004). People are the power behind an enterprise but technology is the tool that enables them

to function. It is important, therefore, that people and technology are in place to facilitate effective business continuity should a contingency arise (Tilley, 1995).

Chapter 6

Information Security Governance

This chapter discusses information security governance and how it fits into the broader picture of corporate governance. It also takes into account the major role people play in the information security process, as well as the regulatory requirements that come with protection of information assets.

6.1 Introduction

Information security is not only a technical issue but a business and governance challenge that involves adequate risk management, reporting and accountability (ITGI, 2006: 8). The information security process is made up of three pillars; namely people, processes, and technology. People are the most critical of these pillars as they are the users of technology and processes (Nicastro, 2006; Mark, 2007). These three pillars need to be included in information security programs as they enhance the development of a better capability for governance (IT Governance Network, 2009). Information security has become essential to corporate success due to organisations' growing dependence on information and information systems. As a result, information assets have become an integral component of operations in organisations (Andersen, 2001; Brotby, 2009a: xiii). Computing is now conducted at anytime and in any place by employees, contractors or business partners using devices that include Personal Digital Assistants (PDAs), Blackberry devices, cellphones, laptops, and notebooks (Krehnke, 2007: 40). Hence, organisations' focus on the confidentiality, integrity and availability of information and the need for governance has increased. Corporate governance has, therefore, been extended to include information security as it has now moved away from being a technical issue to being a corporate one (Mears and von Solms, 2004). This extension has made information security a corporate governance responsibility (von Solms and von Solms, 2006; Andersen, 2001). For this to be effective, the board of directors and senior executives need to be actively involved in the governance process (IOD, 2009: 82).

6.2 Information Security Governance

O'Donovan (2003) defines corporate governance as an internal system which encompasses policies, people and processes, and serves the needs of shareholders and other stakeholders, by directing and controlling management activities with good business intellect, objectivity and integrity. The Organisation for Economic Cooperation and Development (OECD) (OECD, 2004) further defines corporate governance as "the system by which business corporations are directed and controlled". According to Arjoon (2005), corporate governance includes the relationship an organisation has with its shareholders and society, promotion of fairness, transparency and accountability, and manager governing mechanisms for managers to ensure that the actions they take are consistent with the interests of stakeholders.

IT governance on the other hand, deals with the application of technology to business problems and addresses how and to what extent this application adds value to the business (Poore, 2007: 90; Krehnke, 2007: 37). Peltier *et al.* (2005: 240) define Information Security Governance (ISG) as the management structure, organisation, responsibility, and reporting processes surrounding a successful information security program. Von Solms and von Solms (2009: 24, 26-27) further define information security governance as the system by which the confidentiality, integrity and availability of an organisation's electronic assets are maintained. They suggest that both information security governance and IT governance fall under corporate governance. Some concepts of information security governance such as the legal and regulatory framework, however, do not necessarily fall under IT governance but are part of corporate governance. Hence, information security governance is not completely part of IT governance. Figure 6.1 illustrates this relationship.

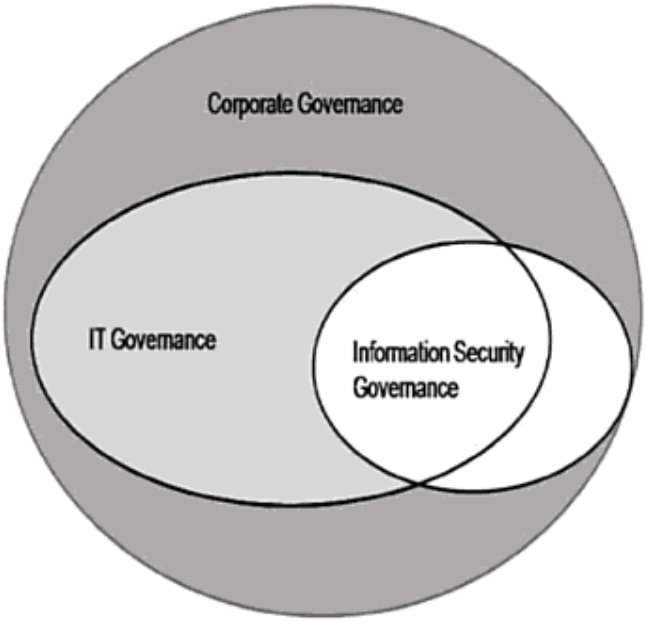

Figure 6.1: Relationships between Corporate Governance, IT Governance and Information Security Governance (von Solms, 2009: 30)

As organisations need to deal with an increasing number of policies, regulations and laws, an information security governance framework is required so that the organisation can consider information security to be part of the overall strategic planning process (Moreira *et al.,* 2008). Moreira *et al.* (2008) further suggest an information security governance framework that is organised into three (3) levels; namely, strategic, tactical and operational. According to

Bernardes (2005) in Moreira *et al.* (2008), these levels will allow the evolution of data (operational level) to information (tactical level) and subsequently, to knowledge (strategic level). This knowledge can then be used by managers in the strategic planning process. In order to maximise the value of the knowledge gathered, however, the framework must be structured to consider controls, people, proceses and technology (Moreira *et al*., 2008).

In their paper, von Solms and von Solms (2004) outline ten (10) essential aspects of information security governance which can be used as a checklist by an organisation to ensure that a comprehensive information security plan has been drawn up. They suggest that top management has a direct corporate governance responsibility to protect information assets in an organisation; otherwise, the organisation may be liable to financial and legal implications. These factors, referred to as information security 'sins' are outlined below:

i. Not realising that information security is a corporate governance responsibility.

ii. Not realising that information security is a business issue and not a technical issue.

iii. Not realising the fact that information security governance is a multi-dimensional discipline.

iv. Not realising that an information security plan must be based on identified risks.

v. Not realising (and leveraging) the important role of international best practices for information security management.

vi. Not realising that a corporate information security policy is absolutely essential.

vii. Not realising that information security compliance enforcement and monitoring is absolutely essential.

viii. Not realising that a proper information security governance structure is absolutely essential.

ix. Not realising the core importance of information security awareness amongst users.

x. Not empowering information security managers with the infrastructure, tools and supporting mechanisms to properly perform their responsibilities.

According to ISACA (2008: 87), ITGI (2006: 11), Brotby (2009a: 33) and Williams (2001), basic outcomes in information security governance include:

i. Strategic alignment of information security with business strategy to support organisational objectives.
ii. Risk management by executing appropriate measures to manage and mitigate risks and reduce potential impacts on information resources to an acceptable level.
iii. Resource management by utilising information security knowledge and infrastructure efficiently and effectively.
iv. Performance measurement by measuring, monitoring, and reporting information security governance metrics to ensure that organisational objectives are achieved.
v. Value delivery by optimising information security investments in support of organisational objectives.
vi. Process integration by de-fragmentation of the organisation's security management assurance process in order to improve overall security and operational efficiencies.

6.2.1 Information Security Management and Information Security Governance

Information Security Management (ISM) falls under information security governance and is, therefore, part of information security governance. Information security governance starts from the top and includes all employees in an organisation while information security management may not be institution-wide (von Solms and von Solms, 2009: 25; Bergsma, 2009). Whereas, information security management deals with strategising and making decisions in order to mitigate risks, information security governance deals with determining who is authorised to make those decisions and aligning strategies with business objectives and regulations (Bergsma, 2009). Table 6.1 lists the aspects that make up both information security governance and information security management.

Table 6.1: Comparison between Information Security Governance and Information Security Management (Bergsma, 2009)

Governance	Management
Oversight	Implementation
Authorises decision rights	Authorised to make decisions
Enact policy	Enforce policy
Accountability	Responsibility
Strategic planning	Project planning
Resource allocation	Resource utilisation

6.3 Information Security Governance Pillars

Mears and von Solms (2004) and Krehnke (2007: 41-43) define the factors that make up the pillars of information security governance. They all agree that these factors include accountability and responsibility, ethics, resource allocation and management, security awareness and education, information security policies, good practice standards, risk management, compliance with legal requirements, and information sharing.

6.3.1 Accountability and Responsibility

According to the King Report (IOD, 2009: 21), accountability and responsibility are two of the four ethical values underpinning good corporate governance. The board of directors, senior executives and other individuals in an organisation should also be responsible for the assets and actions of an organisation and be willing to take corrective action so that the organisation stays on an ethical and sustainable strategic path (ISACA, 2008; ITGI, 2006). Accountability involves safeguarding information during critical business activities such as mergers, acquisitions, business process recovery, and regulatory response (ISACA, 2008).

6.3.2 Ethics

The King Report (2009, 21) suggests four ethical values that support good corporate governance in an organisation. These values are responsibility, accountability, transparency and fairness. Transparency ensures that the right amount of information is availed to stakeholders to enable them to make sound decisions. Fairness ensures that fair consideration

is given to the interests and expectations of stakeholders. Accountability and responsibility are discussed in section 6.3.1.

In information security governance, however, ethical issues include the user's need for privacy, the public's right to know, and the organisation's need to protect proprietary information (Newman, 2009: 19). Ethical compliance contributes to stability and growth of an organisation as it instils confidence in the customers, stakeholders, and shareholders (Arjoon, 2005). Mason (1986) in Forcht (1994: 324) suggests privacy, accuracy, property and accessibility as the four (4) ethical issues of the information age. Tippett (2007: 690) outlines an action plan that can help an organisation encourage ethical use of computers and information systems. These include:

- Development of a computer ethics policy to supplement the computer security policy.
- Ensuring the organisation has an email policy and employees are made aware of what it is.
- Determining whether the organisation has a business ethics policy and expanding it to include computer ethics.
- Development of a corporate guide to computer ethics for an organisation and implementation of employee awareness programs.

6.3.2.1 Codes of Ethics and Professional Organisations

For many businesses, one of the driving forces behind the creation of security policies is compliance with the law (Paquet, 2009: 19; Krehnke, 2007: 42). Ethics involve moral principles which are often formalised into *'codes of ethics'*. Codes of ethics encourage employees to act responsibly in the implementation of information security practices (Mears and von Solms, 2004). There are a number of formalised codes for information security professionals as ethics are also rules or standards governing the conduct of members of a profession (Paquet, 2009: 20). These include:

- Generally Accepted System Security Principles (GASSP).
- International Information Systems Security Certification Consortium, Inc (ISC)^2.
- Information Systems Security Association (ISSA).

- Internet Access Board (IAB).
- Institute of Electrical and Electronic Engineers (IEEE).

As the Internet has no geographical boundaries, or national or cultural lines, it is difficult to enforce laws that apply to all users. Thus, it is the responsibility of groups, companies, organisations, service providers, and even countries to establish codes of ethics that Internet and computer users should strive to live by and achieve (SANS, 2002; Srinivas and Malik, 2009). The Computer Ethics Institute (CEI) is one of the organisations that have developed a code of ethics known as *the ten commandments of computer ethics* which it believes computer users should abide by (CEI, 2009). These commandments are outlined below:

i. Though shall not use a computer to harm other people.
ii. Thou shalt not interfere with other people's computer work.
iii. Thou shalt not snoop around in other people's computer files.
iv. Thou shalt not use a computer to steal.
v. Thou shalt not use a computer to bear false witness.
vi. Thou shalt not copy or use proprietary software for which you have not paid.
vii. Thou shalt not use other people's computer resources without authorisation or proper compensation.
viii. Thou shalt not appropriate other people's intellectual output.
ix. Thou shalt think about the social consequences of the program you are writing or the system you are designing.
x. Thou shalt always use a computer in ways that ensure consideration and respect for your fellow humans.

6.3.3 Employee Security Awareness and Education

Employees should be encouraged to adhere to the behaviour specified by management so that they contribute to the success of an organisation. This behaviour should eventually become part of corporate culture, which as defined by Schein (2004: 17) is a pattern of shared basic

assumptions that a group has learnt throughout history. Corporate culture influences the security strategy in the same way that the security strategy in the long run shapes the organisation's culture towards security (Wang, 2005).

Whitman and Mattord (2009: 206) suggest the implementation of a Security Education and Training Awareness (SETA) program in an organisation to emphasise the importance of information security. Table 6.2 illustrates a comparative framework of SETA which can be used to determine whether an employee requires awareness, training or education.

Table 6.2: Comparative Framework of SETA (NIST, 1995)

	AWARENESS	TRAINING	EDUCATION
Attribute:	"What"	"How"	"Why"
Level:	Information	Knowledge	Insight
Objective:	Recognition	Skill	Understanding
Teaching Method:	Media - Videos -Newsletters -Posters, etc.	Practical Instruction - Lecture - Case study workshop - Hands-on practice	Theoretical Instruction - Discussion Seminar - Background reading
Test Measure:	True/False Multiple Choice (identify learning)	Problem Solving (apply learning)	Eassay (interpret learning)
Impact Timeframe:	Short-term	Intermediate	Long-term

According to ISO/IEC 27002 (2005), security awareness, training and education should be designed to suit the employees' job role, skills, and responsibilities and should make them aware of known threats, contact persons and incident reporting channels. Whitman and Mattord (2009: 206) suggest that education, training, and awareness is required as employees are the first line of defence in any operation and are a critical factor in information security.

6.3.3.1 Employment Policies and Practices

In order for information security to be taken seriously and where necessary enforced, it should be part of every employee's job description. This is done through liaison between the human resources department and information security personnel (Whitman and Mattord,

2009: 492). Whitman and Mattord (2009: 492-498) suggest that, information security should form part of the employment process when hiring personnel. These hiring factors include:

- Job descriptions and interviews.
- Background checks on past criminal offences.
- Employment contracts and non-disclosure and monitoring agreements.
- Induction procedures for new employees.
- On-the-job security training.
- Information security components in employee performance evaluations.
- Termination procedures.

6.3.3.2 Security Considerations for Non-employees

Individuals such as temporary and contract employees, consultants, and business partners may not be subject to rigorous screening, contractual obligations and secured termination in an organisation, yet they have access to sensitive information and may become security risks. These individuals should equally be asked to sign non-disclosure agreements (Whitman and Mattord, 2009: 498; Calder and Watkins, 2006: 105).

6.3.4 Information security policies

According to ISO/IEC 27002 (2005), information security can only be achieved if a suitable set of controls is implemented. These controls include policies, procedures, processes, organisational structures, and software and hardware functions. In as much as an information security policy is the least expensive, it is often the most difficult to implement (Caballero, 2009: 225). A security policy as defined by Whitman and Mattord (2009: 174) is a plan or course of action intended to influence and determine an organisation's decisions, actions, and other matters. It is the backbone of information security and it provides the structure and purpose for all other aspects of information security (Peltier *et al.,* 2005: 17). This policy, according to Wessels *et al.* (2007: 233), needs to be continuously reviewed to ensure it still meets the organisation's confidentiality, integrity and availability needs.

Writing an information security policy depends on an organisation's control objective which as defined by IT Governance Institute (ITGI, 2006) is a "*statement of the desired result or purpose to be achieved by implementing control procedures in a particular process*". An information security policy must cover administrative, legal, managerial and technical requirements (Kadam, 2007). Control objectives can be selected from a standard such as ISO 27001, a framework such as COBIT, or a compliance requirement such as a national data protection act.

Information security policies can be classified into policies for a target group, by topic and by department. Implementation of a security policy also involves preparation of a report to be presented to management which includes a project plan with details of implementing new techniques and equipment, training plans, specific implementation and reporting activities, and Return on Security Investment (ROSI) (Kadam, 2007). An effective information security program approved and implemented by management will help protect the integrity and value of an organisation's data (Whitman and Mattord, 2009: 40; Myler and Broadbent, 2006). Such a program will reflect management's commitment and support for information security and the role it plays in reaching an organisation's vision and should form part of corporate culture (Thomson and von Solms, 2004; ISO/IEC 27002, 2005).

An organisational security policy can be a single document covering all aspects of the organisation or can be divided into a set of policies such as email usage, internet usage, wireless networks, mobile devices, encryption, and malicious software security policies. Having a set of policies in place makes it easier to enforce security management.

6.3.5 Resource Allocation and Management in the IT Security Arena

Allocation of resources for information security should be done in the same way as allocation of other assets in an organisation (IIA, 2001). The corporate asset management program, capital budget, contract management, and resource allocation and planning process can be applied to information security resources (Krehnke, 2007: 42).

6.3.6 Best Practice Standards

Best practice standards are implemented in order to ensure that an organisation has best practices in place that are up to par with other organisations. Implementation of best practice

standards also builds confidence and trust in the organisation's operations by the stakeholders and helps evaluate the level of information security in the organisation (Fitzgerald, 2007: 16).

International guidelines have been developed by the OECD, the International Corporate Governance Framework, Open Compliance and Ethics Group (OCEG), Information Technology Infrastructure Library (ITIL), IT Governance Institute (ITGI), Information Systems Audit and Control Association (ISACA) (Cobit and Val IT), ISO 38500 and the Commonwealth Association for Corporate Governance (King Report, 2001; King Report, 2009; Fitzgerald, 2007: 16). Best practice standards are discussed further in chapter 7.

6.3.7 Risk Management, Measurement and Controls

Information security risk management roles and responsibilities need to be assigned to ensure accountability (Mears and von Solms, 2004). The process of risk management and its controls was discussed in chapter 4.

6.3.8 Compliance with Legal Requirements

Individual countries have different information security regulations. As business is now being conducted across borders on the internet, however, it is important to expose an organisation to international laws as these may even influence the controls the organisation puts in place. These laws and regulations further hold executives accountable for information security governance (Wessels *et al.*, 2007: 251-252).

Organisations and governments require privacy laws to prevent information about employees from being collected, stored, and disseminated without authorisation (Whitman and Mattord, 2009: 91). Privacy involves providing protection for personally identifiable information relating to an individual and should be built into organisational policies, procedures and standards (ISACA, 2008: 375,538). The Zambian government recently enacted an Information and Communication Technologies Act which is meant to protect the rights and interests of providers and consumers alike and repeal the Telecommunications Act of 1994 which caters for the same (National Assembly of Zambia, 2009). Organisations should, therefore, ensure that employees' data receive the same level of protection as other important data in the organisation such as intellectual property (Whitman and Mattord, 2005: 482).

Organisations deal with a variety of third-party material to which Intellectual Property Rights (IPR) in form of copyright, trademarks and design rights may be applied (Calder and

Watkins, 2006: 324). Whitman and Mattord (2009: 43) define Intellectual Property (IP) as "*the ownership of ideas or control over the tangible or virtual representation of those ideas*". Intellectual property rights include software or document copyright, patents, design rights, trademarks, and source code licences (ISO/IEC 27002, 2005; Whitman and Mattord, 2009: 43). According to ISO/IEC 27002 (2005), legislative, regulatory, and contractual requirements may restrict copying of proprietary material and may require that only licensed material or that provided by the developer to the organisation may be used. Appropriate procedures, therefore, need to be implemented to ensure compliance with regulatory, legislative and proprietary requirements on the use of materials which may have intellectual property rights or proprietary software products (ISO/IEC 27002, 2005). The World Intellectual Property Organisation (WIPO) was formed in 1967 to encourage countries to adopt and enforce laws pertaining to intellectual property (Marlin-Bennett, 2004: 48; WIPO, 2009).

6.3.9 Information Sharing

Organisations can learn from each other's successes and failures by sharing them at workshops, conferences and industry groupings, and through working with regulatory bodies (Mears and von Solms, 2004).

6.4 Senior Management's Perception of Information Security

Senior executives are the key players in information security governance as the success of information security lies in their hands. Kajava *et al.* (2006b) and Lindström and Hägerfors (2009) point out that the key component of the information security process is visible support and engagement of senior management. As discussed in section 1.3, lack of awareness and understanding of information security in organisations by senior management is confirmed in the decisions that are made concerning development, implementation, and training (Lindström and Hägerfors, 2009). Close co-operation between security experts and senior management is required to make efficient use of information security for competitive advantage (Anttila *et al.*, 2004). Kajava *et al.* (2006b) propose an information security awareness model for senior management that incorporates the following aspects:

- Understanding their roles as business leaders.

- Defining critical assets that must be protected, and having an understanding of information classification schemes.
- Pledging a holistic commitment to information.

6.5 Benefits of Information Security Governance

A number of benefits can be derived from information security governance (ITGI, 2006: 13). These include:

i. Increased share value for the organisation and a level of assurance that critical decisions are not based on faulty information.
ii. Structure and framework required to optimise a limited allocation of resources.
iii. An assurance of information security policy and policy compliance.
iv. Increased predictability and reduced uncertainty of business operations due to definable and acceptable levels of information security-related risk.
v. Protection from increasing potential for civil or legal liability which are as a result of information inaccuracy.
vi. A firm foundation for efficient and effective risk management, process improvement, and rapid incident response.
vii. Accountability for information safety during critical business activities such as mergers, acquisition, business process recoveries, and regulatory response.

6.6 Information Security Governance in the Mining Industry

A Deloitte Touche Tohmatsu survey conducted in 2008 on information security in the energy and resources industry revealed that 53% of the organisations surveyed had formal information security governance frameworks and strategies in place. These frameworks are, however, at risk of being undermined as they usually lack management involvement and do not receive adequate input to align them properly with corporate objectives (DTT, 2008). Figure 6.2 illustrates the state of the information security governance framework in the industry.

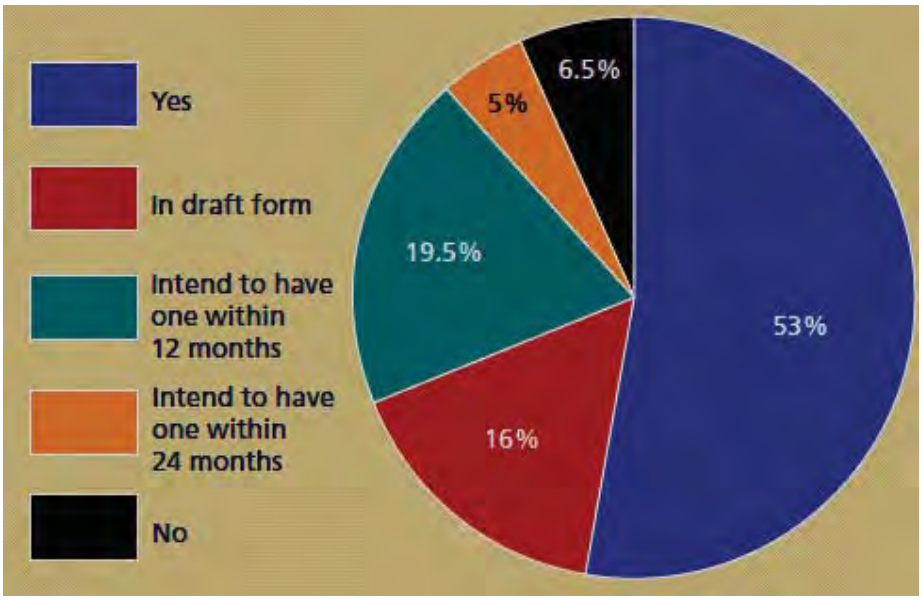

Figure 6.2: State of information Security governance framework (DTT, 2008)

In the same survey, corporate governance was found to be highest on the list of factors influencing compliance with security requirements in the industry (DTT, 2008). This is illustrated in figure 6.3.

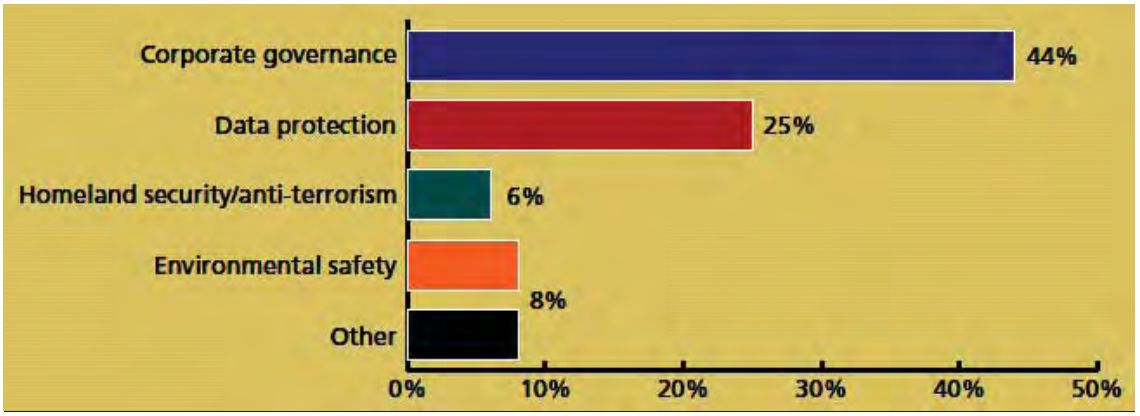

Figure 6.3: Factors influencing compliance with security requirements (DTT, 2008)

In 2009, PricewaterhouseCoopers also conducted a 2010 global state of information security survey on the mining and energy industry, which revealed that compliance and regulatory requirements are still a driving force in the industry's information security function. As 2009 was part of the period of the world's greatest economic turmoil in decades, increased security risks due to weakened business partners and suppliers and increased risks to company data due to employee layoffs were also cited as some of the impacts the economic downturn has

had on the industry. This has further increased the need for information security governance (PWC, 2009).

The Zambian government has enacted a number of laws, policies, and acts which are meant to provide for information security and to which mining organisations and its employees like every other entity in the country has to adhere to. These include:

- National ICT Policy: part of this policy is meant to provide security to government, business and individual information passing through public and private networks and communication systems (Ministry of Communications and Transport, 2006).
- Electronic Communications and Transactions Act: this is meant to cater for the security of electronic communication and repeal and improve on the Computer Misuse and Crime Act of 2004 (National Assembly of Zambia, 2009).
- Copyright and Performance Rights Act No. 44 of 1994: This act is meant to provide copyright protection for computer programs and others such as audiovisual and literary works (GRZ, 1994; Campbell, 2008: 260).

Employees in the mining industry also make use of mobile devices such as two-way radios (EPA, 2007), iPhones and Blackberry handsets, and laptops which create a security loophole in the organisation. Security strategies, employee training and awareness, and a revised IT infrastructure will help achieve effective mobile security governance (Zhang, 2009).

Induction programs for new employees and subsequent training for other employees needs to have information security awareness integrated in them to familiarise new employees with the organisation's policies and procedures and information systems that are in place in the organisation (Yakovleva, 2005: 56; Palabora, 2005; InfoSecurity, 2009; DTT, 2008).

As a member of WIPO and the African Regional Intellectual Property Organisation (ARIPO), Zambian organisations and individuals are liable to legal, regulatory, and contractual requirements for intellectual property (WIPO, 2009; ARIPO, 2009).

6.6 Conclusion

Failure in corporate governance threatens the future of every organisation (Arjoon, 2005). Information security should, therefore, be an integral part of corporate governance, aligned

with IT governance and integrated into strategy, concept, design, implementation and operation (ITGI, 2006: 15). In the same way that corporate governance is supported by management, so should all aspects of information security governance. Management should have a full understanding and be visibly involved in the information security process. Implementation of best practice standards is also important in order to ensure that an organisation's information security governance practices instil confidence in the stakeholders, shareholders and customers (Brotby, 2009b: 84). Ethics are equally an essential ingredient for business success and will continue to serve as the blue print for success in the 21st century (Arjoon, 2005).

Chapter 7

Information Security Standards and Models

Chapter 6 discussed information security governance and outlined best practice standards as one of the pillars of information security governance. This chapter describes information security standards and models, outlining best practice methods, principles and objectives.

7.1 Introduction

As discussed in chapter 6, organisations have had to deal with an increasing need for the fulfilment of information security governance requirements such as risk management and information security policies. This has influenced the need for organisations to examine control structures and ensure that they are in place and operating effectively (Fitzgerald, 2007: 7). One of the contributing factors is that organisations have been increasingly linking their networks to the Internet and with business partners (ISO 27002, 2007; Kizza, 2005: 285; von Solms, 1999). Information security policies, therefore, are no longer good enough to influence the behaviour of users both within and outside the organisation (von Solms, 1999). Although there may be national regulations that organisations should follow, there are no particular defined mandatory information security best practices or blueprints that an organisation has to put in place to cater for both internal and external users. Creation and maintenance of a secure environment requires implementation of a security plan as well as a management model to execute and maintain that plan (Whitman and Mattord, 2004: 210). An organisation will have to adopt a blueprint or select from a number of available frameworks and models that meet the organisation's needs (Upfold, 2005: 64). Blueprints are used to identify, develop and design security requirements, and should be customised to fulfil organisational security requirements which are based on legal and regulatory obligations, and business drivers (Harris, 2007: 78). According to Harris (2007: 79), blueprints lay out security solutions, processes and components that an organisation uses to match its security and business needs and set the foundation for a strong information security program that will cater for all stakeholders of the organisation's information and information facilities.

7.2 Information Security Best Practices

Models and frameworks provide high level guidance in the implementation of an information security program. One way to create a blueprint is to look at what other organisations have implemented and follow their best practices or industry standards (Whitman and Mattord, 2010: 213).

Some of the terminologies surrounding information security blueprints are outlined below:

- **Best Practices:** "*security efforts that seek to provide a superior level of performance in the protection of information*" (Whitman and Mattord, 2010: 249).

- **Guideline:** a description that clarifies what should be done and how to achieve the objectives set out in policies (ISO/IEC 27007, 2007).
- **Baseline:** "*specific rules necessary to implement the security controls in support of the policy and standards that have been developed*" (Fitzgerald, 2007: 15).
- **Procedures:** step-by-step instructions that describe how to use standards, baselines and guidelines to implement specified countermeasures that support policies (Bragg, 2002: 210; Fitzgerald, 2007: 14).
- **Domain:** managerial concepts that are used to limit the scope of a particular security policy (Kent and Williams, 1996: 322) or "*a set of subjects, their information objects, and a common security policy*" (NIST, 2001).
- **Code of Practice: "***a set of rules according to which people in a particular profession are expected to behave*" (MSN, 2009).
- **Processes:** activities, tasks and procedures performed across multiple organisations to implement company policies and standards (Coombs, 2008: 14).

Policies define high-level requirements which are generic enough to be applied to a variety of situations. Standards and procedures translate these high level requirements into implementation details (Purser, 2004: 131). An information security guideline is a generic statement designed to achieve policy objectives by providing a framework within which to implement procedures. A guideline is not mandatory but an organisation should consider adopting one as part of its information security best practices (Peltier, 2002: 26). Policies communicate management's expectations which are fulfilled through the execution of procedures, standards, baselines and guidelines (Peltier, 2002: 25). Figure 7.1 illustrates this relationship.

Figure 7.1: Relationships amongst policies, procedures, standards, baselines and guidelines (Fitzgerald *et al.*, 2007: 9)

As illustrated in figure 7.2, standards, best practice frameworks, and implementation plans such as policies perform different roles but are related. A standard can, therefore, be used in conjunction with a framework as well as policies, procedures and processes (Clinch, 2009). Standardisation reduces complexity by limiting the number of ways in which something can be done, provides a documented preference when a choice has to be made, and helps ensure interoperability (Purser, 2004: 143).

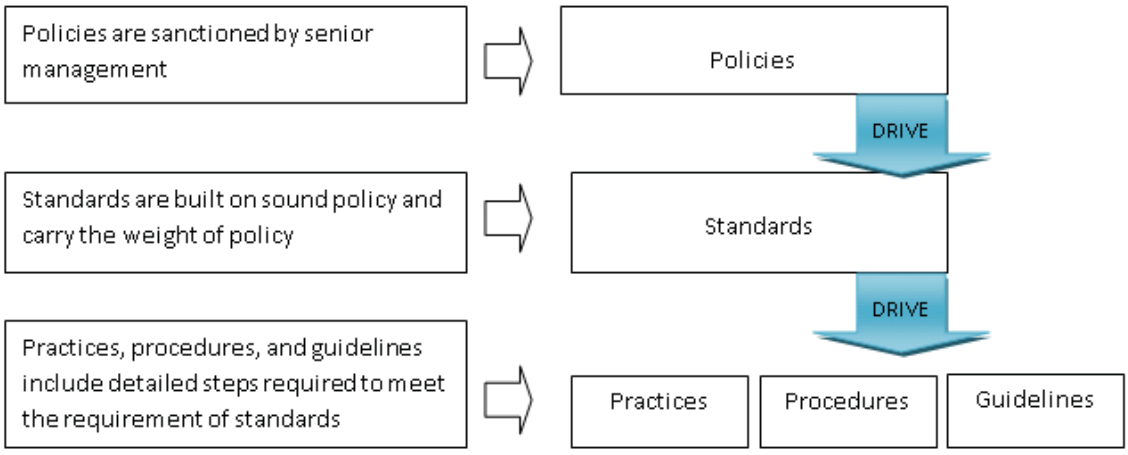

Figure 7.2: Policies, Standards and Practices (Whitman and Mattord, 2009: 174)

7.3 Information Security Models and Frameworks

A security model is a flexible, scalable, robust, and sufficiently detailed generic blueprint offered by a service organisation which expresses a system's security requirements precisely (Whitman and Mattord, 2010: 213; Russell and Gangemi, 1991: 108).

An information security framework is an outline of an organisation's overall security strategy and a roadmap for planned changes to the organisation's information security environment. It provides a more thorough outline of a blueprint (Whitman and Mattord, 2009: 186).

This section discusses some of the most widely used information security models and frameworks:

7.3.1 ISO/IEC 27002:2005/17799:2005: Code of Practice for Information Security Management

ISO/IEC 27002: 2005 (ISO 27002) was initially the U.K. Department of Trade and Industry Code of Practice (CoP) for information security which was introduced in 1993. This was later changed to BS 7799 in 1995 and later to BS 7799-1 in 1998. BS7799-1 was then adopted as an ISO standard called ISO/IEC 17799 in 2000. ISO is arguably known to be the best standards organisation in the world (Purser, 2004: 145). ISO 27002 replaced ISO 17799 in April, 2007 (Praxiom, 2008, Calder, 2006). This standard has over the years become the *de facto* standard for high level definition of an information security management system as it defines a comprehensive set of controls that help organisations implement a good information security program (Wessels *et al.*, 2007: 253). ISO/IEC 27002 contains 134 detailed information security controls based on 11 areas and provides 39 control objectives which are meant to protect organisations' information assets against threats to their confidentiality, integrity and availability (IsecT, 2010). It also serves as a common basis and practical guideline for developing organisational security standards and best practice information security measures (ISO, 2010). ISO has plans of developing an industry specific version of the ISO 27002 standard (ISO 27000 Directory, 2008).

ISO 27002 consists of eleven (11) domains which can be categorised into administrative, technical and physical domains (Upfold, 2005: 72-78). These domains, according to ISO/IEC 27002 (2005) are outlined below:

7.3.1.1 Administrative Domains

- **Information security policy:** An information security policy illustrates management's commitment to information security and should be in accordance with business requirements and legal regulations. This policy must be published and communicated to all employees and external parties.

- **Organising information security:** A management framework is required to initiate and control the implementation of information security within an organisation. Access to an organisation's information and information processing facilities should also be controlled.

- **Asset management:** This is required to achieve and maintain adequate protection of information assets. All organisational assets should be explicitly identified and classified, and an inventory drawn up and maintained, and responsibility and ownership defined.

- **Human resources management:** Organisations should ensure that information security roles and responsibilities of employees, contractors, and third-party users are defined, before, during, and after employment. A code of conduct covering confidentiality, ethics, and protection of information assets is required. Information security education, training and awareness and formal disciplinary procedures for information security breaches should be implemented.

- **Business continuity management:** This is meant to offset interruptions to business activities and protect critical business processes from the effects of major failures and disasters and ensure timely resumption of these processes. A business continuity framework should be maintained to ensure that all plans are consistent enough to address information security requirements and identify priorities for testing and maintenance.

- **Compliance:** As an organisation's use of information systems may be subject to statutory, regulatory or contractual obligations, all legal requirements should be explicitly defined and documented. Intellectual Property Rights (IPR) and privacy policies also need to be defined. Important organisational records and information

system audit tools should be protected from loss, destruction or falsification according to legal requirements.

- **Information security incident management:** This ensures information security events and weaknesses are communicated in a timely manner and through appropriate channels so that corrective action can be taken. Responsibilities and procedures should be in place to handle events and weaknesses when they are reported.

7.3.1.2 Technical Domains

- **Access control:** Access to information, information processing facilities, and business processes should be protected based on business and security requirements. An access control policy should be developed, implemented and reviewed based on an organisation's changing business and security needs.

- **Information systems acquisition, development and maintenance:** Security should be integrated into the acquisition, development, implementation and maintenance of information systems. This domain deals with cryptographic controls, system file security, application system software security during development and support, and technical vulnerability management.

- **Communications and operations management:** Information processing facilities should operate in a correct and secure manner. This domain includes change, capacity, network security, and third party service delivery management, backup strategies, e-commerce, information handling, and protection against malicious and mobile code.

7.3.1.3 Physical Domains

- **Physical and environmental security:** This domain includes controls that deal with protection of the organisation's premises and information from unauthorised physical access and damage.

Although argued to have drawbacks, ISO/IEC 27002 is an agreed upon mechanism that describes security processes and is used as a benchmark to identify 'correct infrastructure' (Harris, 2007: 71). The benefits of using the ISO/IEC 27002 framework with other

regulations is that, the regulations fill in the necessary details that the framework lacks while ISO/IEC 27002 provides the structure required to address multiple sets of requirements consistently. These two concepts in turn provide effectiveness, efficiency and auditability (Mackey, 2008). When implemented, ISO/IEC 27002 is meant to meet the requirements identified by the risk assessment process.

The ISO series standards may be worth the cost to many organisations as they are not only widely recognised but can fill any gap that may be discovered in the management of information security (Whitman and Mattord, 2009: 519). In 2001 and 2003, the South African National Technical Committee adopted the ISO 17799 and BS 17799-2, respectively, as information security management standards for South Africa (Upfold, 2005: 72; CBR, 2003).

7.3.2 ISO/IEC 27001:2005: Information Technology -- Security Techniques -- Information Security Management Systems -- Requirements

According to ISO (2009), ISO/IEC 27001 (ISO 27001) is a standard that covers all types of organisations and provides specifications for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System (ISMS). This is done within the context of an organisation's overall business risks. The standard also specifies requirements that can be used to customise and implement information security controls according to the needs of an organisation or parts of an organisation (ISO, 2009). ISO/IEC 27001 is the only auditable international standard that defines the requirements for an ISMS (BSI, 2010). This standard was originally called BS7799-2 but was adopted by ISO as ISO 27001 in 2005 (Praxiom, 2009).

This standard adopts the *process approach* which is used in the design and deployment of an ISMS. This approach also known as the "*Plan-Do-Check-Act*" (PDCA) model can be used by managers to control their ISMS processes, the interaction between these processes, and the inputs and outputs that keep these processes together (Calder and Watkins, 2006: 35; Praxiom, 2009; Calder, 2006: 37; ISO/IEC 27001, 2005). The PDCA model which was created in the 1950s by Deming says managers should treat business processes as a continuous loop so that they can identify and change those parts of the processes that need improvement (Tarantino, 2008: 176; Calder, 2008: 31). Figure 7.3 illustrates the ISO 27001

PDCA model. SANS 17799-2 (2003) and Vasudevan (2008: 19-20) outline the stages of the PDCA model:

- **Plan:** Establish security policy, objectives, targets, processes and procedures that are relevant to the management of risk and improvement of information security in order to deliver results in accordance with an organisation's policies and objectives.
- **Do:** Implement and operate the security policy, controls, processes and procedures.
- **Check:** monitor and review the ISMS, measure performance against policies, objectives and practical experience, and report the results to management for review.
- **Act:** take corrective and preventive measures to achieve continual improvement of the ISMS based on the results of the management review.

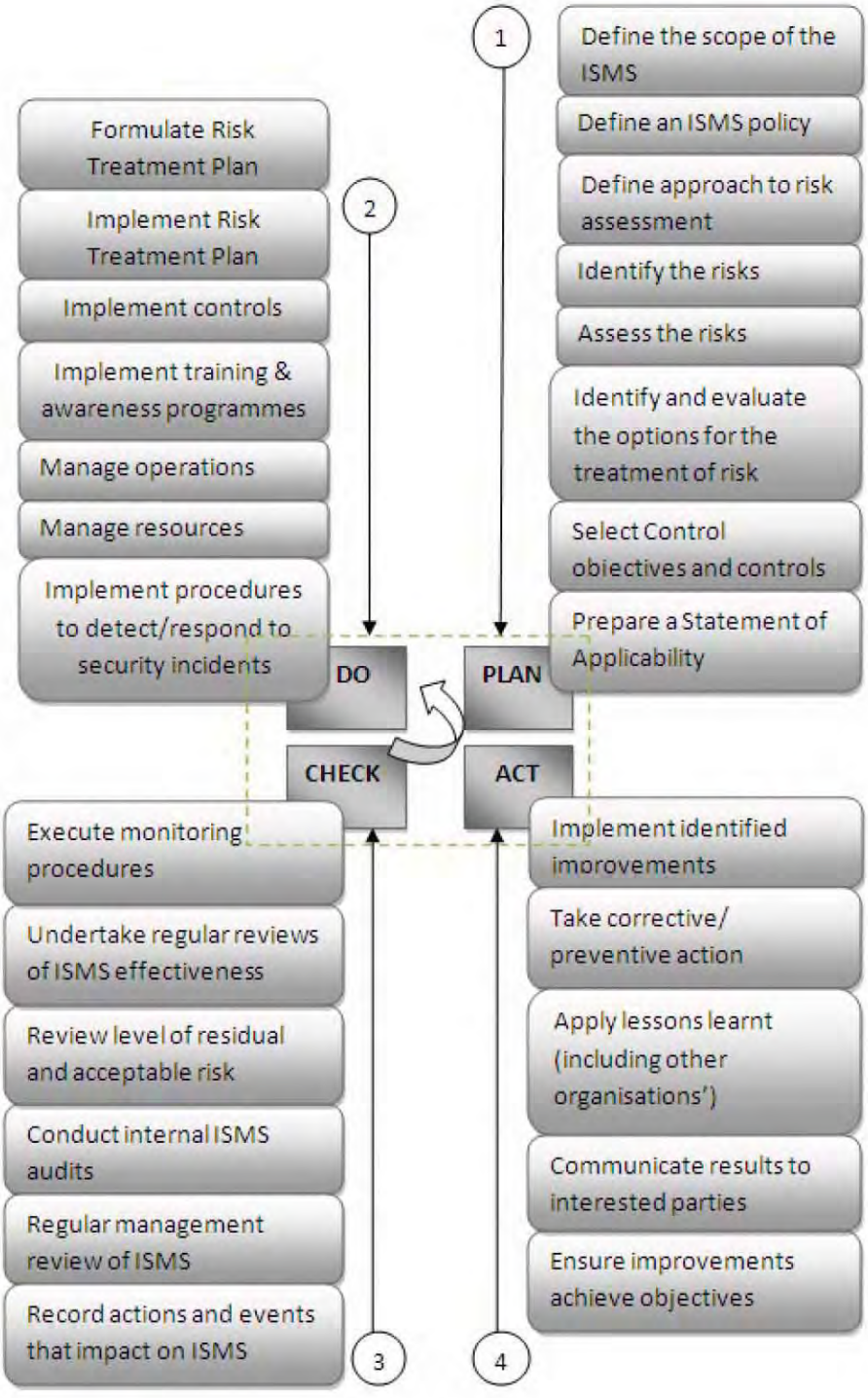

Figure 7.3: ISO 17799-2/ISO 27001 PDCA Model (Whitman and Mattord, 2009: 189)

7.3.3 NIST Security Models

National Institute of Standards and Technology (NIST) information security models are free and easily accessible models developed by the NIST Computer Security Resources Centre (CSRC). NIST models are widely used by government and industry professionals (Whitman and Mattord, 2009: 192). According to ISUCB (2009), NIST SP800-12, NIST SP800-26, NIST SP800-18 and NIST SP800-30 together, make up the NIST model. NIST SP800-26 has, however, been replaced by NIST SP800-53 (NIST, 2009).

7.3.3.1 NIST Special Publication 800-12 (NIST SP800-12): An introduction to Computer Security

This handbook explains the important concepts, considerations and interrelationships of security controls required to secure computer-based resources (NIST, 1995). NIST SP800-12 also serves as a guide to understanding an information security and is based on eight (8) elements which are also used by NIST SP800-14 as its principles (Whitman and Mattord, 2009: 192).

7.3.3.2 NIST Special Publication 800-14 (NIST SP800-14): Generally Accepted Security Principles and Practices for Securing Information Technology Systems

This publication provides best practices and security principles that can be used to direct the security team in the development of a blueprint. It also provides eight (8) principles and fourteen (14) practices that the security team can use to integrate into the information security process (Whitman and Mattord, 2009: 192; NIST, 1996).

7.3.3.3 NIST Special Publication 800-18 (NIST SP800-18) Rev. 1: Guide for Developing Security Plans for Federal Information Systems

NIST SP800-18 introduces a set of activities and security concepts that can be used to develop a security plan (NIST, 2006). According to Whitman and Mattord (2009: 197), this guide can be used as a foundation for a security blueprint and framework as it provides detailed methods for assessing, designing, and implementing controls and plans for various applications. It also includes templates that can be used for major security application plans.

7.3.3.4 NIST Special Publication 800-53 (NIST SP800-53) Rev. 3: Recommended Security Controls for Federal Information Systems

This guide superseded the NIST SP800-26 which was a security self-assessment guide for IT systems. NIST SP800-53 which has since been revised three (3) times is meant to provide guidelines for the selection and specification of information security controls supporting executive agencies of the federal government as well as other public and private institutions. These controls also complement other security standards (NIST, 2009).

7.3.3.5 NIST Special Publication 800-30: Risk Management for Information Technology Systems

This guide provides a foundation for the development of an effective risk management program. It contains guidelines and definitions necessary to assess and mitigate risks identified in IT systems (NIST, 2002; Whitman and Mattord, 2004: 228).

7.3.4 RFC 2196 Site Security Handbook

RFC 2196 was created by the Security Area Working Group of the Internet Engineering Task Force (IETF). It provides a good functional discussion of information security issues and an overview of five basic areas of security coupled with development and implementation details. It includes chapters on security policies, technical architecture, services and procedures, and incident handling (Whitman and Mattord, 2009: 198). It also includes a chapter on ongoing activities which involve actions that can be taken to address information security changes within an environment (Fraser, 1997).

7.3.5 COBIT

Control Objectives for Information and Related Technology (COBIT) is a framework published by the IT Governance Institute (ITGI) to provide an overall structure for IT control. This framework contains 34 high level objectives, each of which represent an IT process such as defining a strategic IT plan, defining the information architecture, managing configuration, managing facilities, and ensuring systems security. COBIT examines the efficiency, effectiveness, confidentiality, integrity, availability, compliance, and reliability aspects of high control objectives (Fitzgerald, 2008: 382). The COBIT framework is built on the following principle as illustrated below in figure 7.4:

"*To provide the information that the enterprise requires to achieve its objectives, the enterprise needs to invest in, and manage and control IT resources using a structured set of processes to provide the services that deliver the required enterprise information.*" (ITGI, 2007)

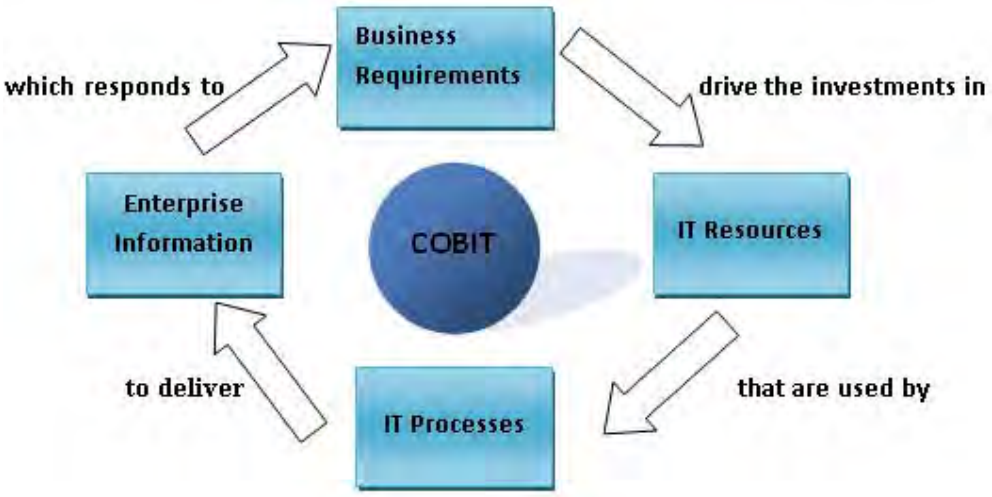

Figure 7.4: Basic COBIT Principle (Adapted from ITGI, 2007)

The COBIT model defines four (4) domains for governance which can be mapped to IT's traditional responsibility areas of plan, build, run and monitor (ITGI, 2007; Fitzgerald, 2008: 382). These domains as illustrated in figure 7.5 are plan and organise, acquire and implement, deliver and support, and monitor and evaluate. Processes and IT activities, and tasks are defined within these domains (Fitzgerald, 2008: 382).

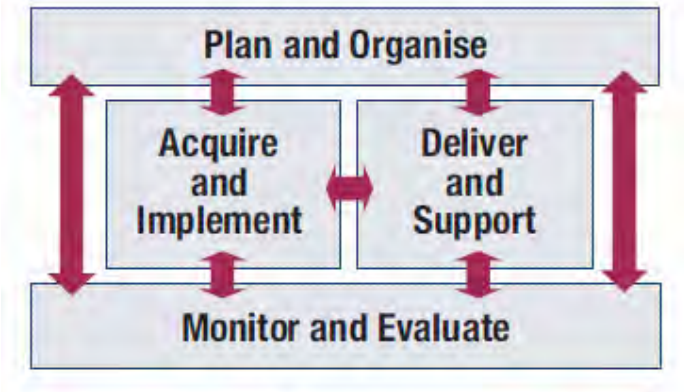

Figure 7.5: The Four Interrelated Domains of COBIT (ITGI, 2007)

Committee of Sponsoring Organisations (COSO) deals with corporate governance while COBIT which was derived from COSO, deals with IT governance (Harris, 2007:70). Where COBIT and (COSO) provide the "what is to be achieved", ITIL and ISO 27002 provide the "how to achieve it" aspects (Harris, 2007: 72). COBIT was developed for management users, and information system audit, control and security practitioners. It allows for standardised assurance initiative planning and scoping in a repeatable way that enables assessment under a single framework.

7.3.6 IT Infrastructure Library (ITIL)

The IT Infrastructure Library (ITIL) is a framework with a set of 44 books published by the British Government's Stationery Office between 1989 and 1992 and was meant to improve IT service management (Fitzgerald, 2008: 381). It was created because of organisations' increasing dependence on information technology to meet business needs (Harris, 2007: 72). ITIL offers a comprehensive framework within which organisations, or their agents can derive a structure which can be used to design and implement their own procedures (Clinch, 2009). ITIL contains a set of IT best practices for core IT operations such as change, release and configuration management, incident and problem management, capability and availability management, continuity and service level management, and IT financial management (Fitzgerald, 2008: 381-382; HKSAR, 2008). This framework can be adapted and applied to suit organisational size, culture, existing management systems, organisational structure and the nature of the business (Clinch, 2009).

7.3.7 Standard of Good Practice for Information Security (SOGP)

This standard addresses information security from a business perspective and provides a practical basis for assessing an organisation's information security requirements and how information security supports an organisation's key processes (ISF, 2007). The standard of Good Practice (SOGP) covers six (6) different aspects, each of which has principles that provide an overview of what needs to be done to meet the standard and objectives outlining the reasons why these actions are necessary. This standard comprises a total of 166 sections each providing a high-level principle and an objective (ISF, 2007). These aspects include security management, critical business applications, computer installations, networks, systems development, and end user environment.

7.4 Selecting Best Practices

The selection of information security best practices varies from organisation to organisation. Two categories of benchmarks are used in information security. Standard of due care is the level of standard of information security implemented in an organisation in order to meet legal requirements while due diligence requires that an organisation maintains the required level of protection using the implemented standards (Whitman and Mattord, 2009: 156).

An organisation wanting to implement security controls which are in compliance with a standard or set of standards requires support from top management and other employees in the development and implementation process. These standardised policies and guidelines must be applicable to the organisation's culture, business and operational practices (HKSAR, 2008).

Although no criteria has been published for the achievement of a *gold standard*, best practices on achieving this standard are publicly available. Organisations can also strive to achieve the gold standard which is a model level of performance that demonstrates industrial leadership, quality and concern for information protection. Implementation of this standard, however, requires a great deal of financial and personnel resources (Whitman and Mattord, 2009: 157).

Whitman and Mattord (2004: 229) suggest a *Hybrid Information Security Framework* which consists of controls derived from a number of sources and can be used as a checklist by any information security practitioner to ensure that their information security plan covers all areas which require controls, as illustrated in table 7.2. There are three categories of controls. These include:

- **Management controls**: cover security processes designed by strategic planners and executed by security administrators.
- **Operational controls**: deal with operational functionality of security in the organisation.
- **Technical controls**: address tactical and technical issues concerned with the design and implementation of security in the organisation.

Table 7.2: Hybrid Information Security Framework (Whitman and Mattord, 2004: 229)

Management Controls	Operational Controls	Technical Controls
Program Management	Contingency Planning	Logical Access Controls
System Security Plan	Security Education, Training and Awareness	Identification, Authentication, Authorisation, and Accountability
Life Cycle Maintenance	Personnel Security	Audit Trails
Risk Management	Physical Security	Asset Classification and Control
Review of Security Controls	Production Inputs and Outputs	Cryptography
Legal Compliance	Hardware and Software Systems Maintenance	
	Data Integrity	

ISO/IEC 27002 (2005) also suggests best practices that should be the centre of every information security program. These are outlined in section 8.2.

The Commonly Accepted Security Practices and Regulations (CASPR) also offer advice and recommendations on security processes and procedures through white papers and other security related documents (Piliouras, 2004: 34).

According to Clinch (2009), a best practice approach should be taken when implementing Information Security Management (ISM).

7.5 Information Security Standards for the Mining Industry

The mining industry like other manufacturing industries is one of the most data intensive industries as it deals with information about processes, product designs, shipping, inventory and customers (Paladion, 2008). Just as quality management standards such as ISO 9000 have become a requirement for doing business in industries such as the mines, internationally recognised information security standards will continue to be accepted and eventually become a necessity for many mines (Ernst&Young, 2008).

In a 2010 PricewaterhouseCoopers survey of the mining and energy industry, 88% of the respondents said they would be adopting a recognised information security framework in preparation for upcoming regulatory requirements. This would be done in order to tighten the

alignment of information security's contribution with the business (PricewaterhouseCoopers, 2009).

7.6 Conclusion

There is no single formula for information security. Hence, there is a need for benchmarks or standards to ensure that an adequate level of security is attained, resources are used efficiently, and best security practices are adopted. Successful implementation of information security standards or controls must take into consideration functional, security, and user requirements (HKSAR, 2008). Adoption of information security best practices in an organisation enhances confidence in legal and regulatory compliance, inter-organisational trading and increased stakeholder confidence in the organisation's operations. As mining organisations are driven by a high level of standards, adoption of information security best practices will not only enhance regulatory compliance but increase competitive advantage.

Chapter 8

Information Security in the Mining Industry vs. ISO/IEC 27002

Chapter 7 explored various widely used international information security models and frameworks. This chapter reviews information security issues as highlighted in the literature review. These issues will then be mapped to ISO 27002 information security controls and domains that are deemed suitable to address these issues.

8.1 Introduction

ISO/IEC 27002 is the most widely adopted information security framework by organisations around the world, irrespective of industry (Layton, 2006: 6; Sipior and Ward, 2008: 53; Whitman and Mattord, 2009: 187). Although argued to be cumbersome and difficult to implement, this standard is highly recommended to organisations wishing to develop a comprehensive and sound information security infrastructure (Upfold, 2005: 87). This chapter lists all the information security concerns being faced by the mining industry as outlined in the literature review. These concerns are first mapped to legislative and common best practice controls found in ISO/IEC 27002 and later to the ISO/IEC 27002 information security domains which are information security best practices. The purpose of this exercise is to:

- List the security concerns identified in the literature review.
- Place the security concerns within the relevant ISO/IEC 27002 security domains.
- Identify to what extent the ISO/IEC 27002 security domains cater for all or part of the security concerns.

8.2 Legislative vs. Common Best Practice Controls

ISO/IEC 27002 has identified controls that can be used as a "*starting point"* for information security or as guiding principles for information security management. These guiding principles are applicable to most organisations and are either based on legislative requirements or considered to be common best practices for information security (ISO 27002, 2005: x-xi). Three (3) legislative controls and seven (7) common best practice controls make up the guiding principles in the ISO/IEC 27002 standard.

Controls considered to be essential to an organisation due to legislative requirements include:

- Data protection and privacy of personal information.
- Safeguarding of organisational records.
- Intellectual Property Rights (IPR).

Controls considered to be essential for common best practices include:

- Information security policy document.
- Allocation of information security responsibilities.
- Information security awareness, training, and education.
- Correct processing in applications.
- Vulnerability management.
- Business continuity management.
- Management of information security incidents and improvements.

Throughout this literature review, a total of 28 security concerns believed to be applicable to the Zambian copper mining industry were discussed. These concerns are listed down the left-hand side of table 8.1. Across the top are ISO/IEC 27002 controls. A tick (✓) is an indication of which control is required to address each information security concern listed on the left-hand side.

Table 8.1: Legislative and Common Best Practice issues being faced by the Mining Industry (Adapted from Upfold, 2005: 88)

	Legislative Controls			Common Best Practice Controls						
Mining industry information security concerns (as explored in the literature survey)	**Data Protection and Privacy of Personal Information**	**Safeguarding of Organisational Records**	**Intellectual Property Rights**	**Information Security Policy Document**	**Allocation of Information Security Responsibilities**	**Information Security Education and Training**	**Correct Processing in Applications**	**Vulnerability Management**	**Business Continuity Management**	**Management of Information Security Incidents and Improvements**
Lack of/inadequate security policies (Bradley, 2008; Welander, 2007)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Lack of/inadequate security procedures (Bajpai and Gupta, 2005; Welander, 2007)	✓	✓	✓		✓	✓	✓	✓	✓	✓
Poor staff awareness (Bajpai and Gupta, 2005; DTT, 2008)	✓		✓			✓	✓	✓	✓	✓
Inadequate risk management process (Pironti, 2008)							✓	✓	✓	✓
Increased regulation (PricewaterhouseCoopers, 2009; WIPO, 2009)	✓	✓	✓			✓			✓	✓
Dispersed data and information (Copans, 2007; PricewaterhouseCoopers, 2008)	✓	✓			✓			✓	✓	✓
Email threats such as viruses and spam (DTT, 2008)						✓		✓	✓	✓
Inadequate control system policies and procedures (Lowe, *et al.*, 2007; Welander, 2007)		✓			✓		✓	✓	✓	✓

Mining industry information security concerns (as explored in the literature survey)	**Data Protection and Privacy of Personal Information**	**Safeguarding of Organisational Records**	**Intellectual Property Rights**	**Information Security Policy Document**	**Allocation of Information Security Responsibilities**	**Information Security Education and Training**	**Correct Processing in Applications**	**Vulnerability Management**	**Business Continuity Management**	**Management of Information Security Incidents and Improvements**
Cultural clashes between IT staff (Bartels, 2005)						✓		✓	✓	✓
Poor asset identification and inventory (PricewaterhouseCoopers, 2008)	✓	✓	✓		✓			✓	✓	✓
Irregular or no patching of systems (Bartels, 2005)		✓			✓			✓	✓	✓
Inadequate access control procedures (Bajpai and Gupta, 2005)	✓	✓			✓		✓	✓	✓	✓
Inadequate email policies (Bradley, 2008; eMedia, 2008)		✓								✓
Informal change management procedures (Bartel, 2005)		✓			✓		✓	✓	✓	✓
Informal BCPs (DTT, 2008)		✓			✓			✓	✓	✓
Lack of or irregular testing of contingency plans (DTT, 2008; ICMM, 2009)		✓			✓			✓	✓	✓
Ill-defined crisis communication procedures (ICMM, 2009)					✓				✓	✓

Mining industry information security concerns (as explored in the literature survey)	**Data Protection and Privacy of Personal Information**	**Safeguarding of Organisational Records**	**Intellectual Property Rights**	**Information Security Policy Document**	**Allocation of Information Security Responsibilities**	**Information Security Education and Training**	**Correct Processing in Applications**	**Vulnerability Management**	**Business Continuity Management**	**Management of Information Security Incidents and Improvements**
Lack of formal information security governance frameworks (DTT, 2008)	✓	✓	✓		✓	✓		✓	✓	
Lack of formal mobile security governance (Zhang, 2009)	✓	✓			✓					✓
Inadequate integration of information security into employment policies and practices (DTT, 2008)		✓				✓				✓
Poor incident response management (Helberger, 2009)					✓	✓		✓	✓	✓
Unsecure application software (Tomlinson, 2007: 12; Dobelis, 2007: 46)		✓	✓		✓	✓	✓	✓	✓	✓
Ill-defined user access privileges (van Holsbeck and Johnson, 2004; Kairab, 2004: 7)	✓	✓	✓		✓		✓			✓
IT-based BCPs (Warner, 2007)					✓				✓	
Ill-maintained legacy systems (Zoufaly, 2009; Welander, 2009; ACS, 2009)		✓			✓	✓		✓	✓	✓

Mining industry information security concerns (as explored in the literature survey)	**Data Protection and Privacy of Personal Information**	**Safeguarding of Organisational Records**	**Intellectual Property Rights**	**Information Security Policy Document**	**Allocation of Information Security Responsibilities**	**Information Security Education and Training**	**Correct Processing in Applications**	**Vulnerability Management**	**Business Continuity Management**	**Management of Information Security Incidents and Improvements**
Human error such as social engineering (Tomlinson, 2007: 12; DTT, 2008; Piccoli, 2008: 431)	✓				✓	✓	✓	✓	✓	✓
Incorrect dissemination of information (MMSD, 2002)	✓	✓			✓	✓				✓
Environmental threats to hardware (Falco *et al.*, 2002)		✓				✓		✓	✓	✓

The information security policy document column in table 8.1 is shaded because it is common to all information security concerns and it serves as the starting point for any information security program.

Based on Table 8.1, of the twenty-eight (28) information security concerns believed to be applicable to the mining industry, **26%** are legislative and **74%** are common best practice concerns as shown in figure 8.1.

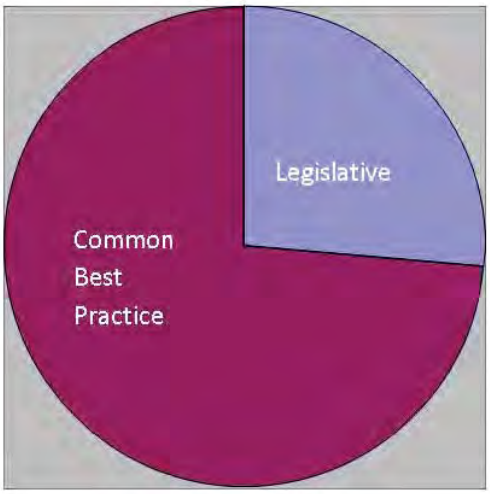

Figure 8.1: Legislative vs. Common Best Practice

Of the security issues considered to be legislative, **29%** are deemed to require controls that address data protection and privacy of personal information, **51%** are deemed to require controls that address safeguarding of organisational records, while **20%** are considered to require controls that address Intellectual Property Rights (IPR). This is illustrated in figure 8.2.

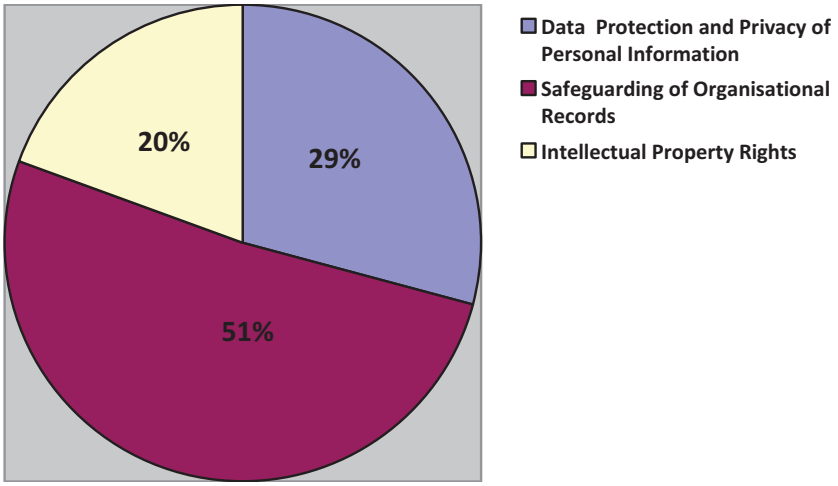

Figure 8.2: Categories of most pressing legislative controls in the mining industry

Figure 8.3 indicates the percentage of controls required to address common best practice issues.

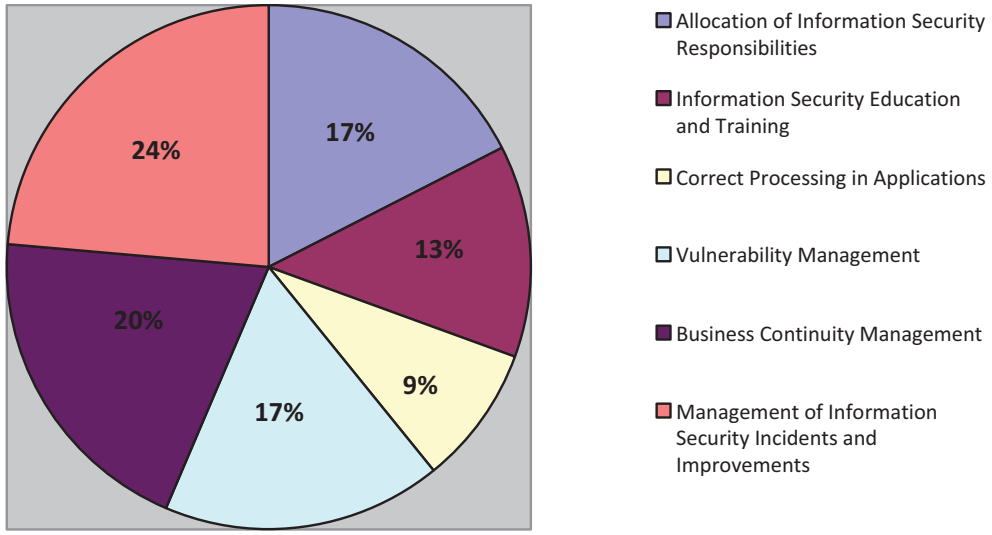

Figure 8.3: Composition of Common Best Practice Controls required to address information security issues in the mining industry

8.3 Mining Industry Security Concerns vs. ISO/IEC 27002 Security Domains

Table 8.2 outlines the mapping of security concerns that were identified to be affecting the mining industry against the eleven (11) ISO 27002 security domains. Unlike table 8.1 which maps security issues against information security guiding principles, table 8.2 maps these concerns against information security best practices. A tick (✓) indicates which information security domain(s) in the top row is required to address each information security concern listed on the left-hand side of the table.

Table 8.2: Mining Industry security issues vs. ISO 27002 Security Domains (Adapted from Upfold, 2005: 92)

	ISO/IEC 27002 Information Security Domains										
Mining industry information security concerns (as explored in the literature survey)	**Section 1** Security Policy	**Section 2** Organising Information Security	**Section 3** Asset Management	**Section 4** Human Resources Security	**Section 5** Physical and Environmental Security	**Section 6** Communications and Operations Management	**Section 7** Access Control	**Section 8** Information Systems Acquisition Development and Maintenance	**Section 9** Information Security Incident Management	**Section 10** Business Continuity Management	**Section 11** Compliance
Lack of/inadequate security policies											
Lack of/inadequate security procedures											
Poor staff awareness											
Inadequate risk management process											
Increased regulation		✓	✓	✓	✓	✓	✓		✓		✓
Dispersed data and information		✓	✓			✓	✓	✓	✓	✓	✓
Email threats such as viruses and spam		✓				✓			✓		
Inadequate control system policies and procedures		✓	✓		✓	✓	✓	✓	✓	✓	✓
Cultural clashes between IT staff		✓		✓		✓		✓			
Poor asset identification and inventory		✓	✓			✓		✓	✓	✓	✓

	Section 1 Security Policy	**Section 2** Organising Information Security	**Section 3** Asset Management	**Section 4** Human Resources Security	**Section 5** Physical and Environmental Security	**Section 6** Communications and Operations Management	**Section 7** Access Control	**Section 8** Information Systems Acquisition Development and	**Section 9** Information Security Incident Management	**Section 10** Business Continuity Management	**Section 11** Compliance
Irregular or no patching of systems		✓				✓		✓	✓	✓	
Inadequate access control procedures		✓		✓	✓	✓	✓	✓	✓	✓	✓
Inadequate email policies		✓	✓			✓			✓		
Informal change management procedures		✓				✓		✓	✓	✓	
Informal BCPs		✓				✓			✓	✓	
Lack of or irregular testing of contingency plans		✓				✓		✓	✓	✓	✓
Ill-defined crisis communication procedures										✓	
Lack of formal information security governance frameworks		✓		✓		✓			✓	✓	✓
Lack of formal mobile security governance		✓	✓			✓	✓		✓	✓	✓
Inadequate integration of information security into employment policies and practices		✓		✓							✓

	Section 1 Security Policy	**Section 2** Organising Information	**Section 3** Asset Management	**Section 4** Human Resources Security	**Section 5** Physical and Environmental Security	**Section 6** Communications and Operations Management	**Section 7** Access Control	**Section 8** Information Systems Acquisition Development and	**Section 9** Information Security Incident Management	**Section 10** Business Continuity Management	**Section 11** Compliance
Poor incident response plans		✓			✓				✓	✓	
Unsecure application software		✓				✓	✓	✓		✓	✓
Ill-defined user access privileges		✓		✓		✓	✓	✓	✓		✓
IT-based Business Continuity Plans		✓				✓				✓	
Ill-maintained legacy systems		✓	✓		✓	✓	✓	✓	✓	✓	✓
Human error such as social engineering		✓			✓	✓	✓	✓	✓	✓	✓
Incorrect dissemination or disclosure of information		✓	✓	✓		✓		✓	✓		✓
Environmental threats to hardware		✓	✓		✓				✓	✓	

The following information security concerns have been shaded, as all 11 information security domains apply to them:

- Lack of or inadequate security policies.
- Lack of or inadequate security procedures.
- Poor staff awareness.
- Inadequate risk management process.

The frequency histogram in figure 8.4 illustrates the number of security concerns that are addressed by each domain in ISO/IEC 27002.

Note: The information security policy domain is not part of the histogram as it is considered to be essential for addressing all information security concerns.

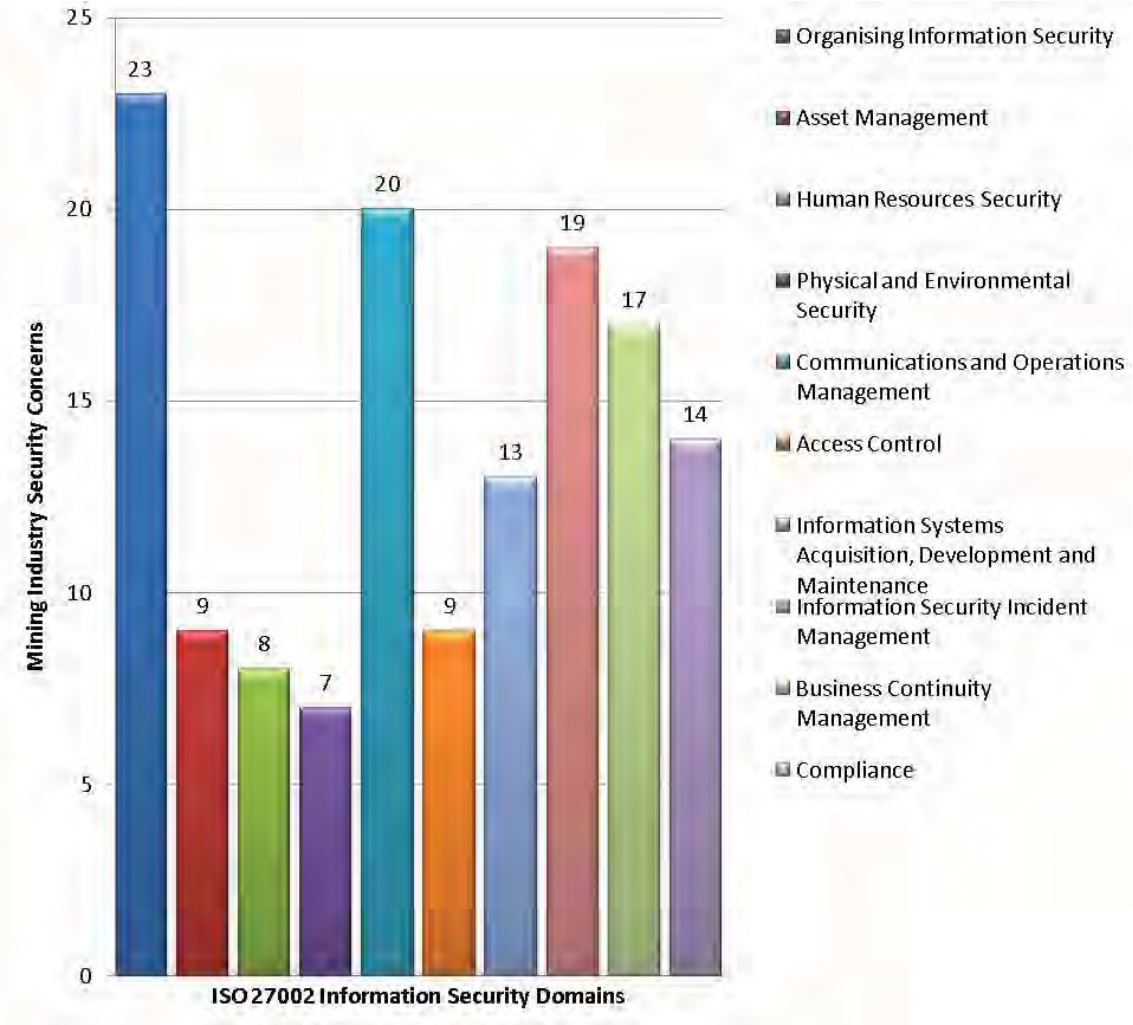

Figure 8.4: Number of mining industry security concerns in each control domain

Figure 8.4 indicates that, of the 28 information security concerns exposed through the literature review, organising information security, communications and operations management, and information security incident management would appear to be the domains that address the majority of security concerns. Conversely, the physical and environmental security domain seems to embrace the least concerns within the mining industry.

8.4 Conclusion

An extensive review of literature revealed twenty-eight (28) information security concerns thought to be applicable to the mining industry. Although detailed, ISO/IEC 27002 suggests core security controls that may be considered universally acceptable. The 28 information security concerns were then mapped against the three (3) universally acceptable ISO/IEC 27002 legislative controls and the seven (7) universally acceptable common best practice controls. 26% were identified as legislative issues while 74% were common best practice issues. Of the legislative issues identified, safeguarding of organisational records is believed to require the most attention. In the same way, of the common best practice issues identified, management of information security incidents and improvements is believed to require the most attention.

The physical and environmental security domain was the least significant as the mining industry is believed to have high physical and environmental controls in place due to legislative requirements. This is coupled with the need for SHEQ certifications. From the security concerns that were identified, poor staff awareness is deemed to be of critical concern as employees are the users of the information systems and play a critical role in 'making' or 'breaking' those systems. Inadequate risk management equally affects all the information security domains and the mining industry needs to be aware of the level of information security risks it is facing and find ways of handling them. Organising information security, communications and operations management followed by information security incident management were the domains which were deemed to have the most security concerns that needed to be addressed in the mining industry.

Chapter 9

Research Design

Chapter 8 outlined how the security concerns identified in the literature review were mapped to the ISO 27002 controls and information security domains. This chapter discusses the design of the research and data collection and analysis processes.

9.1 Introduction

This research in the form of a case study seeks to determine information security practices in copper mining organisations in Zambia based on the ISO/IEC 27002 information security standard. As ISO/IEC 27002 is a universally accepted standard, it provides an appropriate basis for standardised information security practices. Justification of the research method that was used to achieve the research goal as well as the steps that were taken to collect and analyse the research data are outlined.

9.2 Research Methodology

This research is in the form of an *instrumental case study* and includes such data collection methods as surveys in the form of questionnaires, interviews and document reviews. According to Stake (1995: 3), an instrumental case study is used when there is a need for a general understanding and there is a possibility of getting insight into the question by studying a particular case. The case study method was chosen as it is an intensive study that sheds light on a larger class of classes and uses different methods to collect various kinds of information and make observations (Gerring, 2007:20; Hamel *et al.,* 1993: 45). It is through these methods that the object of study is understood (Hamel *et al.*, 1993: 45). Case study methods also answer the "how" and "why" of research questions and also focus on contemporary events (Yin, 2003: 5).

Descriptive statistics were used for quantitative analysis of the data. Fisher and Marshall (2009) define descriptive statistics as "the numerical procedures or graphical techniques used to organise and describe the characteristics or factors of a given sample".

9.3 Design of the Questionnaires

Two sets of questionnaires were used in the study. The first set of questionnaires was divided into two parts and was meant to explore leadership perceptions surrounding information security practices in Zambian copper mines. Questionnaire set A was directed at senior executives while questionnaire set B was directed at heads of Information Technology. In this study, these questionnaires will be referred to as "*Leadership Perception Questionnaires*". The questions that made up these questionnaires were derived from information security concerns that were identified in the literature review as affecting information security

practices in Zambian copper mines. Although all concerns affected both senior executives and IT HoDs, the questions in the two questionnaires were different as some directly affected the corporate level of management which includes senior executives while others directly affected the business level of management which includes IT HoDs. All concerns, however, were strategy oriented in the context of information security. Hence both sets of respondents were considered to be part of senior management.

The second set of questionnaires that were in the form of an ISO/IEC 27002 audit tool were procured from Praxiom Research Group Limited. This audit tool consists of eleven (11) questionnaires that cover all eleven (11) information security domains of ISO/IEC 27002. The questions are comprehensive enough to cover all aspects of the 11 domains.

The questionnaires were designed in such a way that they were:

- Valid, so that they measure what the research intends to measure.
- Reliable, in that they can yield consistent results from repeated samples and different researchers over a period of time.
- Easy enough for respondents to give the necessary information, accurately and completely.
- Unbiased and not suggestive so that the respondent could provide responses without added pressure from the style of questioning in the questionnaire.

9.3.1 Format and Presentation

In the first set of questionnaires that were administered at five (5) Zambian copper mining organisations, respondents were given choices based on a five-point Likert scale ranging from “strongly agree”, “agree”, “neutral”, “disagree”, to “strongly disagree” with a few questions being presented in the “yes”, “no”, and “partial” format. A provision was also made for respondents to make comments after answering each question.

The eleven (11) ISO/IEC 27002 questionnaires that make up the audit tool used for in-depth analysis of information security practices in one Zambian copper mine which will be referred to as “Mine A”, were presented in the same format. Respondents had a choice of selecting “yes”, “no”, “N/A” (Not Applicable) and making notes or comments where necessary, in all

sub-sections of the questionnaires. N/A has been included as the audit tool covers all industries and some practices may not currently be applicable to what has been implemented in the copper mining industry. The provision for notes and comments (N/C) was also used when the response did not fall under the other 3 options.

Both sets of questionnaires were presented in a standardised format to reduce time and effort required from the respondents.

9.4 Data Collection Procedure

According to Stake (1995: 60-68), Hamel *et al.* (1993: 1), and Yin (2003: 83), data sources used in case study research include direct observation, participant observation, interviews, document reviews, archival records, and physical artifacts. The researcher adopted three principles recommended by Yin (2003: 97) which can be used to maximise the benefits derived from the use of these data sources:

i. Use of multiple sources of evidence: more than one source of data was used. This included questionnaires, interviews and document reviews.

ii. Creation of a case study database: the questionnaire data is in both hard and soft copy and interview questions and answers have been typed out in case future reference is required.

iii. Maintaining a chain of evidence: a reader of the research will be able to follow it from the initial research question to the achievement of the research goal and the conclusion of the research.

Data collection for this study was conducted using three (3) methods:

- The questionnaires were administered on site at the organisations in question. Leadership Perception Questionnaires were targeted at senior executives and heads of IT in the copper mining organisations, while the ISO/IEC 27002 Audit Tool Questionnaires were targeted at middle management and personnel who are involved in the implementation and maintenance of information security practices in Mine A.

- Interviews concerning specific issues applying to Mine A that were not explicitly covered in the questionnaires or required further details were conducted with senior and middle management.

- Existing documentation concerning policies, procedures, system and application guides, and manuals were also reviewed in Mine A.

9.5 Pilot Study

A pilot study was conducted on both sets of questionnaires. The pilot study for the Leadership Perception Questionnaires was conducted on an information security consultant who has experience in information security practices in the Zambian copper mining industry. According to Welman *et al.* (2005: 148), a self-developed instrument can be checked for validity by an experienced researcher or expert in the field. The ISO/IEC 27002 Audit Tool survey instrument being used for this research is well known and has been thoroughly tested. An extensive pilot study was, therefore, not required. Hence, a reduced pilot study was conducted on one of the 11 questionnaires that form part of the survey instrument. This was done within the organisation where the instrument was being administered. According to Welman *et al.* (2005: 148), a pilot study is carried out in order to:

- Detect possible flaws in the measurement procedures and processes.

- Identify unclear or ambiguously formulated items.

- Notice non-verbal behavior in participants that may signify discomfort or embarrassment caused by the content or wording of the questions.

9.6 Population and Sample

The Leadership Perception Questionnaires were administered at five (5) Zambian copper mining organisations. These questionnaires were completed by senior executives and heads of Information Technology departments at these organisations. Only four organisations, however, responded to the questionnaires. The ISO/IEC 27002 Audit Tool was administered to 15 respondents who are personnel in charge of infrastructure at one of the four copper mining organisations in question. These respondents included representation from human resource, administration, and personnel in charge of the various sections of the Information Technology department. These questionnaires were not administered to users of the

information systems as the researcher was concerned with exploring senior management perception surrounding information security practices in these organisations along with the actual establishment, implementation and maintenance of these practices. Related feedback from users for whom these practices are enforced was, therefore, not required.

9.7 Data Analysis Procedure

This study uses interpretive and positivist paradigms as both qualitative and quantitative analysis methods were employed in the study. Data analysis was used to determine:

- The information security domains that are considered to be the most important in Zambian mining organisations.
- The information security domains that are considered to be the least important in Zambian copper mining organisations.
- The current state of practice of information security in Zambian copper mining organisations.
- The comparability between current information security practices in the Zambian copper mining industry and the ISO/IEC 27002 standard.
- The applicability of ISO/IEC 27002 to Zambian copper mining organisations.

The results of the quantitative data analysis have been presented as follows:

- Tables, such as frequency distributions.
- Graphs, such as histograms and pie charts.
- Results summaries consisting of percentages and counts.

9.8 Response Rates, Ethics and Confidentiality

The confidentiality of the respondents has been protected. The identity of the organisations or the respondents involved will not be revealed in this study. All questionnaires were completed by the appropriate respondents and approved by the organisations.

9.9 Reliability, Quality, and Validity of the Data Collection

Data triangulation was used for validation of the data as different data sources were used. According to Yin (2003: 98), the advantage of using multiple sources of evidence which is the process of triangulation is the development of "*converging lines of inquiry*".

Four tests that are used to establish the quality of an empirical social research design were carried out. These tests included construct validity, internal validity, external validity, and reliability. They confirm the concepts of trustworthiness, credibility, confirmability, and data dependability (Yin, 2003: 33). More emphasis was placed on external validity as it deals with the problem of knowing whether the findings of a study are generalisable beyond the immediate case study. These tests are described in more detail in table 9.1 below:

Table 9.1: Case Study Tactics from Four Design Tests (Adapted from Yin (2003: 34))

Test	Case Study Tactic	Phase of Research at which Tactic Occurs
Construct validity	- Use multiple sources of evidence - Establish a chain of evidence - Have key informants review draft case study report	Data collection Data collection Composition
Internal Validity	- Do pattern matching - Do explanation-building - Address rival explanations - Use logic models	Data analysis Data analysis Data analysis Data analysis
External Validity	- Use theory in single-case studies - Use replication logic in multiple-case studies	Research design Research design
Reliability	- Use case study protocol - Develop case study database	Data collection Data collection

Although critics argue that single cases are a poor basis for generalisation, case studies rely on *analytical generalisation* whose goal unlike that of statistical generalisation (whose goal is to enumerate frequencies) is to expand and generalise theories (Yin, 2003: 10, 37).

The ISO/IEC 27002 Audit Tool questionnaires that were used for the intensive case study are designed such that all aspects of the ISO/IEC 27002 standard pertaining to information security practices are covered. These questionnaires were obtained from a reputable organisation and they have been used as an audit tool by other organisations. The Leadership Perception Questionnaires were also piloted and administered to the appropriate respondents.

9.10 Limitations

Although a study on leadership perceptions of information security practices was carried out in various organisations, the researcher could only carry out an intensive case study on one organisation due to time limitations. The organisation that was studied will be representative of the other organisations as they have similar information security foundations. The observation method could also not be used as it requires a lot of time to carry out and would have restricted the researcher's range of subjects or sample of behavior of interest in this case (Foster, 1996: 14). The format for the ISO/IEC 27002 audit tool questionnaires did not provide for responses that were not explicitly "yes", "no" or N/A. These responses had to be written down under the notes and comments section.

9.11 Conclusion

This chapter discussed the approach that was used to undertake this research. This includes the methodology, data collection, analysis and other considerations that were put into effect when the research was being undertaken. The case study method was deemed to be the most appropriate for gaining insight at one mine. Three methods were used to collect data. These included interviews, questionnaires, and document reviews. Both qualitative and quantitative analysis was carried out on the data so as to provide a correlation and justify the findings. The case study findings which include the analysis and interpretation of the research findings will be presented in Chapter 10.

Chapter 10

Results and Analysis

This chapter discusses the results that were obtained from the administration of two sets of questionnaires and an ISO 27002 survey instrument using the methods outlined in chapter 9. An analysis of the results is also provided in this chapter.

10.1 Introduction

This chapter outlines the results that were obtained from the administration of the ISO/IEC 27002 survey instrument in the form of an audit tool and two sets of questionnaires, interviews that were carried out, and the documentation that was obtained from a Zambian copper mining organisation. The questionnaires in the form of an audit tool were meant to establish current information security practices in the organisation that was audited. An additional set of questionnaires was meant to explore leadership perceptions regarding information security practices in these organisations. An analysis of the results that were obtained using the methods mentioned above is also provided. Recommendations following the analysis of these results will be discussed in chapter 11.

10.2 Leadership Perceptions of Information Security Practices

Two sets of questionnaires were administered at five copper mining organisations in Zambia. These questionnaires as mentioned in chapter 9 were meant to explore leadership perceptions of information security practices in these organisations. These questionnaires which will be referred to as "*Leadership Perception Questionnaires*" in this study were divided into two parts, namely, Questionnaire A and Questionnaire B. "A" questions below represent questions that were targeted at senior executives in the Zambian copper mining organisations, while "B" questions represent questions that were targeted at overall heads of the Information Technology Departments in these organisations. The results and analyses below are representative of four of the five organisations that responded to the questionnaires. The figures below are a graphical representation of the data outlined in the tables.

10.2.1 Lack of formal information security governance frameworks

Question 1A: An information security governance framework exists in the organisation

Table 10.1: Formal Information Security Governance Frameworks

Information Security Governance Pillars	Yes	No	Partial
Information Security Policies	3	0	1
Ethics (privacy, accuracy, property and accessibility)	3	1	0
Accountability and Responsibility for information security (by board of directors and senior executives)	3	0	1
Information Security Risk Management	3	1	0
Employee Education, Training, and Awareness	2	1	1
Information Sharing (with other organisations and regulatory bodies)	1	0	3
Information Security Resource Allocation	4	0	0
Best Practice Information Security Standards (e.g. ISO 27002, ITIL, COBIT)	2	0	2
Compliance with legal requirements	4	0	0

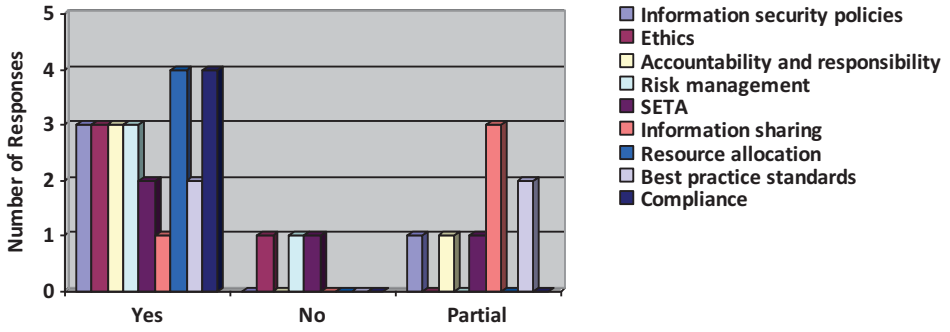

Figure 10.1: Existence of Formal Information Security Governance Frameworks

Figure 10.1 illustrates the extent to which information security governance frameworks have been established in the four (4) organisations in which the questionnaires were administered. As these frameworks consist of different components, varying responses were given by respondents as to what extent each component of the information security governance framework has been established and implemented. 3 respondents, (75%), claim that information security polices exist in their organisations while 1 respondent, (25%), believes that an information security policy only partially exists in their organisation. 3 respondents, (75%), believe that ethics are part of the Information Security Governance (ISG) framework in their organisation while 1 respondent, (25%), claims this is not the case. On whether

accountability and responsibility is part of their ISG framework, 3 respondents, (75%), agree that this is the case while 1 respondent, (25%), claims this has only been partially implemented in the organisation. Furthermore, 3 respondents, (75%), agree that risk management is part of their ISG framework in the organisation while 1 respondent, (25%), does not believe this is the case. 2 respondents, (50%), believe that information security education, training, and awareness are part of their ISG framework, 1 respondent, (25%), does not believe this is the case, while 1 respondent, (25%), claims this has only been partially implemented. 1 respondent, (25%), claims their organisation shares information with other organisations and regulatory bodies while 3 respondents, (75%), believe this information sharing is only partially done in their organisations. All 4 respondents, (100%), believe resource allocation and compliance are part of their organisations' ISG frameworks.

10.2.2 Lack of or inadequate information security policies

Question 2.1A: The organisation has an information security policy.

Table 10.2: Existence of an Information Security Policy

Yes	No	Partial
3	1	0

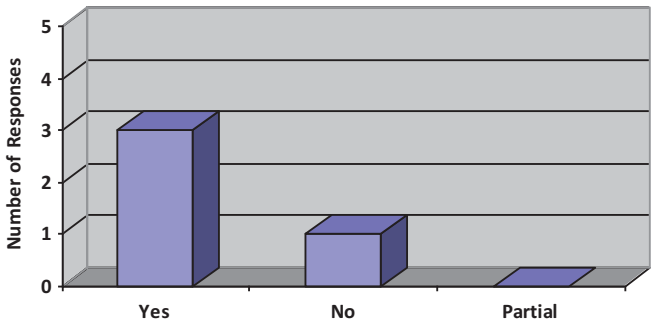

Figure 10.2: Existence of Information Security Policy

Question 2.2A: The organisation's information security policy adequately caters for organisational security requirements, business objectives and changing business requirements.

Table 10.3: Information security policy caters for security and business requirements

	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Policy caters for security requirements	2	1	0	0	0
Policy caters for business objectives	1	2	0	0	0
Policy caters for changing business needs	2	1	0	0	0

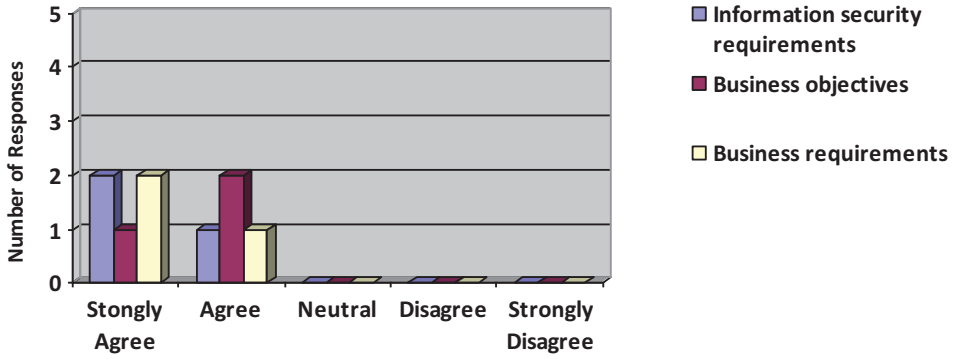

Figure 10.3: Information security policy caters for security and business requirements

Figure 10.2 indicates that 3 respondents, (75%), claim that they have an information security policy in place and 1 respondent, (25%) claims they do not have one. As indicated in figure 10.3, all 3 respondents, (100%), that have developed an information security policy in their organisations believe that it meets their information security requirements, business objectives, and business requirements.

10.2.3 Inadequate integration of information security into employment policies and practices

Question 3A: Information security is integrated into employment policies and practices.

Table 10.4: Information security integration into employment policies and practices

Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
2	2	0	0	0

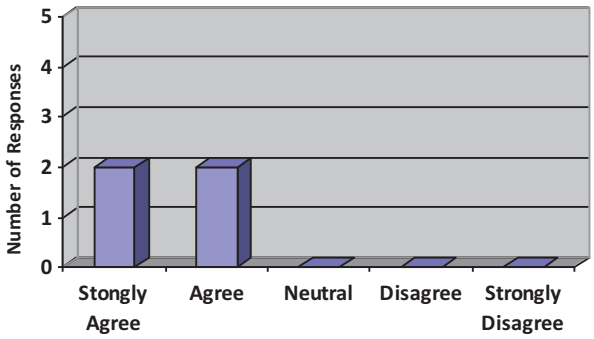

Figure 10.4: Information security integration into employment policies and practices

Figure 10.4 indicates that all 4 respondents, (100%), agree that their organisations have integrated information security into employment policies and practices. Of these respondents, 2 respondents, (50%), firmly believe they have adequately integrated information security into these policies and practices.

10.2.4 Increased regulation

Question 4A: The organisation adheres to all information security regulatory requirements.

Table 10.5: Adherence to information security regulatory requirements

Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
2	1	0	1	0

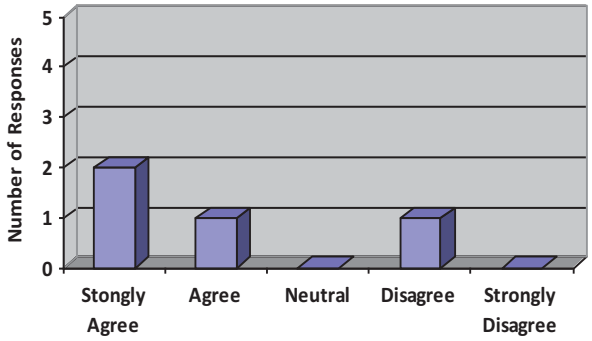

Figure 10.5: Adherence to information security regulatory requirements

Figure 10.5 indicates that 3 respondents, (75%), believe that their organisations adhere to all information security regulatory requirements while 1 respondent, (25%), believes that their organisation does not.

10.2.5 Incorrect dissemination or disclosure of information

Question 5A: Organisational information is disclosed and/or disseminated only to the appropriate stakeholders.

Table 10.6: Incorrect dissemination or disclosure of information

Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
2	2	0	0	0

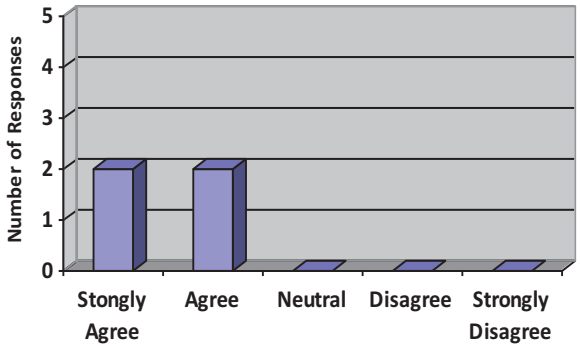

Figure 10.6: Incorrect dissemination or disclosure of information

Figure 10.6 indicates that all four respondents, (100%), disclose or disseminate organisational information to the appropriate stakeholders.

10.2.6 Informal Business Continuity Plans (BCPs)

Question 6A: We have established an enterprise-wide Business Continuity planning process in which our organisation's information security requirements are catered for.

Table 10.7: Enterprise-wide Business Continuity Plans have been established

Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
2	1	1	0	0

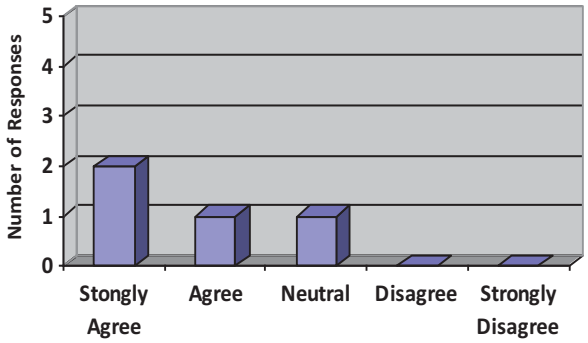

Figure 10.7: Enterprise-wide Business Continuity Plans have been established

Figure 10.7 indicates that 3 respondents, (75%), have developed and implemented enterprise-wide BCPs in their organisations. 1 respondent, (25%), could neither agree nor disagree as to whether such a BCP existed in their organisation.

10.2.7 Lack of or inadequate security procedures

Question 1B: Formal information security procedures that cater for all information system processes have been established.

Table 10.8: Information security procedures have been established

Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
1	2	1	0	0

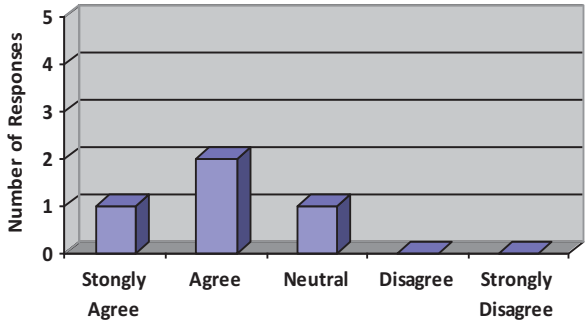

Figure 10.8: Information security procedures have been established

Figure 10.8 indicates that 3 respondents, (75%), believe that their organisations have adequate security procedures in place. 1 respondent, (25%), could neither agree nor disagree as to whether this was the case in their organisation.

10.2.8 Ill-maintained legacy systems

Question 2B: Legacy systems receive the appropriate level of protection as other systems.

Table 10.9: Legacy systems are appropriately protected

Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
0	0	1	1	0

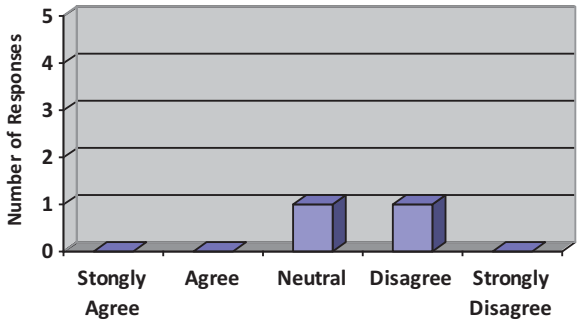

Figure 10.9: Legacy systems are appropriately protected

Figure 10.9 indicates that 1 respondent, (25%), could neither agree nor disagree as to whether their organisation's legacy systems received the same level of protection as other systems, while 1 respondent, (25%), believes their legacy systems are not adequately protected. 2 respondents, (50%), revealed that they no longer have legacy systems in their organisations as they have upgraded all their legacy systems to modern ones.

10.2.9 Cultural clashes between IT staff

Question 3B: Cultural clashes exist between younger and older IT staff over legacy and modern systems.

Table 10.10: Cultural clashes exist between IT staff

Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
0	2	1	0	0

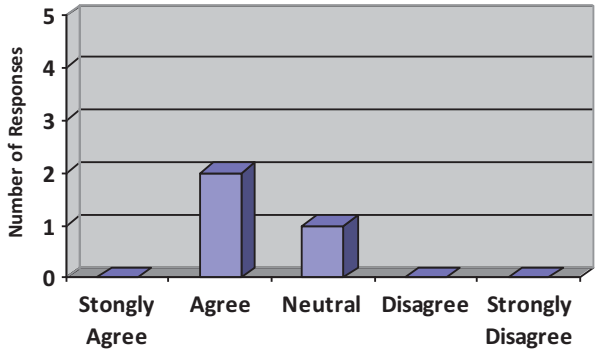

Figure 10.10: Cultural clashes exist between IT staff

Figure 10.10 indicates that 2 respondents, (50%), believe that cultural clashes between IT staff over legacy and modern systems exist in their organisations. 1 respondent, (25%), could neither agree nor disagree as to whether cultural clashes exist in their organisation. 1 respondent, (25%), believed the question was not applicable to the organisation as the organisation does not have legacy systems.

10.2.10 Irregular or no patching of systems

Question 4B: Software patches are regularly applied, thereby improving information security and eliminating security weaknesses.

Table 10.11: Software patches are regularly applied

Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
2	0	2	0	0

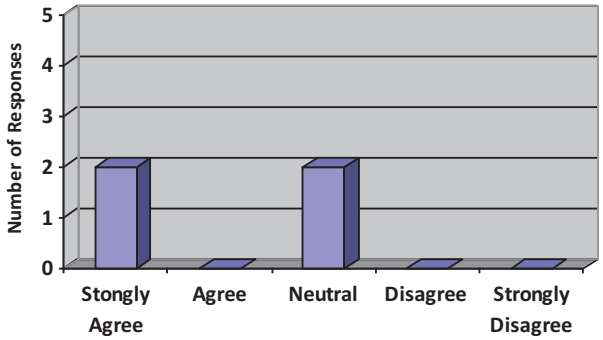

Figure 10.11: Software patches are regularly applied

Figure 10.11 indicates that 2 respondents, (50%), believe that the information systems in their organisations are regularly patched and are thus protected. However, 2 other respondents,

(50%), could neither agree nor disagree as to whether patching of systems in their organisations is done on a regular basis.

10.2.11 Informal change management procedures

Question 5B: Formal change management procedures have been established to control changes to information systems.

Table 10.12: Change management procedures have been established

Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
3	0	0	1	0

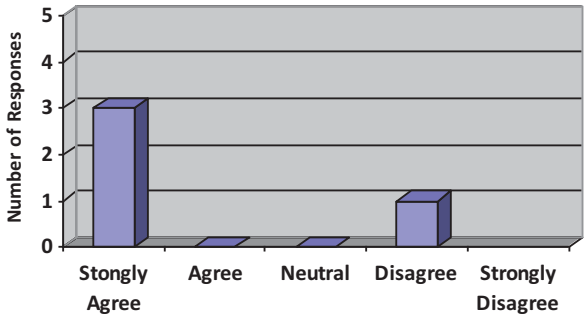

Figure 10.12: Change management procedures have been established

Figure 10.12 indicates that 3 respondents, (75%), firmly believe that formal change management procedures have been established to control changes to information systems in their organisations. 1 respondent, (25%), does not believe this is the case in their organisation.

10.2.12 Environmental threats to hardware

Question 6B: Measures have been put in place to protect information processing equipment from environmental threats

Table 10.13: Equipment is protected from environmental threats

Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
2	2	0	0	0

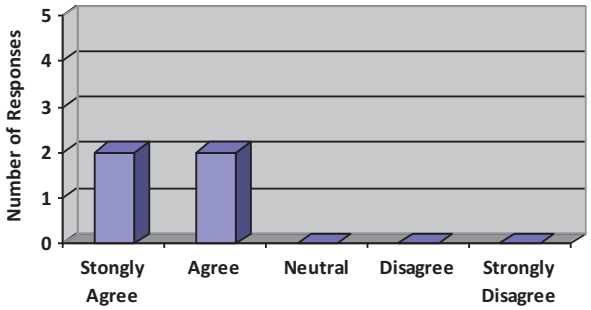

Figure 10.13: Equipment is protected from environmental threats

As illustrated in figure 10.13, all 4 respondents, (100%), believe that their organisations' information processing equipment is protected from environmental threats.

10.2.13 Human error

Question 7B: Information systems are protected from accidental or deliberate human error.

Table 10.14: Information systems are protected from human error

Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
1	3	0	0	0

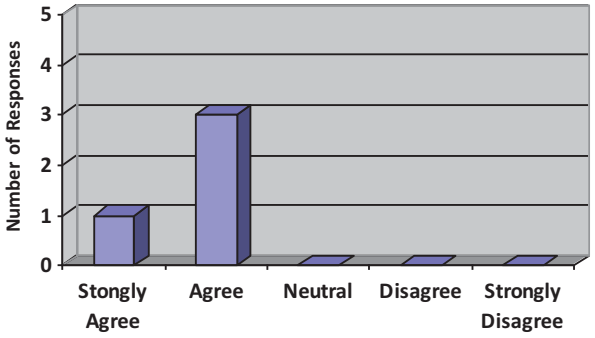

Figure 10.14: Information systems are protected from human error

As illustrated in figure 10.14, all 4 respondents, (100%), believe that their information systems are protected from accidental or deliberate human error.

10.2.14 Ill-defined crisis communication procedures

Question 8B: Crisis management procedures have been clearly defined.

Table 10.15: Crisis management procedures have been clearly defined

Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
2	0	2	0	0

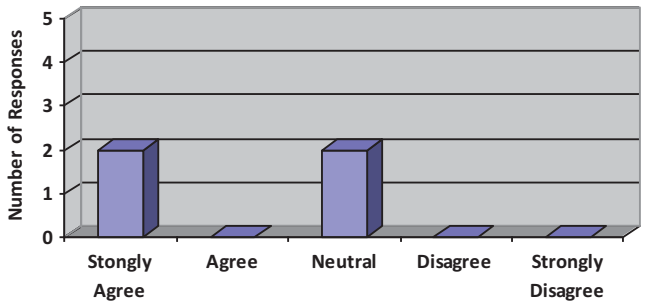

Figure 10.15: Crisis management procedures have been clearly defined

Figure 10.15 indicates that 2 respondents, (50%), believe that crisis management procedures have been clearly defined in their organisations. 2 respondents, (50%), however, could neither agree nor disagree as to whether this was the case in their organisations.

10.2.15 Poor staff awareness

Question 9B: All staff are given adequate and appropriate information security education, training, and awareness.

Table 10.16: Staff are given appropriate security education, training and awareness

Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
2	0	0	2	0

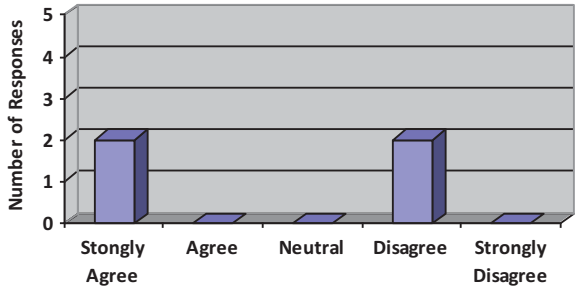

Figure 10.16: Staff are given appropriate security education, training, and awareness

As illustrated in figure 10.16, 2 respondents, (50%), firmly believe that all staff are given appropriate information security education, training, and awareness. 2 other respondents, (50%), feel that this is not the case in their organisations.

10.2.16 Poor asset identification and inventory

Question 10B: All assets used for information processing can be identified and located.

Table 10.17: Assets have been identified and inventoried

Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
2	1	1	0	0

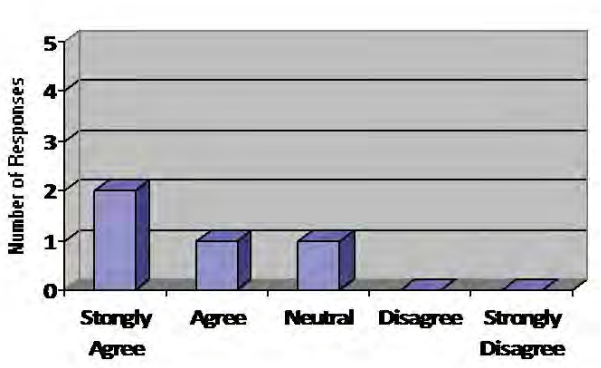

Figure 10.17: Assets have been identified and inventoried

As illustrated in figure 10.17, 3 respondents, (75%), claim all assets used for information processing can be identified and located. 1 respondent, (25%), could neither agree nor disagree as to whether this was the case in their organisation.

10.2.17 Inadequate email policies

Question 11B: Adequate electronic mail management policies and procedures have been implemented.

Table10.18: Adequate email policies and procedures have been established

Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
2	2	0	0	0

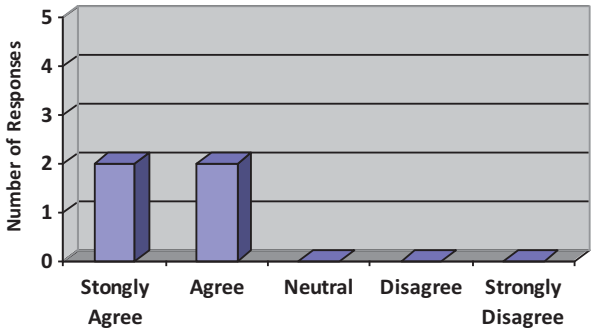

Figure 10.18: Adequate email policies and procedures have been established

As illustrated in figure 10.18, all 4 respondents, (100%), believe their organisations have implemented policies and procedures for adequate electronic mail management in their organisations.

10.2.18 Email threats such as viruses and spam

Question 12B: Electronic communication has been protected against both external and internal threats.

Table 10.19: Electronic communication is protected from threats

Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
2	2	0	0	0

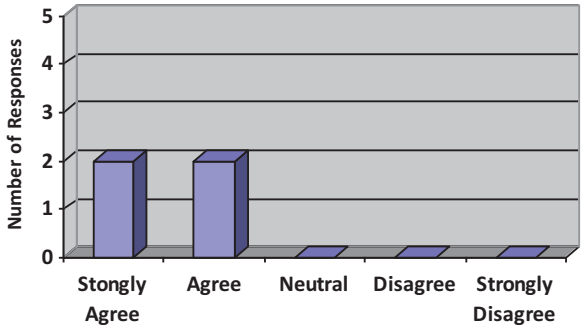

Figure 10.19: Electronic communication is protected from threats

As illustrated in figure 10.19, all 4 respondents, (100%), claim electronic communication has been protected against external and internal threats in their organisations.

10.2.19 Poor incident response plans

Question 13B: Information security incident reporting responsibilities and channels have been defined.

Table 10.20: Incident response plans have been defined

Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
2	0	2	0	0

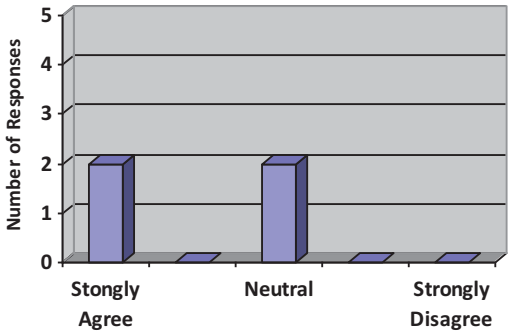

Figure 10.20: Incident response plans have been defined

Figure 10.20 indicates that 2 respondents, (50%), firmly believe that their information security incident reporting responsibilities and channels have been defined. 2 respondents, (50%), could neither agree nor disagree as to whether these incident reporting responsibilities and channels have been defined in their organisations.

10.2.20 Unsecure application software

Question 14B: Information security requirements are emphasised during the procurement and development of application software.

Table 10.21: Information security application software is emphasised

Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
1	1	1	1	0

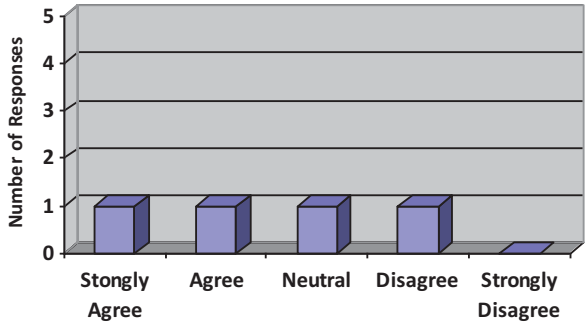

Figure 10.21: Information security application software is emphasised

Figure 10.21 indicates that 2 respondents, (50%), believe that information security requirements are emphasised during the procurement and development of application software in their organisations. 1 respondent, (25%), could neither agree nor disagree as to whether these requirements are emphasised as there are cases when there are violations in the procurement process. 1 other respondent, (25%), believes these information security requirements are not emphasised in their organisation.

10.2.21 Inadequate access control procedures

Question 15B: Adequate access control procedures have been established and they meet the organisation's security requirements.

Table 10.22: Access control procedures and requirements have been established

	Yes	No	Partial
Access control procedures have been established	4	0	0
Access control procedures meet security requirements	3	0	1

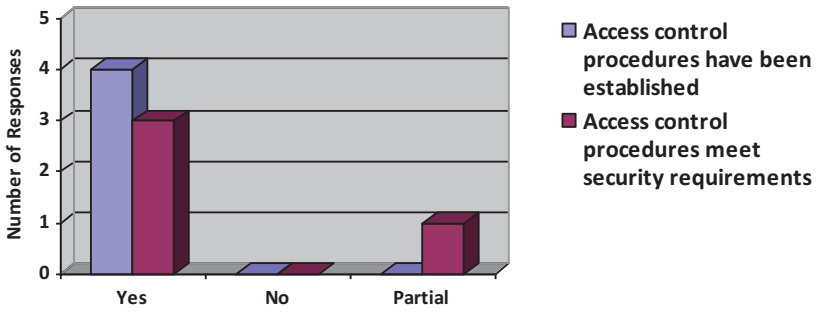

Figure 10.22: Access control procedures and requirements have been established

Figure 10.22 indicates that all 4 respondents, (100%), claim that adequate access control procedures have been established in their organisations. Furthermore, 3 of these respondents, (75%), believe that these access control procedures meet their organisations' security requirements and 1 respondent, (25%), believes these access control procedures only partially meet their organisation's information security requirements.

10.2.22 Lack of formal mobile security governance

Question 16B: Mobile security governance measures have been put in place to address mobile computing and communications.

Table 10.23: Mobile security governance measures are in place

Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
1	1	1	1	0

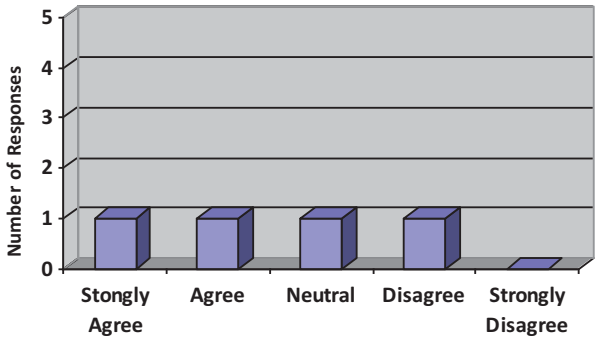

Figure 10.23: Mobile security governance measures are in place

Figure 10.23 indicates that 2 respondents, (50%), believe mobile security governance measures have been put in place to address mobile computing and communications in their organisations. 1 respondent, (25%), could neither agree nor disagree as to whether these security measures have been put in place while 1 respondent, (25%), does not believe these security measures have been put in place in their organisation.

10.2.23 IT-based Business Continuity Plans (BCPs)

Question 17B: We have detailed Business Continuity Plans (BCPs) in place, which specify the actions to be taken to keep the organisation functioning in the event of a disaster.

Table 10.24: Detailed Business Continuity Plans have been established

Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
1	1	1	1	0

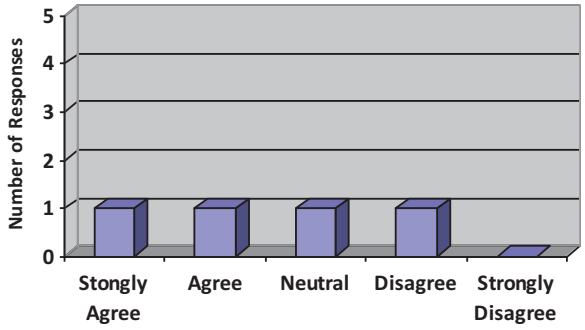

Figure 10.24: Detailed Business Continuity Plans have been established

Figure 10.24 indicates that 2 respondents, (50%), have detailed BCPs in place which specify actions that should be taken in the event of a disaster. 1 respondent, (25%), could neither agree nor disagree as to whether these detailed BCPs are in place, while 1 other respondent, (25%), does not believe these detailed BCPs are in place in their organisation.

10.2.24 Dispersed data and information

Question 18B: All organisational data and information has been consolidated and can be accounted for.

Table 10.25: Organisational data and information have been consolidated

Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
1	0	2	1	0

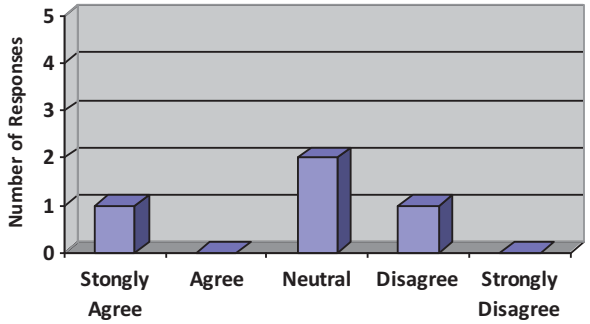

Figure 10.25: Organisational data and information have been consolidated

Figure 10.25 indicates that 1 respondent, (25%), firmly believes that all organisational data has been consolidated and accounted for in their organisation. However, 2 respondents, (50%), could neither agree nor disagree as to whether their organisations' data has been consolidated and accounted for. 1 respondent, (25%), on the other hand does not believe that

all their organisation's data and information have been adequately consolidated for it be appropriately accounted for.

10.2.25 Inadequate control system policies and procedures

Question 19B: Policies and procedures that cater for control systems are in place.

Table 10.26: Adequate control system policies and procedures have been established

Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
1	1	0	2	0

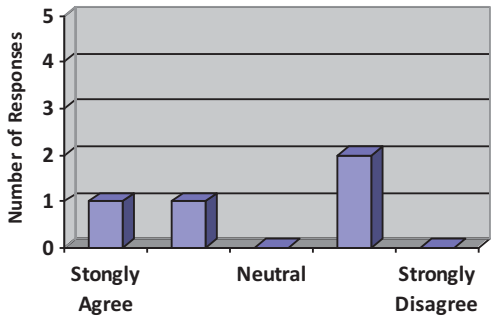

Figure 10.26: Adequate control system policies and procedures have been established

Figure 10.26 indicates that 2 respondents, (50%), believe that adequate policies and procedures for control systems have been implemented in their organisations. 2 other respondents, (50%), do not believe that these policies and procedures are adequate enough to offer complete protection for their control systems.

10.2.26 Lack of or irregular testing of contingency plans

Question 20B: Contingency plans to deal with systems failures have been established and are regularly tested and reviewed.

Table 10.27: Contingency plans are regularly reviewed and tested

Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
2	0	1	1	0

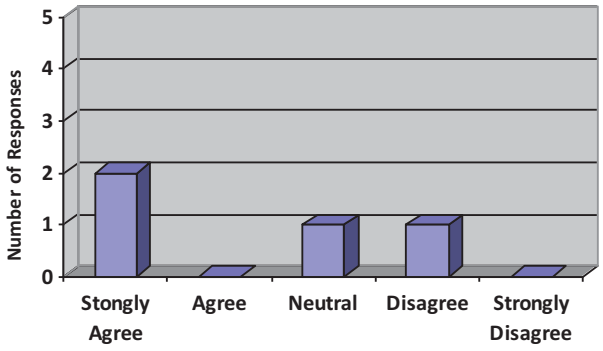

Figure 10.27: Contingency plans are regularly reviewed and tested

Figure 10.27 indicates that 2 respondents, (50%), firmly believe that contingency plans to deal with system failures in their organisations have been established and are regularly tested and reviewed. 1 respondent, (25%), could neither agree nor disagree as to whether these contingency plans have been established and are regularly tested or reviewed. 1 other respondent, (25%), does not believe these contingency plans have been established or are regularly reviewed and tested.

10.2.27 Inadequate risk management process

Question 21B: Information security risks are regularly assessed and managed.

Table 10.28: Risks are regularly assessed and managed

Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
1	2	0	1	0

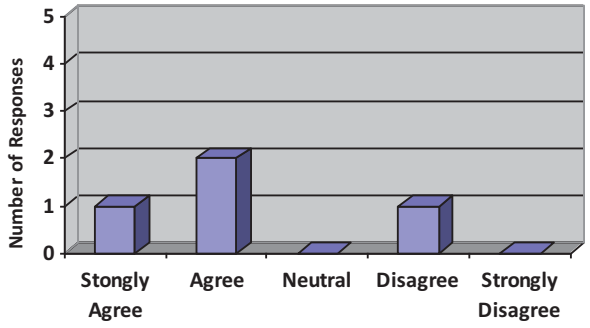

Figure 10.28: Risks are regularly assessed and managed

Figure 10.28 indicates that 3 respondents, (75%), believe that information security risks are regularly assessed and managed in their organisations. 1 respondent, (25%), does not believe this is the case in their organisation.

10.2.28 Ill-defined user access privileges

Question 22B: User access privileges to all systems are restricted and controlled.

Table 10.29: User access privileges are restricted and controlled

Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
3	0	1	0	0

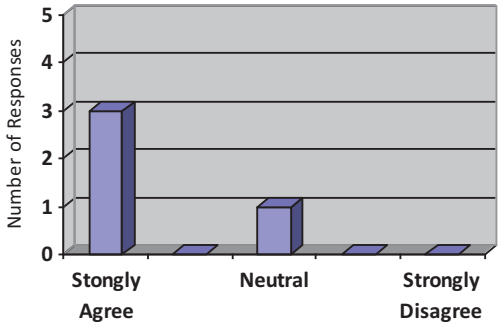

Figure 10.29: User access privileges are restricted and controlled

Figure 10.29 indicates that 3 respondents, (75%), strongly agree that user access privileges to all systems are controlled and restricted. 1 respondent, (25%), could neither agree nor disagree as to whether these privileges are controlled or restricted.

10.2.29 Summary of Leadership Perception Questionnaire Findings

From the findings outlined above, leaders in four copper mining believe information security practices have been implemented in their organisations. They also believe most of the concerns raised in the literature review are adequately addressed and only a few require attention. The concerns deemed by senior management to require a higher level of addressing than others include poor staff awareness and inadequate control system policies and procedures. These findings will be further analysed in Chapter 11.

10.3 Information Security Domains

The ISO/IEC 27002 standard has 11 information security domains; hence each questionnaire in the audit tool represents an information security domain. These questionnaires were administered in one of the four copper mining organisations referred to as "Mine A", in order to gain an in-depth understanding of the actual practices in this mining organisation. The results and analyses of this study are provided per information security domain.

10.3.1 Domain 1: Security Policy Management

This section discusses the development and implementation of an information security policy in an organisation and addresses the extent to which concerns identified in the literature review affect information security policy management in the organisation in question.

As discussed in section 6.3.4, an information security policy is the backbone of information security and provides structure and purpose for all other aspects of information security (Peltier *et al.,* 2005: 17). Therefore, all of the 28 issues identified in the literature review and outlined in tables 8.1 and 8.2 of chapter 8, are deemed to have an effect on information security policy management.

Domain 1 questionnaire covers the establishment of an information security policy in an organisation. This involves developing and reviewing an information security policy.

Of the 28 security concerns identified in the literature review, 8 are relevant to the Domain 1 questionnaire. Of these 8 concerns applicable to Domain 1, 4 were considered to require addressing. These concerns are listed below:

- *Lack of or inadequate information security policy*: The organisation's information security policy is not up to date.
- *Poor incidence response plans*: Incident reporting responsibilities have not been defined in the information security policy.
- *Increased regulation*: Compliance requirements have not been explained or mentioned in the information security policy.

- *Inadequate risk management process*: The organisation's approach to risk management and risk assessment has not been described in the information security policy.

Likewise, of the 8 concerns applicable to Domain 1, 4 of these would seem to be adequately addressed at mine A. These include:

- *Informal BCPs*: Business continuity requirements important to the organisation have been addressed in the information security policy.
- *Inadequate integration of information security into employment policies and practices*: SETA requirements have been briefly explained in the information security policy.
- *Lack of formal information security governance frameworks*: an information security governance framework exists in the organisation (an information security policy exists and management is committed to it).
- *Incorrect dissemination or disclosure of information*: sensitive organisational information will not be disclosed in case the information security policy is wrongly distributed.

The Domain 1 questionnaire results outlined above indicate that 14% of the 28 concerns that were identified in the Domain 1 questionnaire have been addressed while a further 14% still require attention. This is represented in figure 10.30 below.

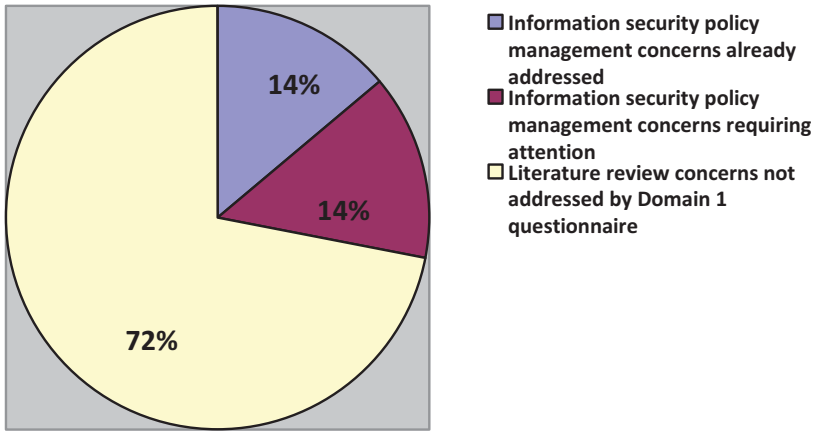

Figure 10.30: Information Security Policy Management Concerns as identified in the literature review

Figure 10.31 below gives a summary of Domain 1 questionnaire responses. The Domain 1 questionnaire addressed establishing an information security policy. N/C (Notes and Comments) represents responses that did not fall under the "Yes", "No" or "N/A" options.

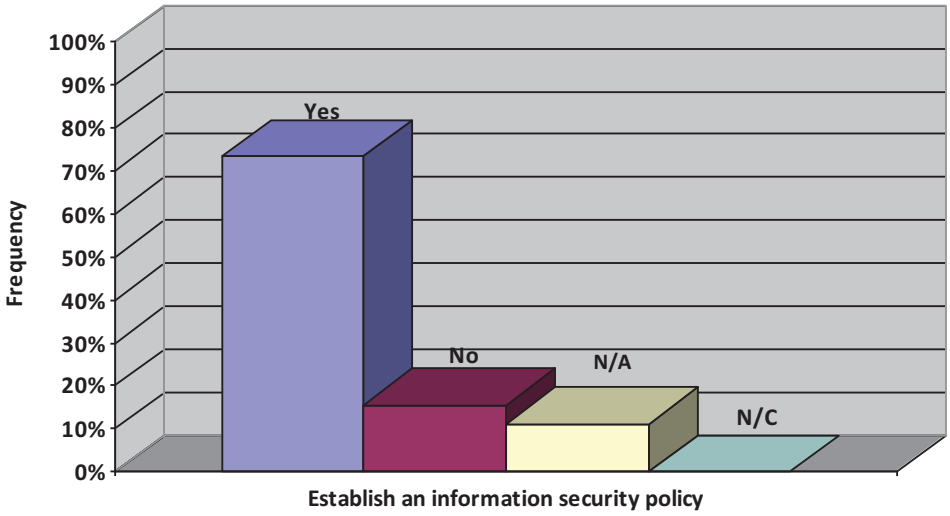

Figure 10.31: Domain 1 Questionnaire Responses

Discussion

From the Domain 1 questionnaire responses as illustrated in figure 10.31, 73% were positive, 16% were negative responses, while 11% of the questions were not applicable to current information security practices in the organisation. None of the questions in the questionnaire were applicable to the "N/C" category.

Furthermore, Domain 1 questionnaire responses revealed that an information security policy exists in the organisation and management supports and is committed to information security. Although not all issues raised in the literature review were represented in the Domain 1 questionnaire, an information security policy creates a foundation for information security in the organisation and was thus deemed to have an effect on all concerns as illustrated in tables 8.1 and 8.2. An information security policy has been established in Mine A and is made available to employees and other relevant parties. Security Education, Training, and Awareness (SETA) requirements for personnel are briefly explained in this policy. This emphasises the importance of this practice in the organisation.

In addition to the above, although Mine A's changing information security requirements are examined, the information security policy is not regularly reviewed and updated. As a result, organisational changes that have occurred since the last revision may not be addressed within Mine A's information security policy. Furthermore, employees may be adhering to policies that are not up-to-date as that is what is availed to them. As discussed in section 1.1, an information security policy should be regularly reviewed, kept up-to-date and all concerned parties made aware of the changes as it is the cornerstone of any information security program. A formal security team does not exist but is in the process of being formed. This has possibly contributed to irregular reviews of the information security policy. Mine A has a principle information security policy which it has further divided into a set of policies to cater for specific issues. Hence, the principle information security policy may not be as comprehensive as the organisation's other information security policies and procedures. However, these policies and procedures are not referred to in the principle information security policy document. According to ISO/IEC 27002, not all issues considered to be relevant in an information security policy, have been mentioned in Mine A's policy document. These issues will be discussed further in chapter 11.

Although Mine A's information security policy seemingly complies with all relevant laws and regulations, information security related regulations have historically not been highly enforced in Zambia. The organisation is also yet to adopt the new ICT regulations that were recently enacted, one of these being the Electronic Communications and Transactions Act of 2009. Mine A has not yet adopted an information security framework that would be used to establish security objectives and controls nor does the information security policy describe a framework that can be used to establish these objectives and controls. Information security standards that are important to the organisation have equally not been explained in the policy. It is worth noting, however, that adoption of the ISO/IEC 27002 standard and ITIL is currently under consideration in Mine A.

Mine A has established an information security governance framework. As feared by the results of a 2008 Deloitte Touche Tohmatsu survey on energy and resources industries discussed in section 6.6, however, some of the information security governance pillars identified in section 6.3 require addressing while others do not. Considering that risk management is a strong pillar of information security management and governance as discussed in sections 6.2.1 and 6.3.7 respectively, it is interesting to note that it has not been

mentioned in the organisation's information security policy, neither does the organisation have an information security risk management policy in place. An organisation-wide risk management policy, however, exists, but does not explicitly address information security risk management.

Although incident management has not been mentioned nor a referral made to it in the information security policy, the organisation has an incident management policy in place.

Although there were more "Yes" responses than "No" responses in the Domain 1 questionnaire as shown in figure 10.31, "No" responses indicate that there are some gaps in information security practices in the organisation that require addressing. Addressing these would make information security policy management more adequate for the organisation.

10.3.2 Domain 2: Corporate Security Management

This section discusses the management of information security in an organisation. It also addresses the extent to which information security concerns identified in the literature review affect effective information security management. According to ISO/IEC 27002, a management framework should be established to develop and implement information security as part of corporate information security management in the organisation.

Domain 2 questionnaire addressed establishing an internal security organisation and controlling external party use of an organisation's information. This involves making an active commitment to information security, coordinating information security implementation for both internal and external parties and performing information security reviews.

Of the 28 concerns identified in the literature review, 12 concerns were relevant to the Domain 2 questionnaire. Of these 12 concerns applicable to Domain 2, 7 were considered to require addressing. These include:

- *Lack of or inadequate information security policies:* the organisation's information security policy is not regularly reviewed.
- *Lack of or inadequate information security procedures:* security communication procedures do not specify when law enforcement agencies should be contacted.

- *Poor staff awareness:* plans and programs to ensure that information security awareness is established and maintained are not adequately set up.
- *Poor incident response plans:* incident related security communication procedures do not specify when to contact law enforcement or emergency response services.
- *Poor asset inventory and identification:* Some areas and assets that need protection have not been identified or responsibility allocated for them.
- *Lack of formal information security governance frameworks:* overall responsibility for managing information security in the organisation has not been assigned to a special management forum or management group.
- *Informal Business Continuity Plans:* responsibility for continuity planning is on a system-by-system basis.

According to Domain 2 questionnaire responses, 5 of the concerns identified in the literature review have been addressed by Mine A. These include:

- *Inadequate risk management process:* risk assessments are carried out whenever external parties require access to the organisation's information.
- *Increased regulation:* the organisation anticipates and prepares for upcoming regulations by maintaining relationships with regulatory bodies.
- *Lack of or irregular testing of contingency plans:* support for business continuity planning is provided by maintaining contact with external organisations.
- *Lack of formal mobile security governance*: business use of personal or privately owned handheld devices and laptops is controlled.
- *Incorrect disclosure or dissemination of information:* confidentiality and non-disclosure agreements have been established to protect the organisation's information.

The Domain 2 questionnaire results outlined above indicate that 18% of the 28 concerns that were identified in the Domain 2 questionnaire have already been addressed while 25% still need addressing. This is illustrated in figure 10.32 below.

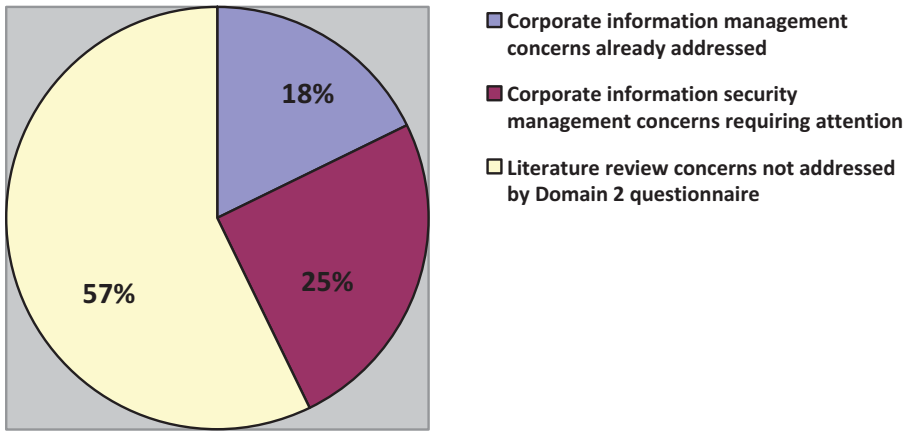

Figure 10.32: Corporate Security Management Concerns as Identified in the Literature Review

Figure 10.33 gives a summary of Domain 2 questionnaire responses from the two questionnaire subsections. The subsections included in this questionnaire are "establish an internal security organisation" and "control external party use of information".

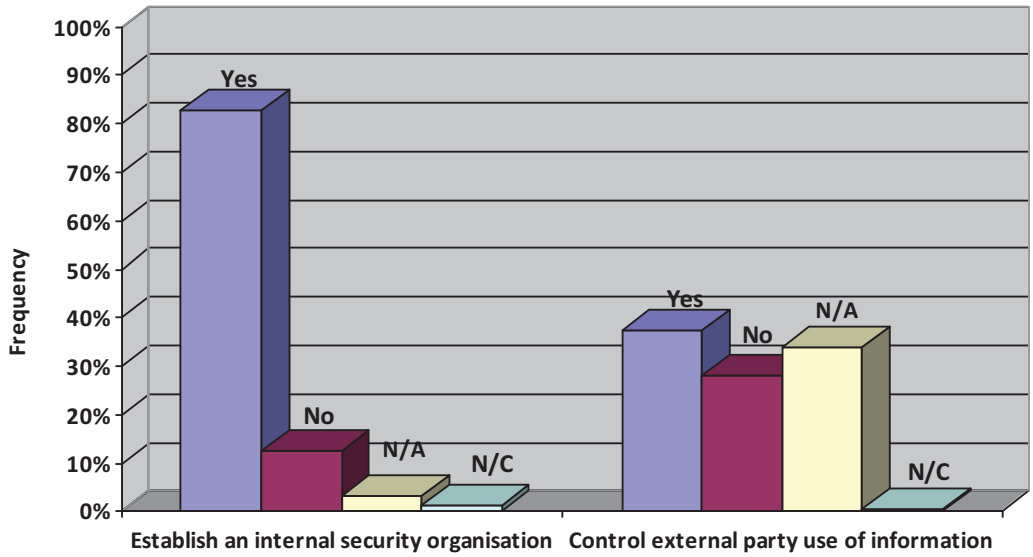

Figure 10.33: Domain 2 Questionnaire Responses

Discussion

Figure 10.33 indicates that Mine A has established corporate security management practices. A high number of "N/A" responses (34%) under the "control of external party use of

information" subsection represents a section of the questionnaire that dealt with addressing security before customers are given access. This section did not apply to Mine A as the organisation's customers only require access to Mine A's public information.

Information security roles and responsibilities in Mine A have not been explicitly allocated which may bring about lack of ownership of information assets. Information security coordinators who work in various sections of the IT function are responsible for handling information security programs. An information security manager or team has not yet been appointed to co-ordinate the information security function in the organisation. Hence, accountability and responsibility for information security programs may not be handled effectively. Furthermore, although information security awareness programs as discussed in 6.3.3 are required to help maintain information security in day-to-day operations, plans and programs to establish and maintain these programs have not been formally set up. In the same way, whereas business use of personal or privately owned handheld devices or laptops is controlled, awareness programs are not in place to emphasise this regulation.

In addition to the discussion in section 10.3.1, management is not interviewed on the need to review the information security policy. Hence the policy's adequacy may be rendered questionable.

Information assets in the organisation have not been formally classified and not all assets associated with a particular system and needing protection have been identified. An informal classification method exists but does not get distributed to all functional areas. Hence, these assets may not be properly protected or accounted for especially since mining organisations possess a large number of both physical and information assets. Section 4.7 identified that with the exception of physical assets, the industry has previously not had all its information assets well covered for adequate risk management purposes. This was found to be the case in Mine A. Responsibility for continuity planning for these assets is, however, done on a system-by-system basis which does not give a complete picture of the continuity process. Although management provides authorisation for new information processing facilities, overall responsibility for information security has not been allocated to a management group but is part of the overall management responsibility of the IT department. The information security function may, therefore, not receive as much attention and support as it should from senior management. An independent information security review is carried out regularly but

is not carried out whenever major implementation changes take place to determine whether any information security enhancements are required. The organisation makes use of internal security reviews which it finds appropriate for the task.

The organisation has not established third-party security agreements but uses organisation-wide policies and procedures when dealing with external parties. Although confidentiality and non-disclosure agreements do not specify an end date for non-disclosure of the organisation's information, these agreements are binding for life. The agreements apply to all situations and do not differ whether they are applying to internal or external parties. In addition, risk assessments are also carried out when external parties require access to the organisation's information processing facilities.

Zambia being a member of WIPO and ARIPO mandates that all organisations and institutions need to take ownership for and protect Intellectual Property Rights (IPR). Ownership and the need for protection of IPR regarding trademarks, copyrights, industrial design rights, patents, and trade secrets have been clarified in Mine A to provide a level of protection for the organisation's assets. However, this is not made clear to all parties involved, especially where copyright accountability is concerned.

The organisation has an incident reporting procedure for insurance purposes and another for reporting information related incidents. These procedures do not, however, specify when law enforcement or emergency response agencies should be notified. This is required for accelerated response to an incident when these agencies are required. The organisation however, has a general emergency response plan.

10.3.3 Domain 3: Organisational Asset Management

This section discusses the achievement and maintenance of appropriate protection of organisational assets. The Domain 3 questionnaire addresses establishing responsibility for assets and using an information classification system to indicate levels of protection assigned to each asset.

Establishing responsibility for assets involves compiling an inventory of assets, selecting owners for these assets and establishing rules for acceptable use of these assets. Similarly, using an information classification system involves developing information classification guidelines and using information handling and labelling procedures.

Of the 28 concerns identified in the literature review, 13 concerns were addressed in the Domain 3 questionnaire. Of these concerns, 8 concerns are considered to require addressing while 5 do not. The 8 concerns that require addressing include:

- *Lack of or inadequate security procedures:* information handling or labelling procedures are not clearly defined.
- *Informal Business Continuity Plans:* an inventory of BCPs has not been completely compiled.
- *Poor asset identification and inventory:* a formal information classification does not exist and asset inventory is incomplete.
- *Poor staff awareness:* some employees are not aware of the organisation's acceptable use rules, guidelines and limits.
- *Dispersed data and information:* data regarding information assets is not centralised and easily accessible but rather dispersed throughout the organisation.
- *Inadequate email policies:* Some employees do not follow the rules that define how electronic mail should be used.
- *Environmental threats to hardware:* computer and communications equipment inventory is incomplete.
- *Lack of mobile security governance:* rules defining how mobile devices should be used both in and outside the organisation's premises are not completely followed.

According to Domain 3 questionnaire responses, 5 of the concerns identified in the literature review have already been addressed by Mine A. These include:

- *Lack of formal information security governance frameworks:* rules defining acceptable use of information have been defined, documented and implemented.
- *Increased regulation:* information classification takes into account legal requirements.
- *Inadequate access control procedures:* asset owners are responsible for defining and reviewing access restrictions to assets.
- *Inadequate risk management process:* inventoried assets support the organisation's risk management activities.

- *Incorrect dissemination or disclosure of information:* information owners are responsible for defining and reviewing access restrictions in accordance with access control policies.

The Domain 3 questionnaire results outlined above indicate that 18% of the 28 concerns that were identified in the Domain 3 questionnaire have already been addressed while 29% still need addressing. This is illustrated in figure 10.34 below.

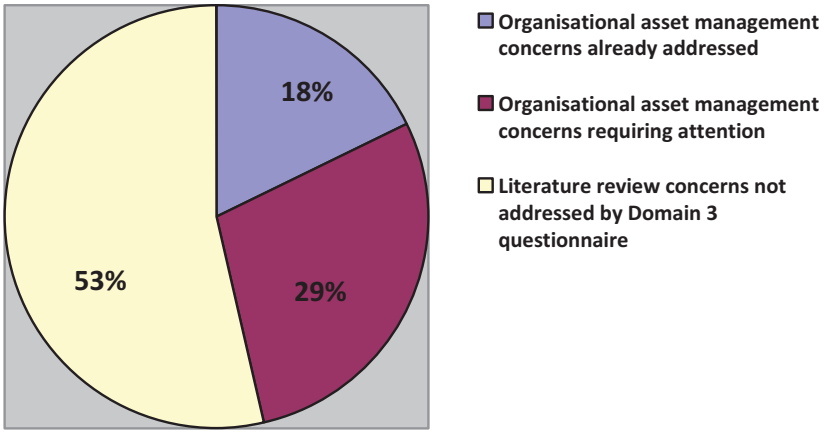

Figure 10.34: Organisational Asset Management Concerns as Identified in the Literature Review

Figure 10.35 gives a summary of Domain 3 questionnaire responses from the two questionnaire subsections. The subsections included in this questionnaire are "establish responsibility for assets" and "use an information classification system".

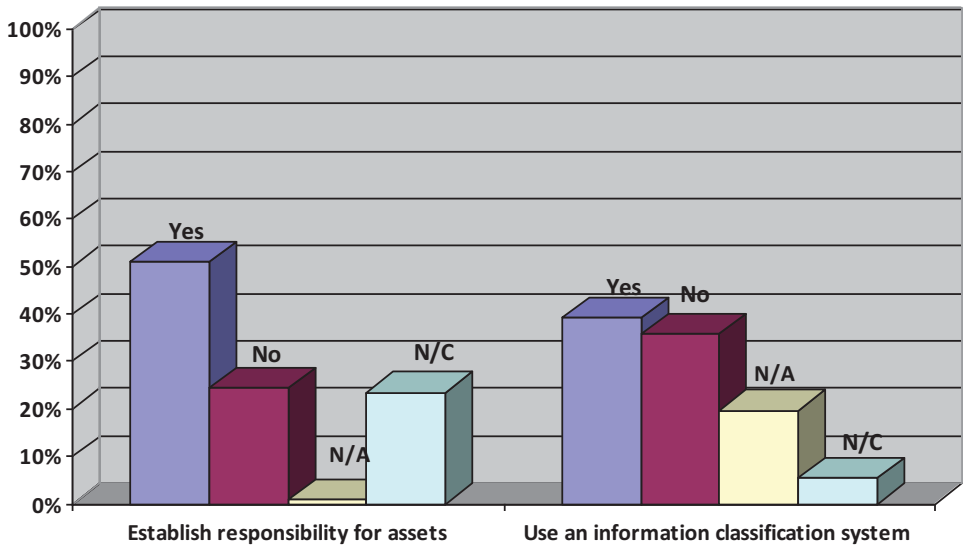

Figure 10.35: Domain 3 Questionnaire Responses

Discussion

From the Domain 3 questionnaire responses, a high number of "yes" responses in both subsections as illustrated in figure 10.35, indicate that Mine A recognises the need for the establishment of responsibility for assets and the use of an information classification system. In as much as this is the case, appropriate measures are not yet fully in place to support the effective management of these assets, hence the equally high number of "No" responses in the questionnaire.

The organisation does not have a formal information classification procedure. Recommended information classification schemes were discussed in section 4.3.1 and will be discussed further in chapter 11. Responsibility for information classification of certain information is assigned to information owners. Although an information classification system has not been formally put in place, information handling procedures have been developed for information assets that have been identified. Although the inventoried assets address Mine A's risk management activities, the absence of a formal information classification system puts the organisation's information assets at risk of being wrongfully disclosed. Zambian copper mines have a lot of stakeholders who either have direct or indirect access to the organisations' information. These stakeholders, as illustrated in figure 2.1 of section 2.4, should receive the appropriate information.

Section 4.7 established that mining organisations have diverse sources of information which often makes it difficult to carry out a complete inventory. Similarly, Mine A does not have a complete inventory of its information sources. Being a large organisation, the exact locations of assets are often not identified as they are usually moved from one place to another. As discussed in section 4.3.1, poor asset identification and inventory will lead to a failed risk assessment project placing the organisation's operations at risk. Nonetheless, Mine A assigns ownership to the assets and business processes that have been identified. Information labelling procedures have also been developed for easy identification of physical assets. Mine A has further established an asset loss prevention procedure where responsibility for asset protection lies in the hands of the employees but is ultimately that of the Heads of Department (HoDs) and supervisors. This responsibility cannot, however, be effective considering that some assets still remain unidentified. As inventory for computer and communications equipment is incomplete, environmental threats to the organisation's hardware may not be adequately catered for. A complete inventory of BCP is also required for effective contingency measures. Mine A's BCP inventory is incomplete thus reducing the effectiveness of these measures.

A policy on acceptable use of electronic communication exists in Mine A. This policy encompasses all electronic communication infrastructure. Email usage and internet usage policies are also in place. However all three (3) policy documents have not been updated to reflect current practices. Use of mobile devices both inside and outside the organisation's premises cannot be easily controlled, neither is the content of emails that are sent using Mine A's facilities. These are information security issues that not only affect Mine A but are also being addressed globally. Although section 4.7 recommends auditing, implementation of policies and archiving to protect sensitive company information, security of this information still cannot be guaranteed. In addition to the above recommendations, Mine A protects itself from legal implications through the use of a disclaimer that is part of every email that is sent outside the organisation. One of the measures Mine A has put in place for the control of mobile device use is the blocking of USB ports. Although this does not completely protect the organisation's information, it minimises unauthorised transfer of information and can reduce virus transmission.

Although all contractors, third parties and new employees undergo information security induction when engaging with the organisation, ongoing awareness programs are currently

not in place for employees who are already in the organisation. These programs are, however, in the process of being initiated. Ongoing awareness programs ensure employees are continuously aware of their information security obligations.

10.3.4 Domain 4: Human Resource Security Management

This section discusses the roles and responsibilities that employees, third parties and contractors have towards information security. This involves emphasis on security prior to, during and after termination of employment.

According to ISO/IEC 27002 and the Domain 4 questionnaire, security prior to employment involves defining information security roles and responsibilities for prospective employees, third party users and contractors, verifying backgrounds of new personnel, and using contracts to protect the organisation's information. Security during employment involves managers being responsible for emphasising security, delivering information security training programs, and setting up a disciplinary process for information security breaches. In addition, security at termination involves assigning responsibility for termination or reassignment, ensuring assets are returned and removing access rights.

Of the 28 concerns identified in the literature review, 11 concerns were relevant to the Domain 4 questionnaire. Of these 11 concerns applicable to Domain 4, 4 concerns were considered to require addressing while 7 do not. The 4 concerns that require addressing include:

- *Poor staff awareness:* The level of SETA is currently inadequate.
- *Lack of formal mobile security governance:* organisational information is not completely removed from personal mobile devices.
- *Inadequate integration of information security into employment policies and practices:* job descriptions are not used to document and communicate the organisation's security roles and responsibilities.
- *Ill-defined user access privileges:* Access rights and privileges are not completely removed or adjusted when employees, contractors, or third parties are terminated, re-assigned or when duties change.

According to Domain 4 questionnaire responses, 7 of the concerns identified in the literature review have already been addressed by Mine A. These include:

- *Lack of or inadequate security policies:* The organisation's security roles and responsibilities are defined in accordance with the organisation's information security policy. Security roles and responsibilities emphasise that all personnel must implement and comply with the organisation's information security policy.
- *Lack of or inadequate security procedures:* procedures are in place to ensure that the organisation's assets are returned on termination.
- *Inadequate risk management process:* Risk of theft, fraud or misuse is minimised by ensuring that employees understand their information security roles and responsibilities before they are hired. Organisational security roles and responsibilities make it clear that security risks must be reported.
- *Increased regulation:* Background checks comply with relevant laws and regulations, employment legislation, personal data protection legislation.
- *Lack of formal information security governance frameworks:* Background checks comply with ethical issues.
- *Human error:* The need for employees to reduce risk of human error is emphasised.
- *Incorrect dissemination or disclosure of information:* Information security roles and responsibilities make it clear that the organisation's information and assets must be protected from unauthorised disclosure, access and modification.

The Domain 4 questionnaire results outlined above indicate that 25% of the concerns that were identified in the literature review have already been addressed while 14% still need addressing. This is illustrated in figure 10.36 below.

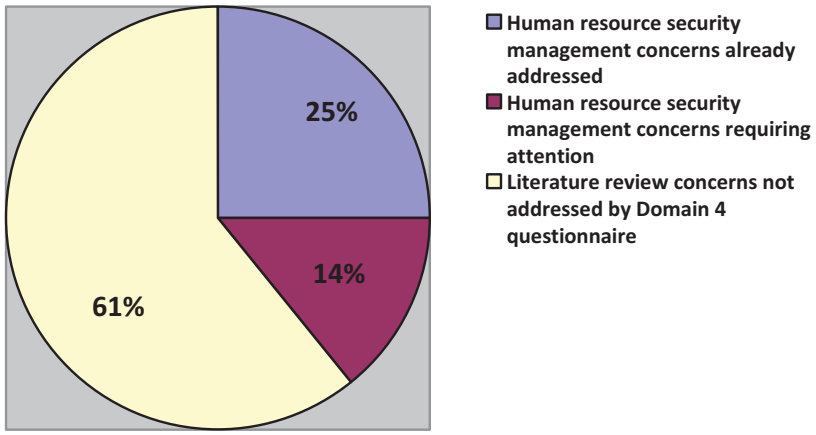

Figure 10.36: Human Resource Security Management Concerns identified in the Literature Review

Figure 10.37 gives a summary of Domain 4 questionnaire responses from the 3 questionnaire subsections. The subsections included in this questionnaire are "emphasise security prior to employment", "emphasise security during employment", and "emphasise security at termination".

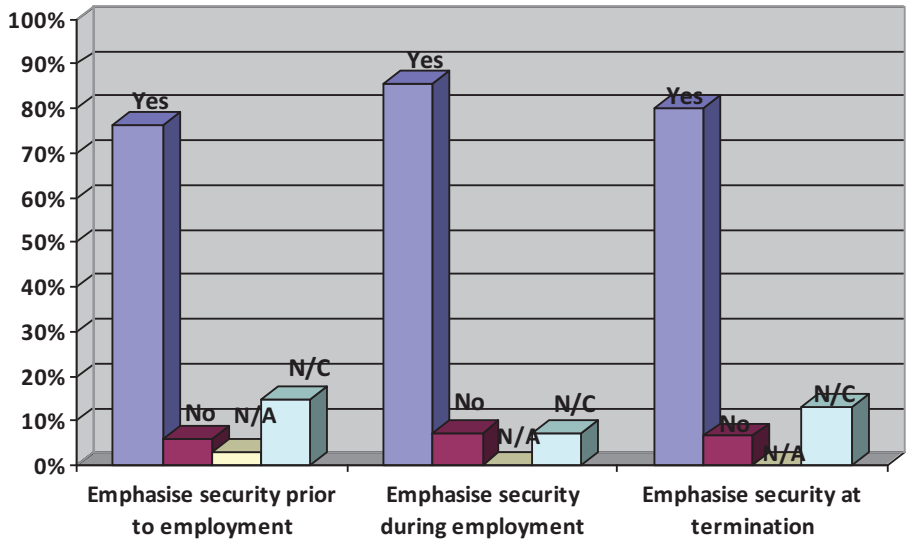

Figure 10.37: Domain 4 Questionnaire Responses

Discussion

From the questionnaire responses as illustrated in figure 10.37, Mine A's information security is highly emphasised to personnel prior to, during and at termination of employment. However, "no" responses indicate that there are still information security gaps that need to be addressed.

Mine A's organisational policies and procedures apply to all personnel who include employees, contractors and third party users. A code of conduct is in place to describe ethical, data protection, and confidentiality obligations and responsibilities. Although personnel sign agreements to specify their information security roles and responsibilities, these roles and responsibilities are not emphasised in the employees' job descriptions or performance appraisals. This may have an effect on the obligatory role that employees play in information security. However, information dissemination and disclosure roles and responsibilities have been integrated into the contracts that employees sign when joining the organisation. Mine A has a formal disciplinary procedure which helps address information security breaches. Confidentiality and non-disclosure agreements are valid for a lifetime which means that there is no end date to information security obligations that personnel have to the organisation. Background checks are also conducted to ensure that the organisation knows the level of risk that potential employees pose to the organisation. These checks comply with ethical and legislative requirements.

Employees are mandated to return company assets on termination. Mine A has a procedure that ensures that company assets are returned on termination and access rights removed. These assets include mobile devices, corporate software, corporate documents, and access cards. The HoD is ultimately responsible for ensuring that these assets are returned. This procedure does not, however, ensure that all information is erased from the employees, third party users or contractor's personal devices. As mentioned in section 10.3.3, organisation's are faced with the challenge of keeping track of information that employees keep on their personal mobile devices. This deters the process of ensuring that employees, contractors, and third parties do not go away with company information on termination.

Both physical and logical access rights to information and information processing facilities for employees, third-party users and contractors are removed on termination. Nevertheless, these controls are still not foolproof. Non-user specific passwords to application systems

together with administrator passwords that were being used by former personnel are not always changed which increases the possibility of an ex-employee conniving with an insider to manipulate these systems. This remains a risk to the organisation especially if the employee was disgruntled on termination. However, plans are underway to enhance physical access controls in the organisation.

Mine A's security policy needs to be up to date as the mine's security roles and responsibilities are defined in accordance with the organisation's information security policy. These roles and responsibilities also emphasise that all personnel must implement and comply with the organisation's information security policy. In addition, security roles and responsibilities emphasise the need to protect the organisation's information assets from unauthorised disclosure, access or modification. The organisation uses induction programs to ensure that potential employees understand these roles and responsibilities before they are given access to information processing facilities. This is meant to minimise the risk of theft, fraud or misuse as the majority of information security incidents are caused by employees. Emphasis is also placed on the need to report any security risks that employees may encounter as well as the need to reduce risk of human error.

Mine A has channels that are used for ongoing awareness. Training and education programs are, however, not in place. Although a formal awareness program is not currently in place, personnel are made aware of information security changes or updates that take place. NIST SP800-12 in section 6.3.3 describes the SETA framework as one that involves the "what" for awareness, the "how" for training and the "why" for education in information security. Therefore, Mine A provides its employees with a certain level of know-how of what information security is all about but does not have programs in place to provide how to go about it or why it needs to be done to achieve the desired level of information security. Part of why it needs to be done is, however, mentioned in the organisation's information security policy and other policies like the incident reporting policy as well as in some of the awareness messages. As suggested by Whitman and Mattord in section 6.3.3, SETA is required as employees are a critical factor in information security and are considered to be the weakest link in information security. This means that no matter how much time and money is spent on information security investments, if the employees' practices and mindsets are not changed, the investment will potentially go to waste.

10.3.5 Domain 5: Physical and Environmental Security Management

This section discusses the management of physical and environmental protection of an organisation's assets.

The Domain 5 questionnaire addresses the use of security areas to protect the organisation's facilities and equipment. Using security areas to protect facilities involves using physical security perimeters, physical entry controls to secure areas, securing offices, rooms, and facilities, protecting facilities from natural and human threats, and isolating and controlling public access points. Protecting the organisation's equipment involves using equipment siting and protection strategies, ensuring supporting facilities are available, securing power and telecommunications cables, maintaining equipment, protecting off-site equipment, controlling equipment disposal and re-use, as well as controlling the use of assets off-site.

Of the 28 concerns identified in the literature review, 12 concerns were relevant to the Domain 5 questionnaire. Of these 12 concerns applicable to Domain 5, 6 concerns were considered to require addressing while 6 were not. The 6 concerns that require addressing include:

- *Poor staff awareness:* Personnel seldom notify security people when they encounter someone not wearing physical identification.
- *Inadequate access control procedures:* Access rights to secure areas are not regularly reviewed.
- *Lack of formal mobile security governance:* Offsite use of personal organisers and mobile phones is not controlled. Portable computers are also not disguised while personnel are travelling.
- *Human error:* clear desk policy is not actively implemented for equipment used offsite.
- *Incorrect dissemination or disclosure of information:* unauthorised use of audio and recording equipment is not completely prevented in secure sites.
- *Dispersed data and information:* Some faults, resolutions and routine maintenance works are not documented.

According to Domain 5 questionnaire responses, 6 of the concerns identified in the literature review have already been addressed by Mine A. These include:

- *Inadequate risk management process:* Physical control methods are commensurate with identified security risks and these risks are assessed to ensure security parameters actually reduce them.
- *Increased regulation:* Physical security controls comply with relevant health and safety regulations and standards.
- *Poor asset identification and inventory:* An inventory of goods leaving and coming into the organisation is carried out.
- *Lack of or irregular testing of contingency plans:* UPS' and generators are in place and tested regularly.
- *Lack of formal information security governance frameworks:* Compliance standards are in place. Management also authorises the removal of information processing facilities for use outside the organisation.
- *Environmental threats to hardware:* Physical methods are used to protect facilities from environmental threats.

The Domain 5 questionnaire results outlined above indicate that 25% of the concerns that were identified in the literature review have already been addressed while 25% still need addressing. This is illustrated in figure 10.38 below.

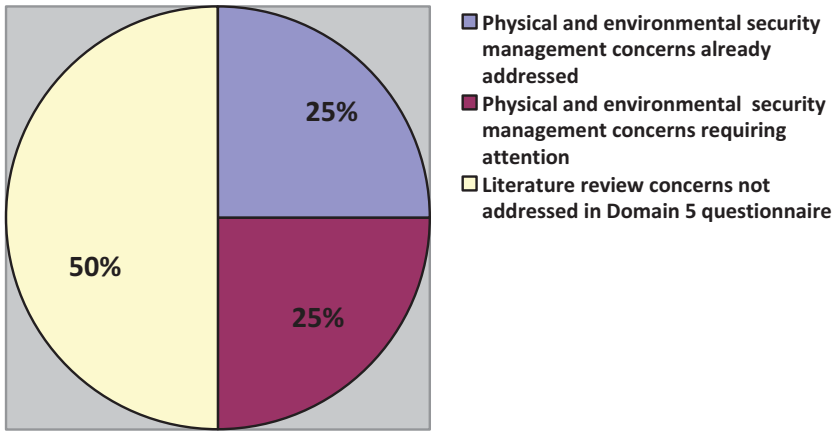

Figure 10.38: Physical and Environmental Security Management Concerns as identified in the Literature Review

Figure 10.39 below gives a summary of Domain 5 questionnaire responses from the 2 questionnaire subsections. The subsections included in this questionnaire are "use security areas to protect facilities" and "protect your organisation's equipment".

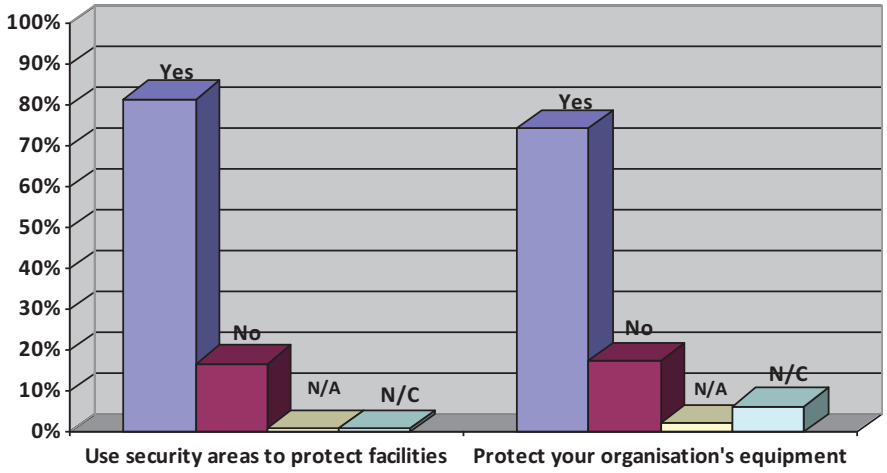

Figure 10.39: Domain 5 Questionnaire Responses

Discussion

Being a high SHEQ regulated organisation, physical and environmental security management is of high priority to Mine A. The high number of "yes" responses indicates that numerous measures have been put in place to comply with these regulations. The organisation equally has certifiable standards in place to ensure high levels of compliance. Physical security controls are established based on these levels of compliance.

Although there is a procedure in place that requires all personnel to wear visible identification, some personnel do not do so and employees have not been sensitised on the need to ensure that they report anyone who is seen without visible identification. Again, as identified from questionnaire responses in Domains 3 and 4 covered in sections 10.3.3 and 10.3.4, respectively, the use of audio and recording equipment cannot be completely controlled in secure areas due to the increasing use of mobile devices,. This puts sensitive information at risk of being wrongly collected and disclosed. A procedure on laptop security requires that organisational laptops are packed in unassuming bags. This is not actively implemented. Equipment that is used offsite cannot easily be monitored nor can the clear desk policy be effectively implemented at home or offsite. Information stored on such

equipment is at risk of being wrongfully accessed, lost or manipulated in addition to the risk of failure that the equipment itself faces. Access rights to secure areas are also irregularly reviewed and may not effectively ensure the security of these areas. Although some areas that accommodate information processing facilities are yet to have access controls effectively implemented, physical access controls to the main information processing facilities have been effectively implemented and are regularly enhanced. Nevertheless, partial implementation of effective physical access controls still leaves potential threats of attack in other areas that are not receiving as much protection. Physical control methods that are implemented in Mine A are assessed commensurate with security risks that are identified to ensure that these risks are reduced. UPS' and generators are in place and are regularly tested for contingency purposes.

Being an organisation that operates under harsh environmental conditions, several measures have been put in place to protect physical information processing facilities. This has been addressed in the organisation's information security policy.

Certain routine maintenance works, faults and resolutions are not documented. This may delay the resolution of a similar fault if it happens to recur. Mine A has a system in place which keeps track of both returnable and non-returnable goods that leave the organisation. The effectiveness of the asset inventorying process is enhanced as management approves the removal of these goods, and is thus accountable and responsible for them.

10.3.6 Domain 6: Communications and Operations Management

This section discusses the establishment of procedures and responsibilities for an organisation's operations and communication facilities.

The Domain 6 questionnaire addresses the establishment of procedures and responsibilities, control of third-party service delivery, future system planning, protection against malicious and mobile code, backup procedures, computer networks, handling of media, information exchange, electronic commerce services, and monitoring of information processing activities.

Of the 28 concerns identified in the literature review, 21 concerns were relevant to the Domain 6 questionnaire. Of these 21 concerns applicable to Domain 6, 13 concerns require addressing while 8 do not. The 13 concerns that require addressing include:

- *Lack of or inadequate security policies:* Policies to protect information and physical media in transit have not been established.
- *Lack of or inadequate security procedures:* Some operating procedures have not been documented. Procedures to protect information and physical media in transit have not been established.
- *Poor staff awareness:* Responsibilities and procedures do not specify what kind of training should be done to cope with malicious code or safeguard sensitive information.
- *Inadequate risk management process:* Risk assessments to determine the level of monitoring is not done for each facility.
- *Inadequate access control procedures:* An independent intrusion detection system is not used to monitor activities of network administrators and some security controls do not prevent collusion.
- *Inadequate email policies:* Controls and restrictions for the forwarding of electronic communications to external destinations have not been established.
- *Informal change management procedures:* Changes to operational and application software are not always tested.
- *Unsecure application software:* Regular security reviews of the data and software that support critical applications are not carried out. Cryptographic controls are not used to authenticate mobile code.
- *Informal Business Continuity Plans:* BCPs do not address the need to recover all necessary data and software.
- *Incorrect dissemination or disclosure of information:* Some of the organisation's printed, faxed or copied data is not controlled and some operating procedures do not explain how information should be handled.
- *Dispersed data and information:* An accurate and complete record of procedures that must be used to restore information is not kept.
- *Lack of or irregular testing of contingency plans:* Backup and restoration procedures are not tested on a regular basis.
- *Human error:* Information handling and storage procedures do not ensure that information is protected from misuse.

According to Domain 6 questionnaire responses, 8 of the concerns identified in the literature review have already been addressed by Mine A. These include:

- *Lack of formal information security governance frameworks:* All changes made to documents and procedures are approved by management.
- *Email threats such as viruses and spam:* Email attachments are checked for malicious code before use.
- *Ill-defined user access privileges:* Logging information is protected from unauthorised changes.
- *Environmental threats to hardware:* Equipment maintenance procedures have been established.
- *Increased regulation:* Retention and disposal guidelines for business correspondence comply with relevant regulations and legislation.
- *Poor incident response plans:* Third parties comply with the organisation's policies and procedures concerning incident management.
- *Poor asset identification and inventory:* Work activities are supervised more closely whenever the security of assets cannot be controlled through segregation of duties.
- *Irregular or no patching of systems:* Malicious code detection and repair software is used to protect the organisation against malicious software.

The Domain 6 questionnaire results outlined above indicate that 29% of the concerns that were identified in the literature review have already been addressed while 46% still need addressing. This is illustrated in figure 10.40 below.

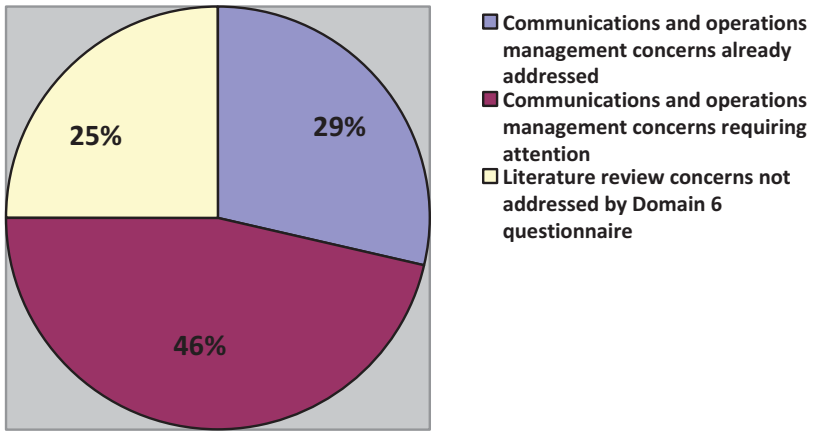

Figure 10.40: Communications and Operations Management Concerns as identified in the Literature Review

Figure 10.41 below gives a summary of Domain 6 questionnaire responses from the 10 questionnaire subsections. The subsections included in this questionnaire are “establish procedures and responsibilities”, “control third-party service delivery”, “carry-out future system planning activities”, “protect against malicious and mobile code”, “establish backup procedures”, “protect computer networks”, “control how media are handled”, “protect the exchange of information”, “protect electronic commerce activities”, and “monitor information processing activities”.

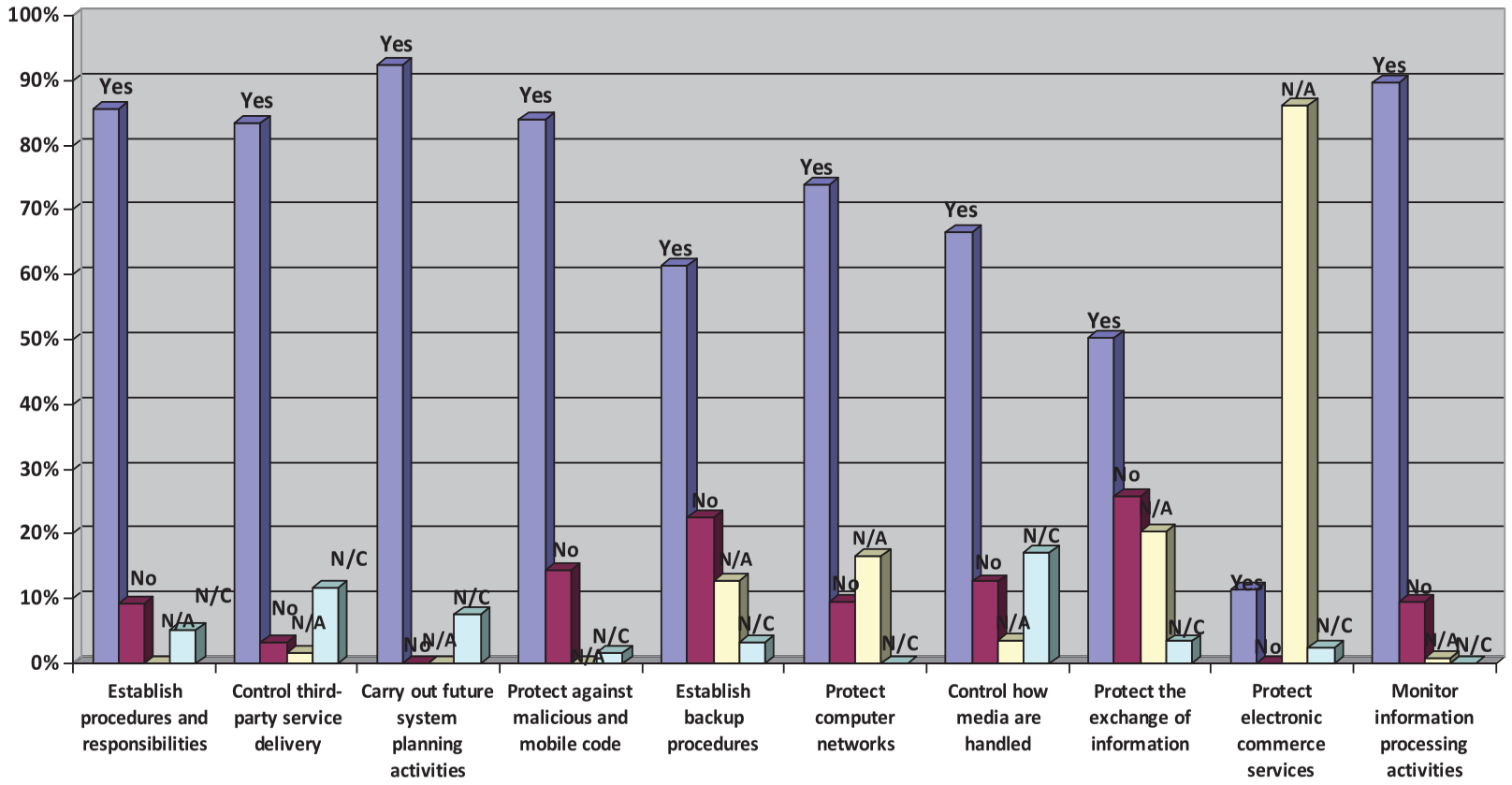

Figure 10.41: Domain 6 Questionnaire Responses

Discussion

There were a high number of "N/A" responses under the "protect electronic commerce services" section as Mine A does not conduct electronic commerce activities but has information that has been made available on public systems.

Mine A has procedures in place that are used to control and operate the organisation's information processing facilities. Plans are also developed to ensure that adequate information processing facilities and capacity will be available in the future. Some operating procedures in the organisation have, however, not been documented. In case of an incident occurring without the availability of the staff who are familiar with the procedures, it would be difficult to carry out these operations. The organisation has established network and media handling controls to prevent unauthorised modifications to information or disruptions to business activities. Although most of Mine A's sensitive and critical information has dedicated printers, facsimiles and photocopiers, some of it is not closely monitored or protected as some users are not made aware of the need to protect this exchange of information. This puts the information that is exchanged through this media at risk of being accessed by unauthorised persons. Guidelines for the retention and disposal of business correspondence which includes messages complies with relevant legislation and regulations.

While procedures are in place to deal with malicious code, responsibilities and procedures do not specify what kind of training is required for users to cope with malicious code. Cryptographic controls which would be used to authenticate mobile code have also not been implemented in the organisation. Nonetheless, email attachments are scanned for malicious code before use. Malicious code detection and repair software provides protection against malicious software in the organisation and minimise the intensification of malicious code in the environment. Mine A has also established a formal policy that prohibits the use of unauthorised software. This makes it easier to control licensing issues and protect the environment from malicious code. New systems are tested to verify acceptance criteria before they are accepted.

As established in sections 10.3.2 and 10.3.3, as only some of the organisation's information has been classified, information may be incorrectly dissemination as controls may not be properly applied. Procedures to control the flow, content and exchange of emails have been established. Section 5.11 identified emails as a critical mode of communication in the mining

industry as well as other industries. Despite all the controls that Mine A has put in place to control electronic communication, restrictions with regards to the forwarding of electronic communications to external destinations have not been effected. Hence organisational information meant for internal use may be forwarded to external destinations. A policy, however, exists to that effect.

Strict change management procedures have been put in place to control changes to the information processing infrastructure. These changes are, however, not always tested before they are carried out. As a result, backout procedures may tend to be challenging in an operational environment. Nonetheless, changes made to documents and procedures are checked and approved by management, thereby, ensuring complete management support of the operational environment.

Access control procedures have been established in Mine A. However, an intrusion detection system has not been set up to monitor the activities of network administrators as they are as susceptible to tampering with systems as are outsiders. Policies and procedures to protect information and physical media in transit have not been completely established. As a result, they are not completely protected while in transit.

Although system backups are carried out in the organisation, they are not tested regularly. Hence the efficiency and effectiveness of restoration procedures for some systems is not checked and tested on a regular basis. As discussed in section 5.6.2, backups need to be regularly tested in order to ensure that they are reliable and useable. The BCPs that are in place do not address the need to recover all the necessary data and software. Mine A's BCP only caters for very critical applications and has not been recently updated. Neither is a complete record of procedures that could be used to restore information kept. This may prove to be a challenge when accounting for data and software that would need to be recovered and the methods by which these should be recovered. Regular reviews of the data and software that support critical applications are also not carried out. This puts the continued availability of critical applications at risk. Equipment maintenance procedures have been developed to protect the organisation's equipment from environmental threats.

Although organisational duties and responsibilities have been segregated to reduce chances of people accidentally or intentionally modifying or misusing assets, information handling and storage procedures do not ensure that information is completely protected from misuse. There

are still chances of employees accessing, using or modifying assets without detection. This does not completely hinder collusion. Third parties are mandated to comply with the organisation's policies and procedures to ensure uniformity in the organisation's compliance process.

High risk areas are reviewed more than low risk areas so that major risks are minimised as much as possible. Risk assessments are carried out on systems to ensure that logging for auditing purposes does not degrade the performance of these systems. This logging information is also protected from unauthorised changes but no one has been given the responsibility of auditing the activities of administrators from the logged information. Work activities are also supervised more closely whenever the security of these assets cannot be controlled through segregation of duties. However, the level of risk monitoring required for each system or facility is not always determined.

10.3.7 Domain 7: Information Access Control Management

This section discusses the control of access to business information, information processing facilities as well as business processes.

The Domain 7 questionnaire addresses control of access to information, applications, operating systems and networked services, management of user access rights, good access practices, and protection of mobile and teleworking facilities.

Of the 28 concerns identified in the literature review, 15 concerns were relevant to the Domain 7 questionnaire. Of these 15 concerns applicable to Domain 7, 8 concerns were considered to require addressing while 7 did not. The 8 concerns that require addressing include:

- *Lack of or inadequate security policies:* the organisation's access control policy has not been recently reviewed.
- *Poor staff awareness:* mobile computer security training programs to address risks are not provided.
- *Inadequate risk management process:* mobile security policy does not address risks associated with all mobile devices in use in the organisation.
- *Lack of formal mobile security governance:* information handled by mobile devices is not completely protected.

- *Inadequate access control procedures:* Formal processes to review user access rights have not been established. Network segregation decisions do not entirely comply with the access control policy and cryptographic control methods are not used to authenticate remote users.
- *Inadequate integration of information security into employment policies and practices:* Personnel contracts do not specify the sanctions that will be applied if personnel attempt to gain access to information without authorisation.
- *Human error:* Unattended fax machines expose the organisation's sensitive or critical information to unauthorised access.
- *Incorrect dissemination or disclosure of information:* The access control policy does not define how information dissemination and authorisation should be controlled. Clear desk and clear screen policies have also not been enforced.

According to Domain 7 questionnaire responses, 7 of the concerns identified in the literature review have already been addressed by Mine A. These include:

- *Lack of or inadequate security procedures:* access control procedures to control the registration and de-registration of users wanting to access information has been established.
- *Increased regulation:* access control policy complies with all relevant data access laws and regulations.
- *Environmental threats to hardware:* information and information processing facilities are prevented from exposure to possible loss or damage.
- *Inadequate email policies:* unprotected mail messages are not used to send passwords and network connection restrictions have been applied to the organisation's email applications.
- *Ill-defined user access privileges:* authorised access to information systems and allocation and use of system privileges is controlled and restricted. Unique identifiers are given to each user or group of users and password complexity is enforced.
- *Unsecure application software:* network control restrictions are used to control access to the organisation's applications. Log on procedures only give the bare minimum of information about a system.
- *Lack of formal information security governance frameworks:* access control rules and procedures are authorised by management.

The Domain 7 questionnaire results outlined above indicate that 25% of the concerns that were identified in the literature review have already been addressed while 29% still need addressing. This is illustrated in figure 10.42 below.

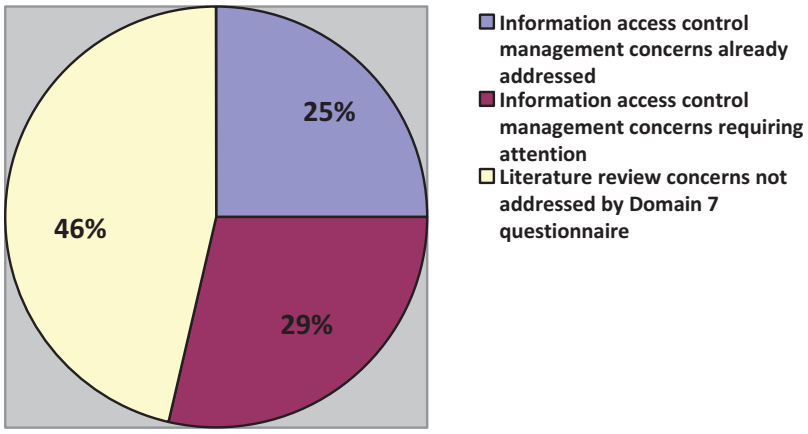

Figure 10.42: Information Access Control Concerns as Outlined in the Literature Review

Figure 10.43 below gives a summary of Domain 7 questionnaire responses from the 7 questionnaire subsections. The subsections included in this questionnaire are "control access to information", "manage user access rights", "encourage good access practices", "control access to networked services", "control access to operating systems", "control access to applications and information", and "protect mobile and teleworking facilities".

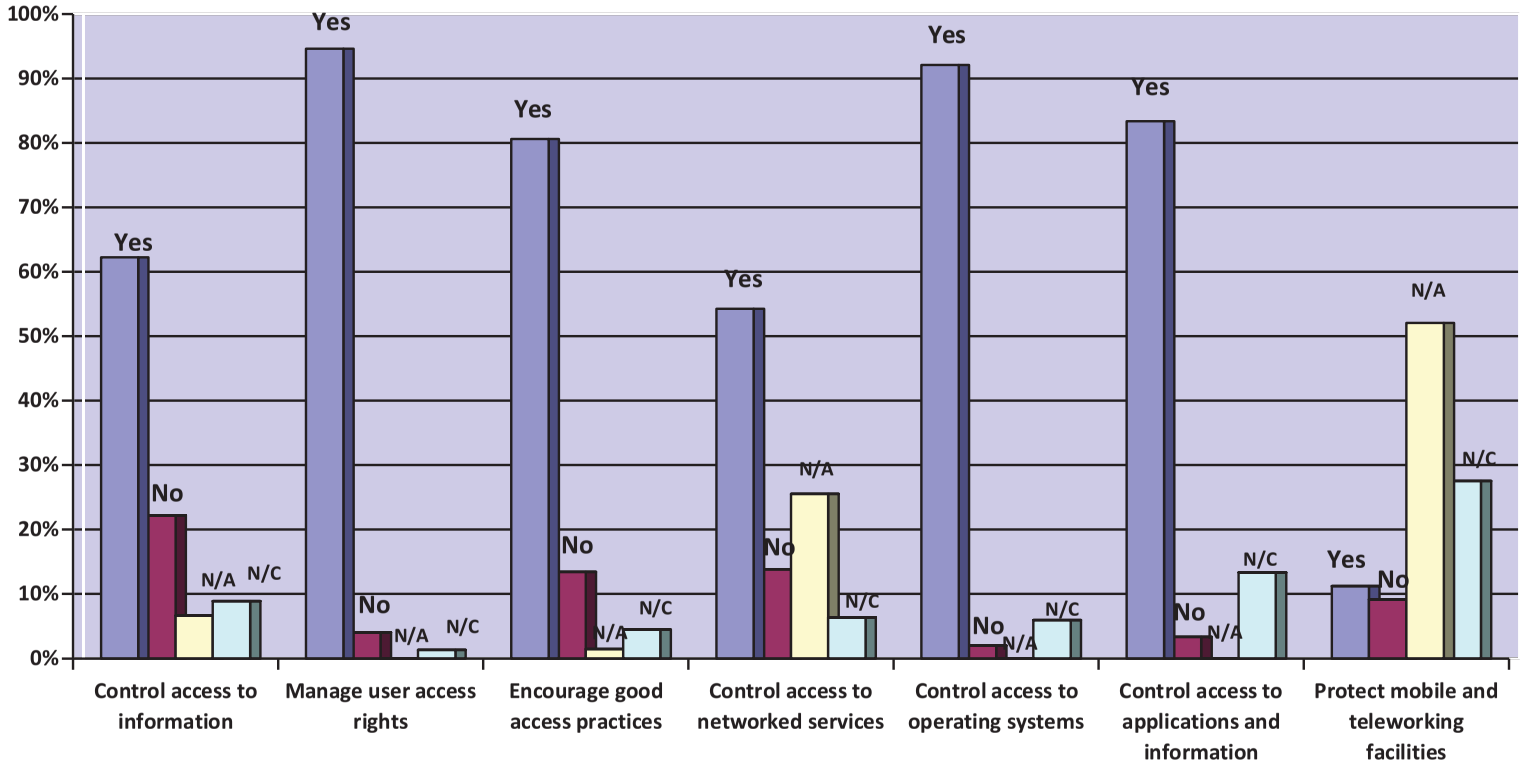

Figure 10.43: Domain 7 Questionnaire Responses

Discussion

Mine A recognises the importance of information in the organisation and has put measures in place to control access to it. From the questionnaire responses illustrated in figure 10.43, user access rights are highly managed as is access to operating systems. An organisation-wide access control policy has been established in the organisation, although it only caters for physical access and not logical access control. Nevertheless, a more specific access control policy meant to control access to information processing facilities caters for both physical and logical access. This policy has, however, not been recently updated despite several access control changes taking place since the last update. Furthermore, the organisation's IT security policy addresses both physical and logical access control at a high level. All policies mentioned above comply with the relevant data access laws and regulations. None of the policies that cater for access control define how information dissemination and authorisation should be controlled. These access control policies and procedures, however, address the control of access to information from registration to de-registration of users in addition to providing support for the management of access rights in a distributed and networked environment.

A centralised mobile security policy has not been established in Mine A. Nevertheless, laptop and removable media policies are in place. These policies have also not been recently reviewed and additional mobile devices that are now in use in the organisation have not been catered for. These policies, therefore, do not address all the risks that are associated with all mobile devices in the organisation. Mobile security training is equally not conducted in order for mobile users to fully understand the risks that come with the use of these mobile facilities. Needless to say, as it is not easy to completely protect mobile devices while they are out of the organisation's premises, use of these devices may not be completely protected from both physical and logical threats. In the same way, as discussed in section 10.3.6, devices such as fax machines and printers are not completely protected during the time that they are unattended making the information that is exchanged through them susceptible to unauthorised access. Mine A does not conduct teleworking as facilities for teleworking are currently not in place. Hence the high number of "N/A" responses in the "protect mobile and teleworking facilities" section in figure 10.43 above.

The relationship between access control rules and information classification has not been clearly defined making the effective implementation of access control difficult. Network control restrictions are used in Mine A to control access to the organisation's applications such as email and file transfer applications. Network segregation decisions, however, do not entirely comply with the access control policy as they have not been addressed in this policy. Cryptographic controls are not used to authenticate remote users or mobile code such as viruses, worms, and Trojan horses. These would help ensure the confidentiality and integrity of information in Mine A. Unprotected mail messages are not used to send passwords. Users are given a generic password which they are prompted to change immediately into a unique password that complies with complexity requirements. Mine A's personnel contracts do not specify the sanctions that would be applied if personnel attempt to gain access to information without authorisation. This is, however, catered for in the agreements that they sign on commencement of employment in addition to the policies and procedures that they have to abide by. Sanctions concerning unauthorised dissemination and disclosure of the organisation's information are specified in these contracts.

Clear screen and clear desk policies have not been enforced although the clean desk policy has been addressed in Mine A's IT security policy. As outlined in section 2.4, the mining industry uses a lot of information systems for planning and operations. These systems should, therefore, provide the right output if full benefits are to be realised. Mine A controls and restricts system privileges and access to these information systems. This minimises human error and misuse of information systems in the organisation. Application owners are also made aware of the risks associated with sharing application system resources so that they fully understand the implications that come with the shared usage of these resources. Unique identifiers (IDs) are given to each user or to a group of users when business need arises. This enhances user accountability. The organisation's log-on procedure only gives the bare minimum of information about a system and standardised profiles are given to users to ensure that users do not have unnecessary privileges availed to them. However, a formal procedure to review user access rights is not in place. This makes the reviews take place in an ad-hoc manner and may hinder effective control of user privileges.

Information and information processing facilities have been protected from possible loss and damage through the use of safes, fire and water resistant facilities.

10.3.8 Domain 8: Information Systems Security Management

This section discusses the security requirements of information systems in an organisation. These information systems include operating systems, off-the-shelf applications, user developed and business applications as well as the information systems infrastructure.

The Domain 8 questionnaire addresses the identification of information systems security requirements, correct processing of information by applications, use of cryptographic controls, protection of system files, control of development and support processes, and the establishment of technical vulnerability management.

Of the 28 concerns identified in the literature review, 17 concerns were relevant to the Domain 8 questionnaire. Of these 17 concerns applicable to Domain 8, 9 concerns were considered to require addressing while 8 were not. The 9 concerns that require addressing include:

- *Email threats such as viruses and spam:* protection of information leakage through exploitation of covert channels is incomplete.
- *Poor asset identification and inventory:* a complete and up-to-date inventory of information assets to support the technical vulnerability process has not been established.
- *Irregular or no patching of systems:* patches are not tested before installation to ensure that they are effective and do not cause intolerable side effects.
- *Inadequate email policies:* cryptographic controls to protect the confidentiality, integrity and confidentiality of information are not used. Some controls to protect message integrity and authenticity have not been implemented.
- *Informal change management procedures:* change control procedures do not ensure that operating documentation is promptly updated to reflect system changes.
- *Unsecure application software:* patches, service packs and other updates are not tested in an environment separate from development and production activities.
- *Informal Business Continuity Plans:* BCPs are not updated whenever changes are made to operating systems.
- *Ill-maintained legacy systems:* some information needed to support old versions of the organisation's software is not archived.

- *Incorrect dissemination or disclosure of information:* hidden information in outbound media and communications is not scanned for information leakage.

According to Domain 8 questionnaire responses, 8 of the concerns identified in the literature review have already been addressed by Mine A. These include:

- *Lack of or inadequate security procedures:* procedures to control the installation of software on the organisation's operational systems are in place.
- *Inadequate risk management process:* risk assessments are used to identify security requirements and select security controls for systems. The vulnerability management process specifies that a risk assessment must be carried out whenever a potentially relevant vulnerability is expected.
- *Dispersed data and information:* old versions of software are archived.
- *Inadequate access control procedures:* the same access control procedures in operational application systems apply to test application systems. Access to program source code is restricted.
- *Lack of formal information security governance frameworks:* business requirements that information systems changes or enhancements must be able to meet are identified.
- *Poor incident response plans:* incident response procedures are used to manage and control the actions that should be taken to address technical vulnerabilities.
- *Ill-defined user access privileges:* change control procedures ensure that only authorised users are allowed to submit changes.
- *Human error:* validation checks are incorporated into applications.

The Domain 8 questionnaire results outlined above indicate that 29% of the concerns that were identified in the literature review have already been addressed while 32% still need addressing. This is illustrated in figure 10.44 below.

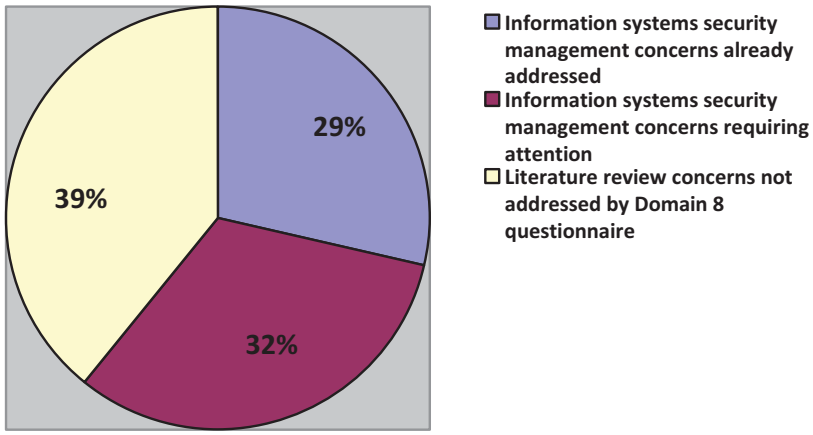

Figure 10.44: Information Systems Security Management Concerns as Identified in the Literature Review

Figure 10.45 below gives a summary of Domain 8 questionnaire responses from the 6 questionnaire subsections. The subsections included in this questionnaire are "identify information system security requirements", "make sure applications process information correctly", "use cryptographic controls to protect information", "protect your organisation's system files", "control development and support processes", and "establish technical vulnerability management".

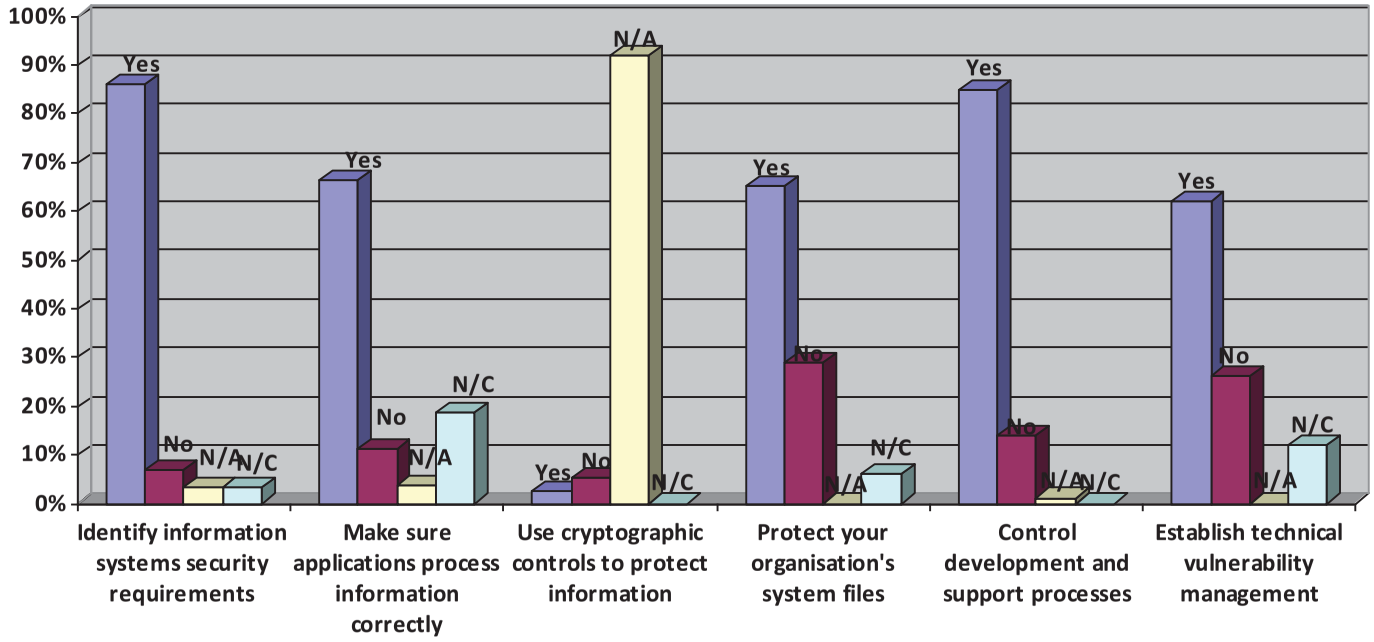

Figure 10.45: Domain 8 Questionnaire Responses

Discussion

As illustrated in figure 10.45 above, Mine A has identified the need for information systems security and it's requirements and has put in place several measures to manage this. There were a high number of N/A responses under the "use cryptographic controls to protect information" section as the organisation has not implemented these controls. Thus, the confidentiality, integrity and authenticity of information may not be fully guaranteed.

Mine A mainly uses off-the-shelf software packages as it does not currently have a software development team in place. Business requirements that new information systems or enhancements to current information systems must meet are identified before procurement. This ensures that investment in these systems adds value to the business. Procedures are in place to control the installation of software on the organisation's operational systems. This, as discussed in section 10.3.6, helps control licensing management, malicious code and intellectual property rights. Validation checks are integrated into most of these systems to ensure that the right data is input and the right information is output.

A test environment for updates and new packages for operating and application systems has not been established in Mine A, although new software is always tested before use. This, according to the Domain 8 questionnaire, increases the risk of "*the cure being worse than the disease*" when these updates are applied.

Although formal change management procedures have been established in Mine A, they do not ensure that documentation is immediately updated whenever a change is made to information systems. As discussed in section 10.3.6, this affects incident response management. These procedures, however, ensure that only authorised users are allowed to submit changes and approval for this change is provided by management. Change management procedures are not fully integrated with BCPs such that changes to operating systems are immediately updated. Hence, the BCPs will not always be up-to-date.

As the inventory of information assets in Mine A is not complete and up-to-date, the technical vulnerability process is not fully supported as the level of vulnerability of unidentified assets will not be sufficiently addressed. In as much as old versions of Mine A's software are archived, some of the information that is needed to support old versions of the organisation's software is not archived. Future maintenance of this software may be affected

resulting in cultural clashes between older and newer staff concerning the support of these systems. These clashes were identified in section 4.7 as one of the concerns that apply not only to the mining industry's legacy systems but their control systems as well.

Information leakage through covert channels is not completely protected. Some of these channels include hidden information in outbound media and communications which are not scanned for information leakage. As a result, information such as email addresses or intranet links that the organisation does not want revealed may be accidentally revealed.

Risk assessments are conducted to identify security requirements and select security controls for operating and application systems. In addition to this, the vulnerability management process also expects a risk assessment to be carried out whenever a potentially relevant vulnerability is expected. As discussed in section 4.4, risk assessments are important as they provide a framework for the establishment of policies and identification of controls and policies that will be used to protect the organisation's assets. Hence, as outlined earlier, Mine A's asset inventory needs to be complete and up-to-date for the vulnerability management process to be effective.

10.3.9 Domain 9: Information Security Incident Management

This section discusses the management of information security incidents in an organisation.

Domain 9 questionnaire addresses the reporting of information security events and weaknesses as well as the management of information security incidents and improvements.

Of the 28 concerns identified in the literature review, 13 concerns were relevant to the Domain 9 questionnaire. Of these 13 concerns applicable to Domain 9, 4 concerns require addressing while 9 do not. The 4 concerns that require addressing include:

- *Lack of or inadequate security policies:* information security incidents are not used to improve the organisation's information security policy.
- *Increased regulation:* a published standard or code of practice has not been identified for use in helping to prove that evidence produced by them is admissible in a court of law.
- *Email threats such as viruses and spam:* formal procedures to handle malicious code have not been developed.

- *Poor incident response plans:* anonymous information security incidents are not used to make users aware of information security incidents and what they can do to avoid and respond to similar incidents.

According to Domain 9 questionnaire responses, 9 of the concerns identified in the literature review have already been addressed by Mine A. These include:

- *Lack of or inadequate security procedures:* security event reporting and escalation procedures have been established.
- *Poor staff awareness:* employees are aware of their responsibility to promptly report all information security events.
- *Inadequate access control procedures:* only authorised personnel are allowed to access live systems and data.
- *Ill-defined crisis communication procedures:* recovery procedures expect people to report emergency responses to management.
- *Lack of formal information security governance frameworks:* information security events are reported using the appropriate management channels.
- *Unsecure application software:* incident reporting and response procedures handle software malfunctions.
- *Human error:* incident reporting procedures handle human error.
- *Incorrect dissemination or disclosure of information:* a strong evidence trail is established by ensuring that original media is untouched and securely stored.
- *Environmental threats to hardware:* incident reporting and response procedures handle loss of equipment incidents.

The Domain 9 questionnaire results outlined above indicate that 32% of the concerns that were identified in the literature review have already been addressed while 14% still need addressing. This is illustrated in figure 10.46 below.

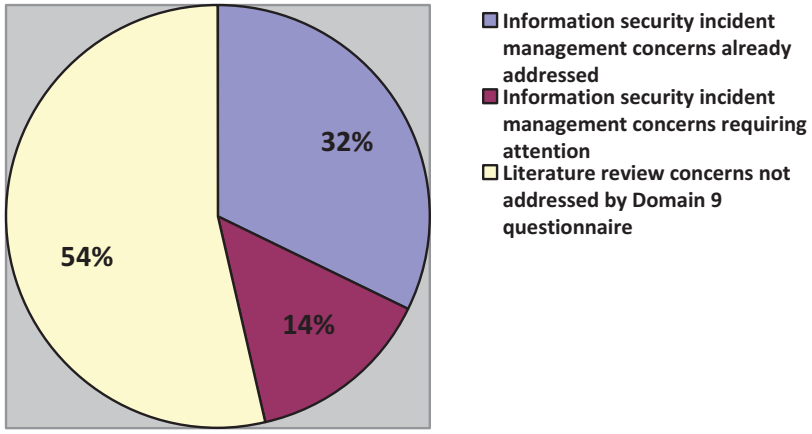

Figure 10.46: Information Security Incident Management Concerns as identified in the Literature Review

Figure 10.47 below gives a summary of Domain 9 questionnaire responses from the 2 questionnaire subsections. The subsections included in this questionnaire are "report information security events and weaknesses" and "manage information security incidents and improvements".

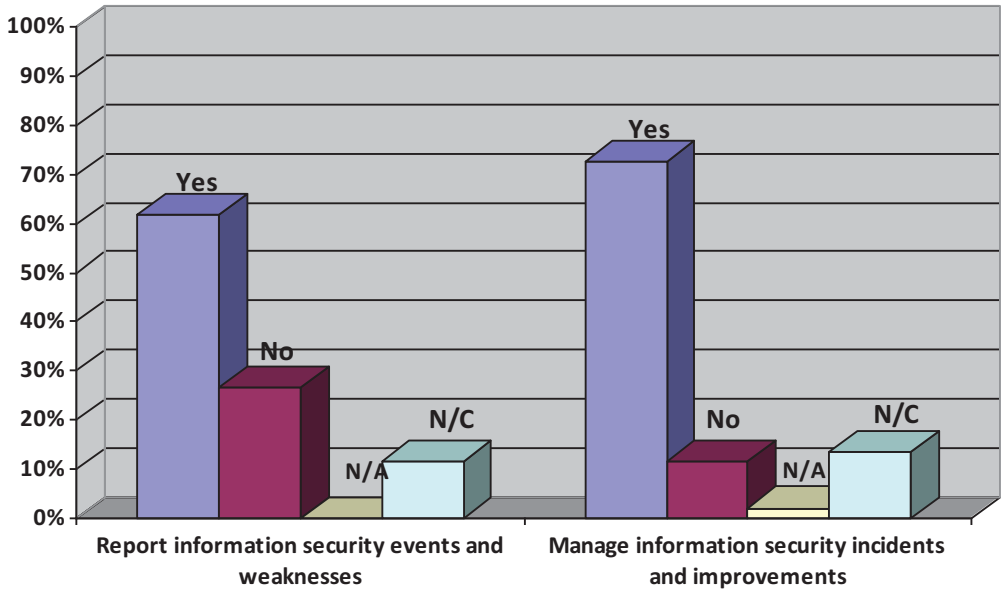

Figure 10.47: Domain 9 Questionnaire Responses

Discussion

As illustrated in figure 10.47, Mine A has established an incident management process. A high number of "no" responses under the "report information security events and weaknesses" section indicates a gap in the incident reporting process. A high number of "yes" responses under the "manage information security incidents and improvements" section, however, indicates that most incidents that are reported are managed and improved upon.

Mine A has developed incident management and incident reporting policies to address its incident management process. Section 5.4.1.6 indicates that post incident activity may involve updating information security policies, procedures and guidelines to address future incidents of the same kind. Although Mine A has made reference to its information security policy in the incident management policy, information security incidents are not used to improve the organisation's information security policy.

Formal incident reporting procedures have been developed and personnel have been made aware of the need to promptly report all information security events. These events are reported using appropriate management channels. In addition, emergency responses are equally expected to be reported to management. Only authorised personnel are allowed to handle live systems and data during the recovery process to prevent unauthorised access when the systems are vulnerable. Incident reporting procedures handle a number of events including software malfunctions, equipment incidents and human error. However, formal procedures to handle malicious code have not been developed.

Evidence about an information security incident is collected whenever it is required to support administrative or legal proceedings. The organisation has, however, not identified a standard or code of practice to help in proving that evidence produced by information systems is admissible in a court of law. This is needed to strengthen the integrity of the evidence that is being produced. Mine A establishes a strong evidence trail by ensuring that original media is untouched and securely stored as forensic evidence.

Anonymous information security incidents are not used as part of the awareness program to make users aware of how they should respond to incidents and what they can do to avoid or

respond to similar incidents. This is so that personnel are not caught unaware when certain incidents occur. However, fire drills are conducted as part of the incident awareness program.

10.3.10 Domain 10: Business Continuity Management

This section discusses the counteraction of interruptions to business processes in an organisation and the protection of critical business processes from the effects of failures. It also discusses the resumption of business activities and processes in a timely manner.

The Domain 10 questionnaire addresses the use of continuity management to protect information in an organisation through the establishment of a business continuity process as well as the development and implementation of business continuity plans.

Of the 28 concerns identified in the literature review, 13 concerns were relevant to the Domain 10 questionnaire. Of these 13 concerns applicable to Domain 10, 4 concerns require addressing while 9 do not. The 4 concerns that require addressing include:

- *Poor staff awareness:* complete rehearsals are not carried out to ensure that all personnel can cope with business interruptions.
- *IT-based Business Continuity Plans:* a single business continuity framework or centralised BCPs do not exist.
- *Poor asset identification and inventory:* some assets have not been identified for the business continuity process.
- *Lack of or irregular testing of contingency plans:* some BCPs are not regularly tested.

According to Domain 10 questionnaire responses, 9 of the concerns identified in the literature review have already been addressed by Mine A. These include:

- *Lack of or inadequate security procedures:* BCPs describe fallback procedures that should be followed to move essential business processes and activities to alternate locations.
- *Inadequate risk management process:* controls to help identify risks have been established.
- *Informal change management procedures:* change management procedures ensure that business continuity matters are always addressed.
- *Informal BCPs:* a formal BCP has been developed and implemented.

- *Ill-defined crisis communication procedures:* crisis management and business continuity procedures have been distinguished.
- *Lack of formal information security governance frameworks:* senior management endorses the organisation's BCP and strategy.
- *Poor incident response plans:* controls to limit the damage that serious incidents could cause have been established.
- *Human error:* The impact that human error could have on the organisation's processes and information has been evaluated.
- *Environmental threats to hardware:* the impact that equipment failures could have on processes and the security of information has been evaluated.

The Domain 10 questionnaire results outlined above indicate that 32% of the concerns that were identified in the literature review have already been addressed while 14% still need addressing. This is illustrated in figure 10.48 below.

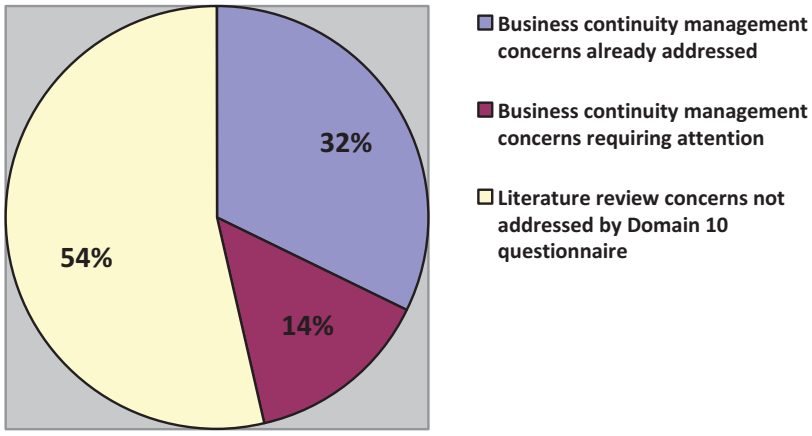

Figure 10.48: Business Continuity Management Concerns as identified in the Literature Review

Figure 10.49 below gives a summary of Domain 10 questionnaire responses. Domain 10 questionnaire addressed using continuity management to protect organisational information.

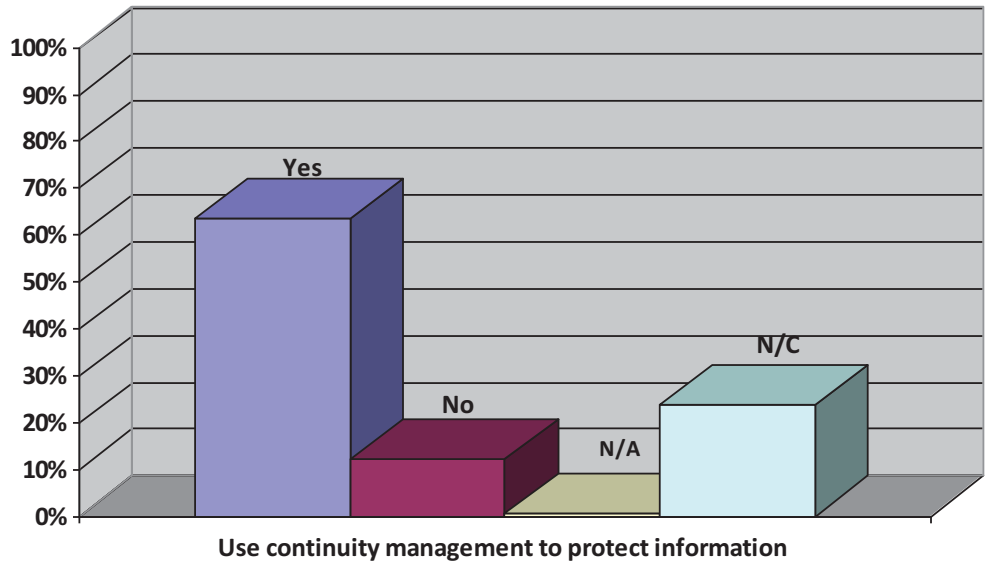

Figure 10.49: Domain 10 Questionnaire Responses

Discussion

A high number of "yes" responses in figure 10.49 indicates that a continuity management process to protect Mine A's information is in place. A slightly high number of N/C responses indicates that although a continuity management process is in place, certain processes have not been completely effected.

Mine A has developed and implemented BCPs which are endorsed by management. There is no single framework that the organisation uses to develop its BCPs and ensure their uniformity. A BCP to address information systems and information processing facilities has been developed and implemented in the organisation. This BCP describes fallback procedures that should be taken to move information processing facilities to an alternate location. Despite this implementation, the BCP is not regularly updated to cater for organisational changes. Although a strict change management process is in place, it does not ensure that the BCP is updated whenever changes are made. As discovered in section 10.3.3, Mine A does not have a complete asset inventory which may affect the effectiveness of the business continuity management process as not all assets will be incorporated into the continuity process.

Complete rehearsals are not carried out for all continuity processes to determine whether personnel can cope with a real situation. Personnel may, therefore, discover that they are not

adequately prepared for the real situation when it occurs. The impact that human error could have on the organisation's processes and information have been evaluated so that they are catered for in the continuity process. The impact that equipment failures could have on processes and the security of information has been evaluated and controls have been put in place to address threats to equipment.

Crisis management and business continuity procedures have been distinguished so that appropriate resources are made available for a particular situation as crises situations are usually confused with disasters.

Controls to minimise the impact that incidents can cause have been established so that these incidents do not turn into disasters. In addition, controls to help identify risks have also been established so that information security risks in Mine A can be minimised.

10.3.11 Domain 11: Compliance Management

This section discusses an organisation's compliance with statutory, regulatory and contractual obligations and requirements.

Domain 11 questionnaire discusses compliance with legal requirements, review of security compliance and information system audits.

Of the 28 concerns identified in the literature review, 10 concerns were relevant to the Domain 11 questionnaire. Of these 10 concerns applicable to Domain 11, 4 concerns require addressing while 6 do not. The 4 concerns that require addressing include:

- *Lack of or inadequate security policies:* an intellectual property rights compliance policy has not been published.
- *Poor staff awareness:* personnel are not made aware of policies that are designed to protect intellectual property rights.
- *Lack of formal information security governance frameworks:* procedures to ensure that the organisation complies with intellectual property rights and requirements have not been established.
- *Inadequate access control procedures:* users do not receive written authorisation before they are granted access to information processing facilities.

According to Domain 10 questionnaire responses, 6 of the concerns identified in the literature review have already been addressed by Mine A. These include:

- *Lack of or inadequate security procedures:* security procedures comply with the organisation's security policies.
- *Increased regulation:* the organisation complies with all relevant legislation that governs the collection, processing, transmission, and dissemination of information. Information systems also comply with relevant regulatory, statutory, and contractual security requirements.
- *Dispersed data and information:* the organisation's important records are protected from falsification, loss and destruction.
- *Poor asset identification and inventory:* a register of the organisation's proprietary software and information assets is maintained.
- *Unsecure application software:* information systems are procured from reputable suppliers and audited for appropriate use.
- *Incorrect dissemination or disclosure of information:* organisational records have been identified and categorised so that they are appropriately managed.

The Domain 11 questionnaire results outlined above indicate that 21% of the concerns that were identified in the literature review have already been addressed while 14% still need addressing. This is illustrated in figure 10.50 below.

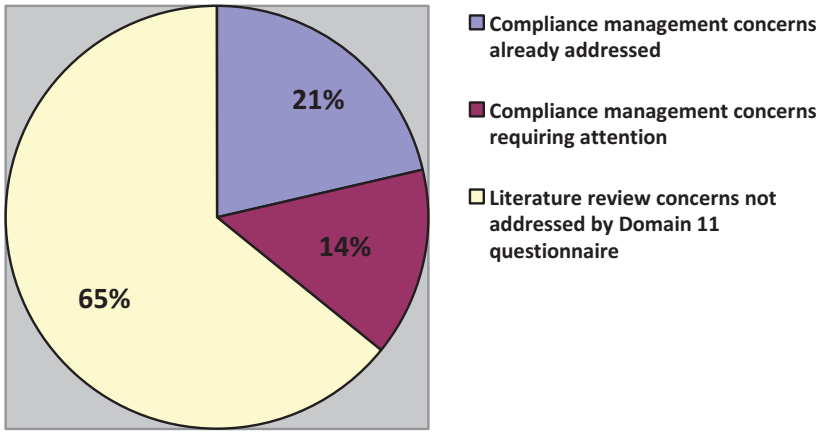

Figure 10.50: Compliance Management Concerns as identified in the Literature Review

Figure 10.51 below gives a summary of Domain 11 questionnaire responses from the 3 questionnaire subsections. The subsections included in this questionnaire are "comply with legal requirements", "perform security compliance reviews", and "carry out information system audits".

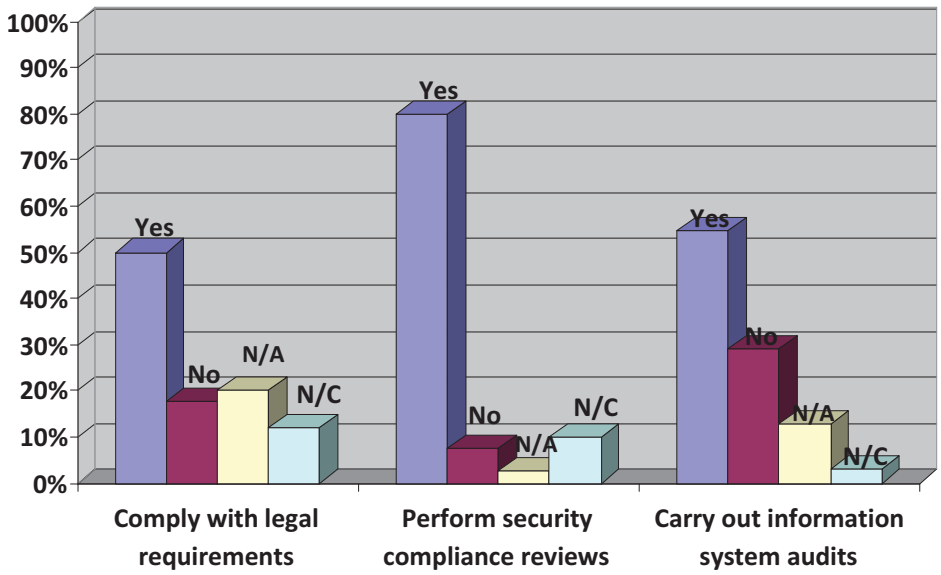

Figure 10.51: Domain 11 Questionnaire Responses

Discussion

A high number of "yes" responses in figure 10.51 indicates that Mine A conducts information security compliance reviews to ensure that the organisation complies with all relevant statutory, regulatory and contractual requirements.

The organisation's method of collection, transmission, processing and dissemination of information complies with all relevant legislation. Compliance security procedures implemented in Mine A comply with Mine A's security policies. This puts these procedures in line with the overall policies of the organisation. In the case of IPR, however, employees are not made aware of the policies that are designed to protect these rights, neither has an IPR compliance policy been published. As a member of WIPO and ARIPO, all Zambian organisations and individuals are liable to compliance with IPR. This membership was discussed in section 6.6.

Although personnel have to sign confidentiality and non-disclosure agreements when applying for access to information processing facilities, they do not always receive written

authorisation before they can access them. This is due to the magnitude of users in the organisation.

Until recently when Zambia enacted an ICT policy, Information and Communications Technology Act, and the Electronic Communications and Transactions Act, statutory and regulatory ICT requirements have not been highly enforced in the country. This has in the past affected the effective execution of legal action.

Mine A procures its information systems from reputable suppliers and conducts regular audits of these systems. These audits are conducted by both internal and external auditors. audit tools have, however, not been adequately identified for appropriate protection from misuse. The organisation ensures that its information systems comply with relevant regulatory, statutory, and contractual security requirements. Organisational records are identified and categorised to enhance their management and control unauthorised access and dissemination. Mine A maintains a register of proprietary software and information assets so as to ensure that their management is centralised and old versions are maintained for compatibility and contingency purposes. Important organisational records are protected from falsification, loss, and destruction. This is to ensure that they are in the appropriate locations and are adequately protected. Mine A's management has put in place disciplinary and when necessary, legal measures for cases where personnel make unauthorised use of information processing facilities.

10.3.12 Summary of Domain Questionnaire Findings

Table 10.30 below presents a summary of the frequency of concerns that were identified as being applicable to each of the 11 domains that were represented in the ISO/IEC 27002 audit tool.

Table 10.30: Summary of Domain Questionnaire Findings

Domain	Information Security Concern	Requires Addressing	Already Addressed
Security Policy	Lack of or inadequate security policies	6	1
Organising Information	Lack of or inadequate security procedures	3	6
	Lack of formal information security governance frameworks	2	9
	Dispersed data and information	3	2
	Incorrect dissemination or disclosure of information	4	6
Asset Management	Poor asset identification and inventory	4	3
Human Resources Security	Inadequate integration of information security into employment policies and practices	2	1
	Poor staff awareness	8	1
Physical and Environmental Security	Environmental threats to hardware	1	5
Communications and Operations Management	Informal change management procedures	2	1
	Inadequate email policies	3	1
	Email threats such as viruses and spam	2	1
Access Control	Inadequate access control procedures	4	4
	Lack of formal mobile security governance	4	1
	Ill-defined user access privileges	0	4
Information Systems Acquisition, Development, and Maintenance	Inadequate control system policies and procedures	0	0
	Unsecure application software	2	3
	Cultural clashes between IT staff	0	0
	Irregular or no patching of systems	1	1
	Ill-maintained legacy systems	1	0
Incident Management	Poor incident response plans	3	3
	Human error	3	4
Business Continuity Management	Informal BCPs	3	2
	Lack of or irregular testing of contingency plans	2	2
	Ill-defined crisis communication procedures	0	2
	IT-based Business Continuity Plans	3	0
	Inadequate risk management process	3	6
Compliance	Increased regulation	2	7

Figure 10.52 below provides a graphical representation of questionnaire findings based on the 11 domains of the ISO/IEC 27002 standard.

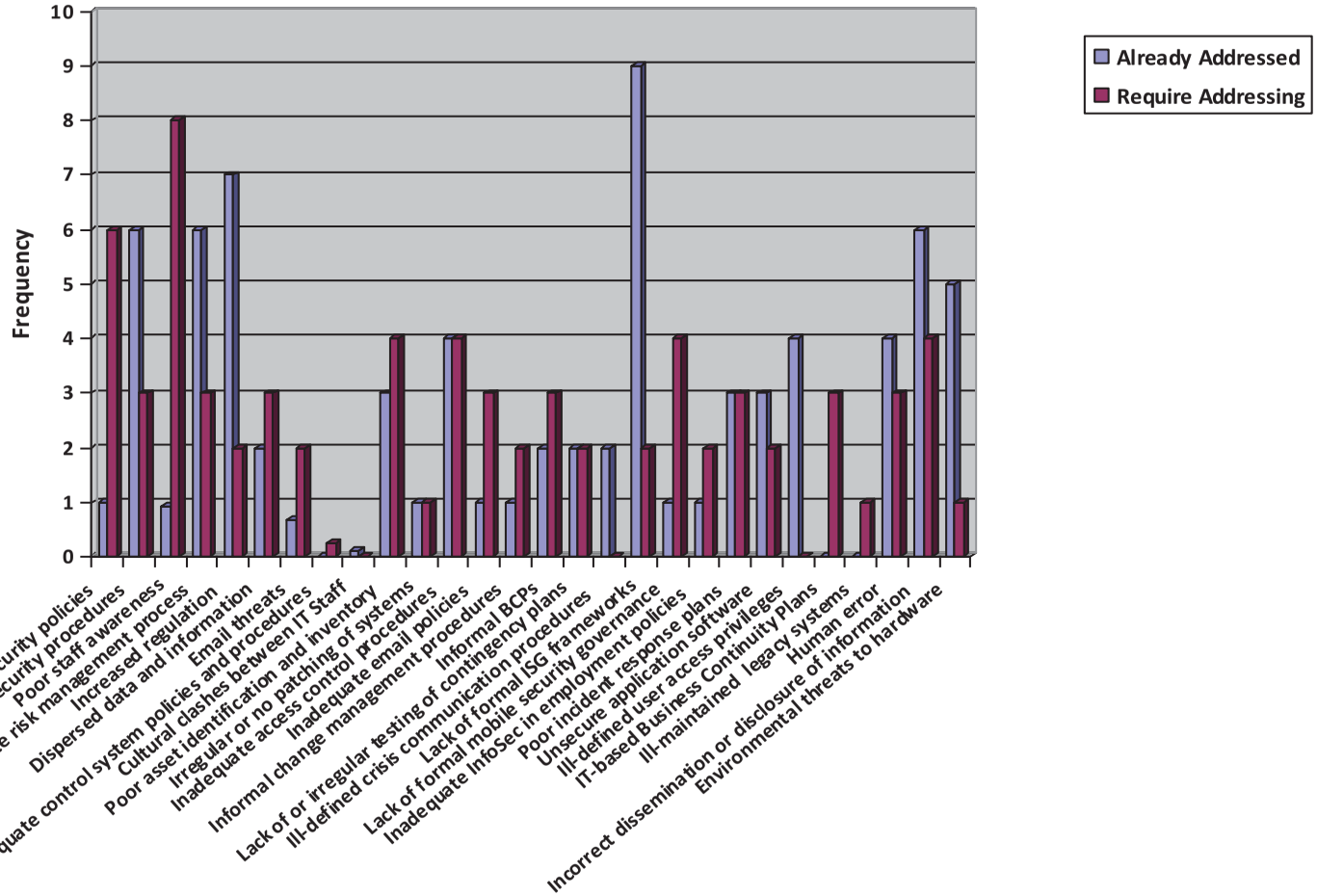

Figure 10.52: Summary of Information Security Concerns from Domain Questionnaire Findings

From the ISO/IEC 27002 audit tool questionnaire findings representing the 11 ISO/IEC 27002 information security domains, sufficient evidence suggests that the "lack of formal information security governance frameworks" concern is the concern that would seem to have been most adequately addressed by Mine A. Likewise, the "poor staff awareness" concern is the concern that would seem to have been least adequately addressed by Mine A. The "inadequate information system control procedures" concern was not explicitly represented in the audit tool but the "unsecure application software" concern findings were somewhat applicable to this concern which is very specific to the copper mining industry. In addition, the "cultural clashes between IT staff" concern was not explicitly represented but alluded to in the ISO/IEC 27002 audit tool. These concerns were distinctly addressed in the set of questionnaires that explored leadership perceptions concerning information security practices in Zambian copper mines.

10.4 Overall Summary of Findings

Findings from the Leadership Perception Questionnaires and the ISO/IEC 27002 audit tool reveal that senior management do indeed have a different perception of information security from that of middle management. Whilst perceptions between the two levels of management may differ, it was revealed that poor staff awareness was a common aspect that was deemed to be a barrier to effective implementation of information security in these organisations.

10.5 Conclusion

Following the administration of the ISO/IEC 27002 audit tool in Mine A and the leadership perception questionnaires in different copper mining organisations in Zambia, there is sufficient evidence to suggest that these organisations have similar information practices in place, thereby, making the proposed framework for information security practices in Zambian copper mines be deemed relevant. Furthermore, according to the practices that have been recommended in the ISO/IEC 27002 standard this evidence also suggests that gaps exist in these information security practices. Further analysis and recommendations for the gaps that have been identified will be discussed in chapter 11.

Chapter 11

Recommendations

Chapter 10 presented and analysed findings from the two sets of questionnaires administered in four copper mining organisations in Zambia. Based on the results and responses obtained from these questionnaires, this chapter discusses recommendations that would support the creation of optimal information security practices in Zambian copper mining organisations.

11.1 Introduction

Recommendations will be made based on the ISO/IEC 27002 standard on which the Leadership Perception and ISO/IEC 27002 Audit Tool questionnaires were based. These recommendations will be presented domain by domain based on the 11 information security domains of the ISO/IEC 27002 standard. Furthermore, these recommendations have been derived from the information security gaps identified from questionnaire responses received from both senior and middle management in the Zambian copper mining organisations.

11.2 ISO/IEC 27002 Information Security Domains

11.2.1 Security Policy

As indicated in the results, Zambian copper mines are currently aware of the importance of information as a tool for competitive advantage and stakeholder confidence. Hence, most of them have since established information security policies in their organisations. Most of these organisations seem to address the implementation of information security policies reasonably adequately and certainly management is committed to information security and information security policies, and these policies are availed to personnel. It is, however, interesting to note that in the Leadership Perception Questionnaire, senior management believe information security policies in their organisations adequately address information security requirements, business and organisational requirements and that they also cater for changing business needs. Middle management, on the other hand, as revealed in the ISO/IEC 27002 Audit Tool Domain 1 Questionnaire felt that the information security policy was in need of attention. Information security policies provide support for information security governance and serve as a backbone for information security programs in an organisation. It is, therefore, recommended that the following two (2) issues receive appropriate consideration:

- Regular reviews of information security policies at planned intervals or when a significant information security change is made in the organisation. This is in order to ensure that these policies continue to reflect the organisation's current business and information security requirements. Users should be notified of subsequent updates to information security policies and procedures.

- Inclusion of such statements in the organisation's information security policy as:
    - References to more specific policies and procedures which provide support to the main security policy and which are adequately detailed to outline all the necessary requirements that users should comply with. Emphasis should be placed on such policies as:
        - *Acceptable use of electronic communications policy*: This caters for electronic mail controls as they are now an important means of communication in the mining industry. This policy would also emphasise internet usage controls particularly with the increased usage of social networking sites.
        - *Removable media or mobile device or usage policy*: An increase in the usage of mobile devices in this industry warrants emphasis on this policy to govern this usage.
        - *Information system usage policy*: this would define user responsibilities towards information systems as well as the consequences of violating this policy.
        - *Information security incident reporting policy*: this places emphasis on user responsibilities towards incident reporting.
    - A framework that defines the organisation's controls and control objectives. This should include risk management and risk assessment structures.
    - Definition of personnel responsibilities towards reporting of information security incidents.
    - A brief description of information security policies, standards, principles and regulatory requirements that are considered to be important to the organisation. This should include the organisation's legislative, contractual, and regulatory

compliance requirements, especially since Zambia has recently started enhancing its ICT regulations. These will be discussed further in section 11.2.11.

- User education, awareness, and training requirements for all information security policies and procedures coupled with their responsibilities towards information security requirements addressed by these policies and procedures.

11.2.2 Organising Information Security

As indicated in the results, Zambian copper mines are currently aware of the importance of managing information security both within and outside their organisations. Hence, they have since implemented measures to achieve this. They seem to address the disclosure and dissemination of information reasonably adequately and certainly information security governance frameworks have been established. It is interesting to note that in both the Leadership Perception Questionnaire and the ISO/IEC 27002 Audit Tool Domain 2 Questionnaire, both senior management and middle management believe some organisational data has not been consolidated. Not all data and information in the organisation can, therefore, be accounted for. Implementation of information security measures both within and outside the organisation helps protect the organisation's information and information processing facilities. It is, therefore, recommended that the following five (5) issues receive appropriate consideration:

- Assignment of overall responsibility for the management of information security to a management group or forum.
- Clear identification, definition, and allocation of responsibility for each information asset. This includes definition of responsibilities for specific information security processes such as business continuity. Allocation of responsibilities should be done according to the information security policy and further documented.
- Establishment of procedures to specify when and who should be contacted in case of an incident or where it is suspected that laws may have been broken. These contacts include law enforcement authorities and emergency response services.

- Identification of the need for both internal and external specialist advice for information security and specialists, thereof. Management should be responsible for further review and coordination of the results of this advice.
- Regular review of the organisation's confidentiality agreements so that they continue meeting the organisation's needs and requirements. These requirements should include the identification and specification of the expected duration of the agreements even in cases where individuals are expected to maintain confidentiality for an indefinite period.

11.2.3 Asset Management

As indicated in the results, Zambian copper mines are currently aware of the importance of managing information assets in their organisations. Hence, they have since established measures for the management of these assets. As revealed in the Leadership Perception Questionnaire and the ISO/IEC 27002 Audit Tool Domain 3 questionnaire, both senior and middle management believe asset management still requires attention. Management of assets in an organisation ensures that information assets in the organisation are appropriately protected. It is, therefore, recommended that the following five (5) issues should receive appropriate consideration:

- Identification and inventorying of all information assets. This inventory should be regularly updated and should include among other things:
    - Business Continuity Plans (BCPs).
    - Contracts and agreements, archived and research information.
    - Training materials and user manuals.
    - Audit trails.
- Enhancement of disaster recovery procedures through the inclusion of adequate information in the asset inventory. This information should include the asset type, format, location, backup information, and the value the organisation places on the asset.
- Adoption of a formal information classification scheme in the organisation. Each information asset should be classified depending on its level of importance in the

organisation. Information handling and labeling procedures should be developed and implemented based on the classification scheme that the organisation adopts.

- Assignment of ownership to each asset in the organisation. Each asset owner should be responsible for the classification and control of access to the asset.

- Personnel awareness on limits concerning the use of information processing facilities. These include internet, electronic mail, and usage of mobile devices both within and outside the organisation.

11.2.4 Human Resources Security

As indicated in the results, Zambian copper mines are currently aware of the importance of ensuring that personnel understand their information security roles and responsibilities in their organisations. Hence, they have since established measures to achieve this. It is interesting to note that in the Leadership Perception Questionnaire, senior management believe information security is adequately integrated into employment policies and procedures while middle management on the other hand, as revealed in the ISO/IEC 27002 Audit Tool Domain 4 Questionnaire felt that the organisation's security roles and responsibilities are not documented or communicated in employees' job descriptions. Both senior and middle management, however, agree that personnel do not receive adequate information security education, training, and awareness. Effective management of personnel information security roles and responsibilities ensures that their use of information processing facilities is appropriately managed and minimises insider threats. It is, therefore, recommended that the following four (4) issues receive appropriate consideration:

- Management to undertake the responsibility of ensuring that all personnel receive the appropriate level of awareness, training, and education which is relevant to their job role, responsibility and skills. Information security training and education programs should be considered for:

    - Senior management: appreciation of the importance of information security in relation to organisational operations.

- General staff: importance and application of information security best practices.
- IT personnel: implementation of information security best practices.

- Complete removal of organisational information from personal devices upon termination of personnel.
- Change of known passwords for accounts that will remain active upon termination of personnel, when personnel change job roles and responsibilities or when a contract or agreement is terminated.
- Use of job descriptions as a means of documenting and addressing employees' information security roles and responsibilities.

11.2.5 Physical and Environmental Security

As indicated in the results, Zambian copper mines are currently aware of the importance of securing their assets from physical and environmental threats. Hence, measures to protect these assets have been implemented. It is interesting to note from the Leadership Perception Questionnaire, however, that, while senior management believe their organisations' equipment is protected from environmental threats, middle management on the other hand, as revealed in the ISO/IEC 27002 Audit Tool Domain 5 Questionnaire felt that although this was the case, security of equipment from physical threats still requires attention. Adequate protection of the organisation's assets from physical and environmental threats helps prevent loss, misuse, theft or compromise to an organisation's activities. It is, therefore, recommended that the following four (4) issues receive appropriate consideration:

- Implementation of physical access controls to only allow authourised access to secure areas:
  - Regular review and update of access rights to secure areas.
  - All personnel and visitors should be required to wear visible identification and personnel should notify security personnel when they encounter anyone not wearing visible identification.

- Ensure that guidelines for secure areas do not permit phones with cameras or any form of photographic, audio and video recording equipment in these areas.
- Documentation of all reported faults, and their subsequent resolutions, routine maintenance and preventative measures that have been implemented.
- Enhancement of measures for the protection of information processing equipment used offsite. These measures should include:
    - Disguising portable computers when travelling.
    - Using risk assessments to identify and further implement home working controls including clear desk policies.

11.2.6 Communications and Operations Management

As indicated in the results, Zambian copper mines are currently aware of the importance of correct and secure operations of information processing facilities and exchange of information in their organisations. Hence, they have established measures to manage these operations. It is interesting to note that in the Leadership Perception Questionnaire, senior management believe adequate electronic communication policies and procedures have been developed in their organisations while middle management on the other hand, as revealed in the ISO/IEC 27002 Audit Tool Domain 6 Questionnaire felt that electronic communication procedures and controls still require attention. Effective management of the organisation's operations and communication processes enhances the control of communication facilities and operational activities of information processing facilities. This helps reduce security risks on the organisation's information assets by enhancing system and network management. It is, therefore, recommended that the following nine (9) issues receive appropriate consideration:

- Documentation of all operating procedures and subsequently availing them to the users who require access to them.
- Use of information handling and storage procedures to ensure that information is protected from misuse or unauthorised disclosure. These procedures should apply to information in

mobile communication devices, facsimile machines, printers, voice communications, mail, computer systems, networks and postal facilities. The following guidelines should be considered:

  - Restricted access to facilities.
  - Protection of spooled data.
  - Regular review of distribution lists.
  - Correct labeling and classification of all media and clear marking of media for the intended recipient.

- Use of formal policies, procedures, and controls to address the control of the exchange of information through all communication facilities. These controls should include:
  - Use of cryptographic controls in information exchange to ensure the authenticity, confidentiality, and integrity of information.
  - Restrictions on the forwarding of electronic mails to external mail destinations.
- Testing of all changes to be made to application and operational systems.
- User awareness on the dangers of malicious code and what to do when they encounter such code.
- Regular reviews of the software and data that support critical applications and processes, any unauthorised changes to systems or the presence of malicious code.
- Monitoring of administrator and operator activities by:
  - Logging administrator and operator activities.
  - Implementing an independent intrusion detection system to monitor administrator and operator compliance to system activities.

- Use of risk assessments to determine the level of monitoring required for each information processing facility.
- Regular testing and updating of backup plans and complete, accurate and up-to-date documentation of restoration procedures to ensure that critical information can easily be restored.

11.2.7 Access Control

As indicated in the results, Zambian copper mines are currently aware of the importance of controlling both physical and logical access to information processing facilities in their organisations. Hence, they have implemented measures to address these physical and logical access requirements. They seem to address the establishment of access control procedures reasonably adequately and certainly, control of user access privileges receives appropriate attention. As revealed from both the Leadership Perception Questionnaire and the ISO/IEC 27002 Audit Tool Domain 7 Questionnaire, it is interesting to note that both senior and middle management believe mobile security governance requires attention. Adequate physical and logical access controls in an organisation help protect the organisation's assets from unauthorised access. It is, therefore, recommended that the following seven (7) issues receive appropriate consideration:

- Regular review of the access control policy based on the organisation's business and security requirements.
- Adoption of a clear screen policy for information processing facilities and a clear desk policy for both papers and media.
- Use of the mobile computing and communication policy to address all mobile devices in use in the organisation coupled with personnel training to raise awareness on the risks associated with mobile computing. This policy should include requirements for:
    - Physical protection and access control.
    - Backup facilities.

- Virus protection and cryptographic controls.

- Inclusion of a clause in personnel contracts that specifies the sanctions that will be imposed on personnel if they attempt to access facilities without authorisation.

- Address policies for information dissemination in the access control policy. This would include the need to know principle and information classification levels.

- Formal and regular review of user access rights so as to maintain control over access to information processing facilities.

- Network segregation of groups of users, information systems, and information services based on the organisation's access control policy.

11.2.8 Information Systems Acquisition, Development and Maintenance

As indicated in the results, Zambian copper mines are currently aware of the importance of securing information systems in their organisations. Hence, they have since established measures to address information security during the acquisition, development and implementation of information systems. These organisations mostly use off-the-shelf software products and two (2) of these organisations have since phased out the use of legacy systems. As revealed in both the Leadership Perception Questionnaire and the ISO/IEC 27002 Audit Tool Domain 8 Questionnaire, both senior and middle management believe emphasis on information security requirements during the acquisition, development, and implementation of information systems still requires attention. Effective information systems acquisition, development, and implementation processes in an organisation ensure that these information systems add value to the business. It is, therefore, recommended that the following eight (8) issues receive appropriate consideration:

- Identification and implementation of controls to be used for ensuring authenticity and message integrity in applications. This includes implementation of cryptographic controls and development of a policy on the use of these controls.

- Ensuring that updating of documentation on completion of each change to an information processing facility is addressed in change management procedures. Old documentation should also be archived if needed to support older versions of the software or disposed of using the appropriate document disposal procedures. BCPs should also be updated whenever changes to systems take place.
- Establishment of a testing environment that is separate from the production and development environments. This environment should be used to test new software and software updates.
- Establishment of controls to limit opportunities for information leakage. This should include protection against covert channels by:
    - Scanning outbound communications.
    - Regular monitoring of personnel and system activities as well as resource usage in computer systems.
- A complete and up-to-date inventory of assets for effective vulnerability management.
- Testing and evaluation of patches before applying them to the operational environment to ensure that they will be effective and their side effects can be withstood.
- Usage of cryptographic techniques including digital signatures to achieve confidentiality, authenticity and integrity, and non-repudiation of information.
- Archiving of previous versions of application software together with all procedures, configuration details, and supporting software for contingency purposes.

11.2.9 Information Security Incident Management

As indicated in the results, Zambian copper mines are currently aware of the importance of managing information security incidents in their organisations. Hence, measures pertaining to incident reporting and management have since been established. These organisations address the protection of information systems from human error reasonably adequately. It is, however,

interesting to note from both the Leadership Perception Questionnaire and the ISO/IEC 27002 Audit Tool Domain 9 Questionnaire that both senior and middle management believe the establishment and implementation of incident response plans still requires attention. Effective information security incident management ensures appropriate corrective measures are quickly taken whenever an incident occurs. It is, therefore, recommended that the following four (4) issues receive appropriate consideration:

- Incorporation of information security incidents into personnel awareness programs as examples of possible incidents, how they could be handled and prevented in the future.
- Incorporation of information security incidents into information security policy reviews.
- Adoption of a code of practice or standard that will ensure evidence is admissible in a court of law.
- Establishment of procedures that would be used to handle different information security incidents. These procedures should cater for, among others:
    - Malicious code.
    - Denial of service attacks.
    - Breaches of integrity.

11.2.10 Business Continuity Management

As indicated in the results, Zambian copper mines are currently aware of the importance of protecting business activities from interruptions and timely resumption of business processes as well as minimising the effects of major failures and disasters. Hence, they have put in place measures to minimise interruptions to business activities. Senior management endorses business continuity strategies in these organisations and certainly the impacts that failures could have on the organisations' processes have been evaluated. The inclusion of information security requirements in the BCPs and regular reviews of these BCPs, however, still require attention. It is interesting to note that both senior and middle management are aware that some aspects of business continuity management still require addressing. This was revealed in both the

Leadership Perception Questionnaire and the ISO/IEC 27002 Audit Tool Domain 10 Questionnaire. Effective business continuity management reduces the chances of interruptions to business activities and minimises the impact these interruptions would have on the business. It is, therefore, recommended that the following three (3) issues receive appropriate consideration:

- Identification of all assets required for critical business processes. This should be carried out in a managed business continuity process that addresses information security requirements.
- Regular testing, review, and updating of BCP and processes to ensure that they are realistic and can be used in a real-life scenario. This includes adoption of techniques such as
    - Complete rehearsals.
    - Supplier facility and services testing.
    - Simulations.
    - Table-top testing of different scenarios.
- Adoption or maintenance of a single framework for BCPs to ensure that all plans are consistent and that they consistently address information security requirements, along with the identification of priorities for testing and maintenance.

11.2.11 Compliance

As indicated in the results, Zambian copper mines are currently aware of the importance of compliance with legislative requirements in their organisations. Hence, legislative requirements have been identified and some measures put in place to ensure their organisations' compliance. They address the protection of the organisation's important records reasonably adequately and certainly procurement and auditing of application software is receiving sound attention. Procedures that deal with intellectual property rights and proprietary software products as well as user awareness regarding the protection of these rights, however, still require attention. It is interesting to note that in the Leadership Perception Questionnaire, most members of senior management believe their organisations adhere to regulatory requirements while middle

management on the other hand, as revealed in the Domain 11 Questionnaire felt that requirements for intellectual property rights are in need of attention. Compliance with legal, statutory, contractual, and regulatory requirements is necessary for the organisation to avoid legislative implications. It is, therefore, recommended that the following three (3) issues receive appropriate consideration:

- Implementation of appropriate procedures to ensure compliance with legislative, contractual, and regulatory requirements regarding intellectual property rights and proprietary software products. These procedures would include:
    - Publication of an intellectual property rights compliance policy which defines the legal use of information and software products.
    - Maintenance of personnel awareness on policies intended to protect intellectual property rights.
- Explicit identification, documentation and regular update of all regulatory, statutory, and contractual requirements that are applicable to the organisation. This should also be done for each information system. These requirements include, among others:
    - Information Communications and Technologies Act, 2009.
    - Electronic Communications and Transactions Act, 2009.
    - Copyright and Performance Rights Act, 1994.
    - National Information and Communication Technology (ICT) policy.
- User awareness on the scope of access for information processing facilities that is permitted. Users should be given a written undertaking to this effect which they should in turn sign and return to the organisation. A warning message should also be displayed at log-on to indicate that the particular information processing facility is owned by the organisation and should only be accessed as authourised.

11.3 Recommendations for Senior Management

- Senior management should have a thorough understanding of information security in their organisations in order for them to make informed decisions about the information security process in their organisations.
- Information security should be strategically aligned with business processes if full benefits are to be realised.
- Senior management should be part of information security training and awareness programs. This should include both strategic and operational awareness.

11.4 Conclusion

The Zambian copper mining industry like other industries has embraced the importance of information security in their operations and business activities. This study revealed that several measures have actually been put in place to encompass information security in these organisations. There are still areas of concern, however, that would seem to require addressing as outlined in this chapter. Overall, communications and operations management, information system acquisition, development, and maintenance, and access control have more issues that require consideration than other areas. The use of mobile devices for business activities is now becoming commonplace and poses a risk to the security of organisations' information. Personnel awareness at all levels is a critical factor in the effective implementation of information security. Information security compliance requirements are currently being explicitly identified and enforced in Zambia. Hence, Zambian copper mining organisations equally need to integrate these into their information security programs. Ultimately, this responsibility for enhancing information security lies with management fully understanding the strategic importance of information security. This should be coupled with full management commitment and support for information security programs and spearheading of information security governance frameworks. Chapter 12 concludes this research.

Chapter 12

Information Security Framework for Zambian Copper Mines

Chapter 11 provided recommendations that Zambian copper mining organisations should consider as they work towards securing their information processing facilities. This chapter provides a framework that Zambian copper mines can use in their operations.

12.1 Introduction

Chapter 11 provided recommendations for information security practices in Zambian copper mines based on the information security gaps that had been identified in the research. This chapter describes key aspects that would enhance effective implementation and management of information security in Zambian copper mines.

12.2 Information Security Framework for Zambian Copper Mines

The following were identified as key aspects of information security in Zambian copper mines that if appropriately addressed would enhance the effective management of information security programs in these organisations:

- Information security should be strategically aligned with business operations in Zambian copper mines as its implementation should start from the highest level of the organisation.
- Management should support and be fully committed to the information security process as it is responsible for driving information security programs in organisations. Not only should senior management in Zambian copper mining organisations show full commitment and accountability to information security but they should also have a thorough understanding of information security as a strategic instrument in their organisations.
- Information security policies should be developed and kept up-to-date to ensure that a baseline for the implementation of information security in these organisations is created.
- In as much as corporate governance is important to these organisations, information security governance should equally form part of the governance frameworks for Zambian copper mining organisations. Management should be held accountable for the implementation of these frameworks.

- Mobile security governance should also be implemented as the use of mobile devices in these organisations has expanded.

- Personnel, who include employees, contractors, and third-party users, should be the key players in information security programs as they are a critical component of these programs. Personnel awareness should be one of the top priorities in information security programs. These awareness programs should include all users of information systems who consist of senior management, employees, third-party users and contractors. It is equally important that an information security culture is developed in conjunction with the organisational culture so that personnel feel that they are part of the information security programs.

- Mining organisations are inherently large organisations that produce and use a lot of information which is mostly in dispersed locations. Complete and up-to-date asset inventories are required for the accountability, effective risk management and correct use of this information if full benefits for their strategic business use are to be realised.

- Risk management is an important aspect of the information security process. Increased use and dependence on information systems raises the risk that comes with information usage. Regular internal and independent risk assessments need to be carried out and they should form a vital part of the risk management process.

- A business continuity framework should be implemented to address the security of critical information assets in Zambian copper mines. This should include identification of these assets, their information security requirements and priorities for testing and maintenance.

- Information security staff in an organisation cannot always be experts in the entire information security process. Zambian copper mining organisations should identify areas of information security where specialist advice is needed and identify the specialists who can provide advice on these areas.

- Although deemed not to be strongly enforced, information security regulations are now being enhanced in Zambia. Adoption and adherence to these regulations will help Zambian mining organisations conform to information security legislative requirements more effectively.

- Industrial Control Systems (ICS) such as SCADA systems and PLCs form a vital part of operations in Zambian copper mining organisations. Their security is, however, often neglected compared to corporate systems and they are generally not made part of the overall information security program. Although the ISO/IEC 27002 standard does not explicitly cater for control systems, guidelines such as the National Institute of Standards and Technology's NIST SP800-82 (Guide to Industrial Control Systems (ICS) Security)which although is still in draft form, should be adopted to provide guidance for the security of ICS. Industrial Control Systems require as much protection as other corporate systems as they are an important part of information systems in Zambian copper mines.

- Mining organisations rely on ERPs for the consolidation of information systems and integration of data. These ERPs, therefore, need to be protected by ensuring that their security is taken into consideration before, during and after implementation, security access controls highly enforced, and their usage regularly audited.

- Access controls should address both logical and physical access to information. These controls will only work effectively if all data in the organisation is identified and can be accounted for.

12.3 Conclusion

A generic information security standard is not enough to adequately address information security in Zambian copper mines. A specific framework that is customised for these organisations would serve as a checklist and help enhance effective implementation of information security in these copper mines.

Chapter 13

Conclusion

Chapter 12 proposed a framework that Zambian copper mining organisations should consider as they work towards securing their information processing facilities. This chapter concludes the research, provides areas for future research and the contributions that this research has made.

13.1 Introduction

In their quest for efficient and strategic operations, Zambian copper mines have embodied the adoption of information technologies into their operations. Information has, therefore, become an important tool in these organisations. Hence as the dependence on information grew, so have the risks associated with this usage and the importance of safeguarding information assets and information processing facilities. This dependence has been seen in electronic communication where emails have become an important communication tool in these organisations, so has the increased usage of mobile devices for business use. In addition, systems such as ICS' and ERPs are used for strategic decision making in these organisations. Several measures have been put in place to safeguard and control the usage of these facilities. Although information security measures and controls are implemented in Zambian copper mining organisations, there are still areas that are in need of attention. Furthermore, some of these practices have not been standardised by the adoption of an information security standard or framework.

13.2 General Contributions of the Research

- Management is responsible for driving information security programs in organisations. Not only should senior management in Zambian copper mining organisations show full commitment and accountability to information security but they should also have a thorough understanding of information security as a strategic instrument in their organisations. The research revealed that in certain cases, senior management perceptions of information security practices in these organisations were different from those of middle management.

- Mining organisations are driven by the need to adhere to strict SHEQ standards as well as mining regulations. These require the application of accurate information which would be enhanced by a sound information security program.

- Adoption of an information security standard complements an organisation's information security policy and assists in making the policy implementation more effective. There are a variety of information security standards available for Zambian copper mining organisations to adopt. Most of these standards are internationally recognised and

universally accepted. Selection of this standard depends on the information security policies that have been agreed upon by management as policies drive the information security program. Most Zambian copper mining organisations have information security policies in place; hence information security blueprints are already in place which would make the implementation of a standard or framework easier. Some respondents expressed interest in adopting an information security standard and others were already in the process of doing so. Interestingly, one Zambian copper mine is planning on adopting the ISO/IEC 27002 standard as part of its information security program.

13.3 ISO/IEC 27002 and Recommendations for Zambian Copper Mines

The ISO/IEC 27002 standard is a universally accepted and widely used standard globally. It was used in this research as it provided a framework that was suitable for Zambian copper mining organisations. This standard encompasses 11 information security domains which are universally accepted information security domains. These domains were all applicable to current information security practices in the Zambian copper mining industry.

The ISO/IEC 27002 standard by itself, however, does not sufficiently cater for information security best practices in the Zambian copper mining industry. The introduction of an additional framework or standard for this industry would ensure that aspects not catered for in the ISO/IEC 27002 standard are addressed. In addition, the standard does not explicitly address the security of ERPs which are commonly used in the Zambian copper mining industry.

13.4 Future Work

The researcher believes that conducting further in-depth case studies by administering the ISO/IEC 27002 Audit Tool Questionnaires in more than one copper mining organisation in Zambia, would yield further in-depth understanding of information security practices in these organisations, especially from a middle management perspective.

Furthermore, including a standard or framework that caters for such aspects of information security in the mining industry as Industrial Control Systems in addition to the ISO/IEC 27002

standard would ensure all aspects of these practices are addressed from a standardised perspective. Although the ISO/IEC 27002 caters for information systems implementation and maintenance,

A possible limitation of this work could relate to the 'halo' effect in which perhaps a slightly optimistic view of questionnaire responses could have been given by respondents. In addition, administering a similar audit tool to the users themselves would give a more complete picture of information security practices in these organisations from a senior management, middle management and user perspective.

13.5 In Closing

Zambian copper mining organisations like others face numerous challenges when it comes to safeguarding their information assets. These organisations are coming from a background where technological progress leading to business efficiency mostly affected the physical component of business operations. These organisations have over time become multifaceted and have adopted newer technologies which have led to an increased dependence on information for efficient and strategic operations. This evolution requires that management takes up the ultimate responsibility of driving the efficient use of this information which effectively involves safeguarding information assets in order for this efficiency to be achieved. Information security programs, therefore, have to be effectively implemented and should emphasise allocation of information security responsibilities, implementation of Security Education, Training and Awareness (SETA), and adoption of an information security framework or standard. Adoption of a standard or framework will ensure that information security practices in these organisations are standardised and evidence from their information systems can be admissible in court in case of legal implications. Although the security of information can never be foolproof as new risks and new solutions are identified every day, measures can still be put in place to reduce the effect these risks will have on business activities and the organisation's operations. No organisation is spared from information risks as long as they use information. The need for effective ongoing information security practices in Zambian Copper Mines can, therefore, not be overlooked.

List of References

AKANER, M. (2003) — **Application of ISO 9000 and OHSAS 18000 to a Mining Company, a case study.** [Online]. Available: http://etd.lib.metu.edu.tr/upload/3/1054980/index.pdf [Accessed 19 March 2009]

ALOINI, D., DULMIN, R. AND MININNO, V. (2007) — Risk Management in ERP Project Introduction: Review of the Literature. **Information & Management.** 44: 547–567

ANDERSEN, P.W. (2001) — Information Security Governance. **Information Security Technical Report.** 6, 3: 60-70

ANTTILA J., KAJAVA J., AND VARONEN R. (2004) — Balanced Integration of Information Security into Business Management. **Proceedings of the 30th EUROMICRO'04, IEEE. 558-564**

AFRICAN REGIONAL INTELLECTUAL PROPERTY ORGANISATION (ARIPO) (2009) — **About ARIPO.** [Online]. Available: http://www.aripo.org/index.php?option=com_content&view=article&id=19&Itemid=53 [Accessed 25 October 2009]

ARJOON, S. (2005) — Corporate Governance: An Ethical Perspective. **Journal of Business Ethics. 61: 343-352**

ASHBAUGH, D. A. (2008) — **Security Software Development: Assessing and Managing Security Risks.** Boca Raton: CRC Press

AT&T (2002) — **Achieving Resilience – Best Practices in Business Continuity.** [Online]. Available: http://www.continuitycentral.com/bestpractices.pdf [Accessed 10 October 2009]

ATKINSON, T. (1992) — Future Concepts in Surface Mining. In: Hartman, H. L. (ed). **SME Mining Engineering Handbook, Volume 2 (2e).** Littleton: SME

AVRAMENKO, A. AND THOMAS, R. (2000) — Managing The Perception of Geological Hazards. In: Scott, P. W. and Bristow, C. M. (Eds). **Industrial Minerals And Extractive Industry Geology**. Bath: Geological Society

BACIK, S. (2008) — **Building an Effective Information Security Policy Architecture**. Boca Raton: CRC Press

BAJPAI, S. AND GUPTA, J. P. (2005) — Site Security for Process Industries. **Journal of Loss Prevention in the Process Industries.** 18,4-6: 301-309

BARNDT, D. AND SCHAEFER, T. V. (2003) — What are the Major Components of a Disaster Recovery Plan? In: Laube, D. R. and Zammuto, R. F. (eds). **Business-driven Information Technology: Answers to 100 Critical Questions for Every Manager.** Stanford: Stanford University Press

BARTELS, N. (2005) — **Securing the Process Industries.** [Online]. Available: http://www.mbtmag.com/article/193165-Securing_the_process_industries.php [Accessed 07 August 2009]

BERCHET, C. AND HABCHI, G. (2005) — The Implementation and Deployment of an ERP System: An Industrial Case Study. **Computers in Industry.** 56: 588–605

BERGSMA, K. (2009) — **IT Security Guide 2: Information Security Governance.** [Online]. Available: https://wiki.internet2.edu/confluence/display/itsg2/Information+Security+Governance [Accessed 17 October 2009]

BOPA DAILY NEWS (2001) — **Jwaneng Mine Environmentally Certified at Last.** [Online]. Available: http://www.gov.bw/cgi-bin/news.cgi?d=20010209 [Accessed 04 May 2009]

BOTHA, J. AND VON SOLMS, R. (2004) — A Cyclic Approach to Business Continuity Planning. **Information Management and Computer Security.** 12, 4: 328-337.

BRADLEY, C. (2008) — **Top Five Steps to Proactively Manage Email Risk and Keep Compliance in Check.** [Online]. Available: http://www.itsecurityjournal.com/index.php/Latest/Top-Five-Steps-to-Proactively-Manage-Email-Risk-and-Keep-Compliance-in-Check.html [Accessed 01 September 2009]

BRAGG, R. (2002) **CISSP - Certified Information Systems Security Professional: Training Guide.** Indianapolis: Que Publishing

BRAGG, R. RHODES-OUSLEY, M. AND KEITH, S. (2004) **Network Security: The Complete Reference. New York:** McGraw-Hill Professional

BRITISH STANDARDS INSTITUTION (BSI) (2010) **ISO/IEC 27001 Information Security.** [Online]. Available: http://www.bsigroup.com/en/Assessment-and-certification-services/management-systems/Standards-and-Schemes/ISO-IEC-27001/ [Accessed 10 September 2010]

BRODER, J. F. (2006) **Risk Analysis and the Security Survey** (3e). Burlington: Butterworth-Heinemann

BRODERICK, J. S. (2001) Information Security Risk Management — When Should It be Managed?. **Information Security Technical Report. 6, 3: 12-18.**

BRÖRING, S. (2006) **The Front End of Innovation in Converging Industries: The Case of Nutraceuticals and Functional Foods.** Wiesbaden: DUV

BROTBY, K. (2009A) **Information Security Governance.** Hoboken: John Wiley and Sons

BROTBY, W. K. (2009B) **Information Security Management Metrics: A Definitive Guide to Effective Security Monitoring and Measurement**. Boca Raton : Auerbach Publications

BRYSON, J. (2006) **Managing Information Services: A Transformational Approach** (2e). Aldershot: Ashgate Publishing

BUTLER, S. (1998) **Establishing a System of Policies and Procedures: Setting Up Successful Policies and Procedures System for Printed, On-Line, and Web Manuals** (2e). Westerville : Process Improvement

CABALLERO, A. (2009) Information Security Essentials for IT Managers: Protecting Mission-Critical Systems. In: Vacca, J. R (ed). **Computer and Information Security Handbook.** Burlington: Morgan Kaufmann

CALDER, A. (2006) **Implementing Information Security Based on ISO 27001/ISO 17799: A Management Guide**. Zaltbommel: Van Haren Publishing

CALDER, A. (2008) **ISO27001/ISO27002 A Pocket Guide.** Ely: IT Governance

CALDER, A. AND WATKINS, S. (2006) **International IT Governance: An Executive Guide to ISO 17799/ISO 27001.** London: Kogan Page Publishers

CANO, J. (2002) **Critical Reflections on Information Systems.** Hershey: Idea Group Inc (IGI)

CAMPBELL, C. (2008) **Legal Aspects of Doing Business in Africa.** Salzburg: Yorkhill Law Publishing

CARPENTER, T, AND BARRETT, J. (2007) **CWNA Certified Wireless Network Administrator: Official Study Guide: Exam PW0-100** (4e). New York: McGraw-Hill Professional

CARTER, K. AND PRESNELL, M. (1994) **Interpretive Approaches to Interpersonal Communication.** Albany : State University of New York Press

CASTEELE, S. V. (2005) **Threat Modeling For Web Applications Using The Stride Model.** [Online]. Available: http://www.slideshare.net/stijnvdc/threat-modeling-for-web-applications-using-the-stride-model-2794119 [Accessed 10 September 2010]

CÁRDENAS, A. A., AMIN, S. AND SASTRY, S. S. (2008) "**Research Challenges for the Security of Control Systems**". Proceedings of the 3rd USENIX Workshop on Hot topics in security, USENIX, Article 6. [Online]. Available: http://www.usenix.org/event/hotsec08/tech/full_papers/cardenas/cardenas.pdf [Accessed 10 August 2009]

CERULLO, V. AND CERULLO, M. J. (2004) **Business Continuity Planning: A Comprehensive Approach.** [Online]. Available: http://www.itknowledgebase.cn/dynamic_data/3138_1893_bcp.pdf [Accessed 26 February 2009]

CHANDLER, R. (2007) Security on a Global Scale. In: Barton, L. (ed). **Crisis Leadership Now: A Real-World Guide to Preparing for Threats, Disaster, Sabotage, and Scandal.** New York: McGraw-Hill Professional

CHANG, A. AND YEH, Q. (2006) On Security Preparations Against Possible IS threats Across Industries. **Information Management and Computer Security.** 14, 4: 343-360

CHRISTMANN, P., ARVANITIDIS, N., MARTINS, L., RECOCHÉ, G. AND SOLAR, S. (2006) **Towards the Sustainable Use of Mineral Resources: a European Geological Surveys perspective** [Online]. Available: www.coleurop.be/file/content/StudyProgrammes/eco/chair/toyota/20061 2_conference/.../Christmann_Paper_Growth_Conf_Bruges.pdf. [Accessed 01 June 2009]

CITECT (2008) **Change is at the Core of Evolution as Citect Launches Version 3.2 of its Next-gGneration MES Solution, Ampla.** [Online]. Available: http://www.itweb.co.za/office/citect/0804170804.htm

[Accessed 01 September 2009]

CLINCH, J. (2009) **ITIL v3 and Information Security.** [Online]. Available: http://www.best-management-practice.com/gempdf/ITILV3_and_Information_Security_White_Paper_May09.pdf [Accessed 20 November 2009]

COCCA, P. (2004) **Email Security Threats.** [Online]. Available: http://www.sans.org/reading_room/whitepapers/email/email_security_threats_1540?show=1540.php&cat=email [Accessed 15 July 2009]

COMPUTER ETHICS INSTITUTE (CEI) (2009) **Ten Commandments of Computer Ethics.** [Online]. Available: http://computerethicsinstitute.org/ [Accessed 19 October 2009]

CONKLIN, A. (2009) Threat Modeling and Secure Software Engineering Process. In: Gupta, J. N. D. and Sharma, S. K. (eds). **Handbook of Research on Information Security and Assurance.** Hershey: Idea Group Inc (IGI)

CONTESTI, D., ANDRE, D. AND WAXVIK, E. (2007) **Official (ISC)2 Guide to the SSCP CBK.** Boca Raton: CRC Press

COOMBS, W. T. (2008) **PSI Handbook of Business Security: Securing the Enterprise.** Westport: Greenwood Publishing

COOPER, D. (2003) **Psychology, Risk & Safety: Understanding How Personality & Perception Can Influence Risk Taking. *Professional Safety*. 2003: 39–46.**

COPANS, G. (2007) **ERP Integrator Company Provides Consolidation, Governance to Mine Operations.** [Online]. Available: http://www.miningweekly.com/article/erp-integrator-company-provides-consolidation-governance-to-mine-operations-2007-10-05 [Accessed 12 May 2009]

COYLE, B. (2004) **Risk Awareness and Corporate Governance** (2e). Canterbury: Institute of Financial Services

CRI ENGLISH (2009) **Zambia's Copper Production up in First Quarter.** [Online]. Available: http://english.cri.cn/6826/2009/05/14/1601s484645.htm [Accessed 14 May 2009]

CROCKER, K. J. (2003) Risk and Risk Management. In Meyer, D. J (ed). **The Economics of Risk.** Kalamazoo: W.E. Upjohn Institute

CULP, C. L. (2001) **The Risk Management Process: Business Strategy and Tactics.** New York: John Wiley And Sons

DATTATREYA, Y. (2008) **Building Enterprise Security Programs**. [Online]. Available: http://articles.directorym.com/Building_Enterprise_Security_Programs-a1145193.html [Accessed 17 June 2009]

DAVENPORT, T. (1993) **Process Innovation: Reengineering Work through Information Technology.** Boston: Harvard Business Press

DAVENPORT, T. H. AND HARRIS, J. G. (2007) **Competing on Analytics.** Boston: Harvard Business Press

DAVIS, M. (2007) **Using Business Intelligence For Competitive Advantage** [Online]. Available: http://www.knowledgepoint.com.au/business_intelligence/Articles/BI_MD001a.html [Accessed 19 May 2009]

DEANS, P. C. AND KARWAN, K. R. (1994) **Global Information Systems and Technology: Focus on the Organization and its Functional Areas.** Hershey: Idea Group Inc (IGI)

DELL (2006) **Better Business Protection Through Virtualization.** [Online]. Available: http://www.dell.com/downloads/global/power/ps4q06-20070169-Ziff.pdf [Accessed 14 September 2009]

DELOITTE TOUCHE TOHMATSU (DTT) (2008) **Gaining momentum. The 2008 Energy & Resources Global Security Survey.** [Online]. Available: http://www.deloitte.com/assets/Dcom-Australia/Local%20Assets/Documents/Gaining%20momentum%20The%202008%20Energy%20Resources%20Global%20Security%20Survey.pdf [Accessed 20 October 2009]

DENBY, B. AND SCHOFIELD, D. (1999) Advanced Computer Techniques: Developments for the Minerals Industry Towards the New Millenium. In: Xie, H. & Golosinski, T. S. (eds). **Mining Science and Technology '99.** Rotterdam: A. A. Balkema

DEPARTMENT OF PRIMARY INDUSTRIES (DPI) (2005) **Minerals Industry Risk Management (MIRM)** [Online]. Available: http://www.dpi.nsw.gov.au/minerals/safety/resources/risk-management [Accessed 05 August 2009]

DOBELIS, E. (2007) Expert Systems for Business Decision on Security Requirements. In: Meersman**,** R., Tari, Z., Herrero, P., Herrero, H. M. (eds). **On the Move to Meaningful Internet Systems 2007: OTM 2007 Workshops.** Berlin: Springer

DODGSON, M. **The Challenges and Opportunities of Globalization**

AND VANDERMARK, S. (2000) **and Innovation in the Minerals Industry.** [Online]. Available: http://www.atypon-link.com/EMP/doi/pdf/10.5555/impp.2000.3.4.3 [Accessed 20 November 2009]

DODSON, R. (2001) Information Incident Management. **Information Security Technical Report,** 6, 3: 45-53

DOUGHTY, K. (2001) **Business Continuity Planning: Protecting Your Organization's Life.** Boca Raton: Auerbauch

DOUGHTY, K. (2007) **Selecting The Right Business Continuity Strategy.** In: Tipton, H. F. and Krause, M. (eds). **Information Security Management Handbook (6e).** Boca Raton: Taylor and Francis group.

ENCYCLOPÆDIA BRITANNICA (2009) **Science & Technology: Information System.** [Online]. Available: http://www.britannica.com/EBchecked/topic/287895/information-system [Accessed 18 May 2009]

ELROD, R. (2005) **So You Think You Have a Good Business Recovery Plan? – Steps an Asset Management Company Can Take to Recover From a Major Disaster.** [Online]. Available: http://www.infosecwriters.com/text_resources/pdf/Good_Business_Recovery_Plan.pdf [Accessed 26 September 2009]

ENDORF, C. F. (2006) **Secured Computing: A SSCP Study Guide**. St, Victoria: Trafford Publishing

ERNST & YOUNG (2008) **Ernst & Young's 2008 Global Information Security Survey: Moving Beyond Compliance.** [Online]. Available: http://www.ey.com/Global/assets.nsf/Russia_E/GISS_2008_EN/$file/GISS_2008_EN.pdf [Accessed 26 February 2009]

ESRI (2009) **ArcView.** [Online]. Available: http://www.esri.com/software/arcgis/arcview/index.html [Accessed 27 June 2009]

FAGG, S. (2009) **Mining, Financial Services Leading Risk Charge.** [Online]. Available: http://www.riskmanagementmagazine.com.au/articles/fb/0c02c6fb.asp [Accessed 12 November 2009]

FALCO, J., STOUFFER, K., WAVERING, A. AND PROCTOR, F. (2002) **IT Security for Industrial Control Systems.** [Online]. Available: http://www.isd.mel.nist.gov/documents/falco/ITSecurityProcess.pdf [Accessed 01 December 2009]

FERRIS RESEARCH (2009) **Industry Statistics.** [Online]. Available: http://www.ferris.com/research-library/industry-statistics/ [Accessed 17 July 2009]

FISCHER, R., HALIBOZEK, E. AND GREEN, G. (2008) **Introduction to Security (8e).** Burlington: Butterworth-Heinemann

FISHER, M. J. AND MARSHALL, A. P. (2009) Understanding Descriptive Statistics. **Australian Critical Care.** 22: 93—97

FITZGERALD, T. (2008) Compliance Assurance: Taming the Beast. In: Tipton, H. F. and Krause, M. (eds). **Information Security Management Handbook (6e v2).** Boca Raton: Taylor and Francis group

FITZGERALD, T. (2007) Information Security Governance In: Tipton, H. F. and Krause, M. (eds). **Information Security Management Handbook (6e).** Boca Raton: Taylor and Francis group.

FLEGEL, U. (2007) **Privacy-Respecting Intrusion Detection.** New York: Springer

FORCHT, K. (1994) **Computer Security Management.** Cambridge: Course Technology.

FOSTER, P. (1996) **Observing Schools: A Methodological Guide.** London: Paul Chapman Publishing

FRASER, B. (1997) **RFC2196 - Site Security Handbook.** [Online]. Available: http://www.faqs.org/rfcs/rfc2196.html [Accessed 12 November 2009]

FULMER, K. L. (2004) **Business Continuity Planning: A Step by Step Guide with Planning Forms on CD-ROM** (3e)**.** Brookfield: Rothstein Associates

GALLIERS, R. AND LEIDNER, D. E. (2003) **Strategic Information Management: Challenges and Strategies in Managing Information Systems** (3e). Oxford: Butterworth-Heinemann

GARCIA, A. (2008) Business Continuity Best Practices. **eWeek.** 25, 33: 32-40

GARTNER (2002) **Best Practices and Trends in Business Continuity Planning.** [Online]. Available: http://symposium.gartner.com/docs/symposium/itxpo_orlando_2002/documentation/sym12_15a.pdf [Accessed 27August 2009]

GARTNER (2008) **Gartner Says Most Organizations Are Not Prepared For a Business Outage Lasting Longer Than Seven Days.** [Online]. Available: http://www.gartner.com/it/page.jsp?id=579708 [Accessed 10 September 2010]

GARTNER (2009) **Hype Cycle for Business Continuity Management, 2009.** [Online]. Available: http://www.gartner.com/DisplayDocument?id=1090713 [Accessed 20 November 2009]

GATEWOOD, B. (2009) Clouds On The Information Horizon: How To Avoid The Storm. **Information Management.** 43, 4

GERBER, M. AND VON SOLMS, R. (2005) Management of Risk in the Information Age. **Computers & Security.** 24, 1: 16-30

GEMCOM SOFTWARE (2009) **Gemcom Products.** [Online]. Available: http://www.gemcomsoftware.com/products/ [Accessed 19 September 2010]

GERRING, J. (2007) **Case Study Research: Principles and Practices.** New York: Cambridge University Press

GOLLMAN, D. (2005) **Computer Security** (2e)**.** New Delhi**:** Wiley-India

GOVERNMENT OF THE REPUBLIC OF ZAMBIA (GRZ) (1973) **Government of the Republic of Zambia: Guide to the Mining Regulations.**

GOVERNMENT OF THE REPUBLIC OF ZAMBIA (GRZ) (1994) **Copyright and Performance Rights Act, 1994.** [Online]. Available: http://portal.unesco.org/culture/en/files/30413/11425068613zm_copyright_1994_en.pdf/zm_copyright_1994_en.pdf [Accessed 27 October 2009]

GOVERNMENT OF THE REPUBLIC OF ZAMBIA (GRZ) (2000) **Mines and Minerals Act, 1995.** [Online]. Available: http://faolex.fao.org/cgi-bin/faolex.exe?rec_id=046304&database=FAOLEX&search_type=link&table=result&lang=eng&format_name=@ERALL [Accessed 14 September 2009]

HALL, J. (2008) **Accounting Information Systems** (6e). Mason: Cengage Learning

HAMEL, J., DUFOUR, S. AND FORTIN D. (1993) **Case Study Methods.** Newbury Park: SAGE Publications

HARRIS, S. (2007) **CISSP All-in-One Exam Guide** (4e). New York: McGraw-Hill Professional

HAWKER, A. **Security and Control in Information Systems: A Guide for**

(2000) **Business and Accounting.** London: Routledge

HAWKINS, S. YEN. D.C. AND CHOU, D.C. (2000) Disaster Recovery Planning: A Strategy for Data Security. **Information Management & Computer Security.** 8, 5: 222-229

HAGEN, J. M., ALBRECHTSEN, E., AND HOVDEN, J. (2008) Implementation and Effectiveness of Organizational Information Security Measures. **Information Management & Computer Security.** 16, 4: 377-397

HEATH, R. (2008) A Crisis Management Perspective of Business Continuity Planning. In**: The Definitive Handbook of Business Continuity Management.** Chichester: John Wiley & Sons

HEEKS, R. (2001) **Reinventing Government in the Information Age.** London: Routledge

HELBERGER, C. (2009) **10 Key Information Security and Compliance Activities for 2010.** [Online]. Available: http://www.itbusinessedge.com/cm/community/features/guestopinions/blog/10-key-information-security-and-compliance-activities-for-2010/?cs=34705 [Accessed 18 October 2009]

HENTEA, M. (2008) Improving Security for SCADA Control Systems**. Interdisciplinary Journal of Information, Knowledge, and Management**. 3: 73-86

HESS, K. M. AND HESS, K. M. (2008) **Introduction to Private Security** (5e). Belmont: Cengage Learning

HILL, T. AND ALVARADO, E. (2003) **HP Nonstop Server Security: A Practical Handbook.** Burlington: Digital Press

HINTON, W. AND CLEMENTS, R. (2002) Are You Managing the Risks of Downtime?. **Disaster Recovery Journal**. 15, 3. [Online]. Available: http://www.drj.com/articles/sum02/1503-12.html [Accessed 17 September 2009]

HITZMAN, M. W. (2002) R&D in a "declining" Industry (Mining): Support For The Development Of Revolutionary Technologies? **Technology in Society.** 24, 1-2: 63-68

HOLTSNIDER, B. AND JAFFE, B. D. (2007) **IT Manager's Handbook: Getting Your New Job Done (2e).** San Francisco: Morgan Kaufmann

HONAN, B. (2009) **Implementing ISO27001 in a Windows Environment.** Ely: IT Governance Ltd

HONG KONG SPECIAL **An Overview of Information Security Standards.** [Online]. Available:

ADMINISTRATIVE REGION (HKSAR) (2008) http://www.infosec.gov.hk/english/technical/files/overview.pdf [Accessed 20 November 2009]

HONOUR, D. (2007) Preface. Hiles, A. (ed). **The Definitive Handbook of Business Continuity Management** (2e). Chichester: John Wiley and Sons

HUSTRULID, W. A. AND BULLOCK, R. C. (2001) **Underground Mining Methods: Engineering Fundamentals and International Case Studies.** Littleton: SME

INSTITUTE OF INTERNAL AUDITORS, THE (IIA) (2001) **Information Security Governance: What directors need to know (Critical Infrastructure Assurance Project).** Altamonte Springs: The Institute of Internal Auditors

INFOSECURITY (2009) **RSA Europe: Information Security and data value should be part of education and training.** **[Online]. Available:** http://www.infosecurity-magazine.com/view/4791/rsa-europe-information-security-and-data-value-should-be-part-of-education-and-training/ **[Accessed 28 October 2009]**

INFORMATION SECURITY FORUM (ISF) (2007) **The Standard of Good Practice for Information Security.** [Online]. Available: https://www.isfsecuritystandard.com/SOGP07/pdfs/SOGP_2007.pdf [Accessed 04 November 2009]

INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION (ISACA) (2008) **CISA Review Manual 2009.** Rolling meadows: ISACA

INTERNATIONAL COUNCIL ON MINING AND METALS (ICMM) (2009) **Case Study: Communication Plans for Crisis Management.** [Online]. Available: http://www.icmm.com/page/722/communication-plans-for-crisis-management [Accessed 12 November 2009]

ISECT (2010) **ISO/IEC 27002:2005 Information Technology -- Security Techniques -- Code of Practice For Information Security Management.** [Online]. Available: http://www.iso27001security.com/html/27001.html [Accessed 10 September 2010]

ISO/IEC 27001 (ISO 27001) **Information Security Management Systems — Requirements.**

(2005)

ISO/IEC 27002 (ISO 27002) (2005) **Information Technology - Code of practice for Information Security Management.**

ISUCB (2009) **NIST and VISA Model.** [Online]. Available: http://www.lsucb.org/2009/06/nist-and-visa-model.html [Accessed 02 November 2009]

IT GOVERNANCE INSTITUTE (2007) **COBIT 4.1 Excerpt: Executive Summary Framework.** [Online]. Available: http://www.stanford.edu/dept/Internal-Audit/infosec/docs/COBIT4.1-executive_summary-membership.pdf [Accessed 16 October 2009]

IT GOVERNANCE INSTITUTE (ITGI) (2006) **Information Security Governance: Guidance for Boards of Directors and Executive Management** (2e). Rolling Meadows: ITGI

IT GOVERNANCE NETWORK (2009) **What is IT Governance?.** [Online]. Available: http://www.itgovernance.com/00/index.php/articles-aamp-news-mainmenu-2/27-governance [Accessed 28 October 2009]

JANCZEWSKI, L. AND COLARIK, A. M. (2005) **Managerial Guide for Handling Cyber-Terrorism and Information Warfare.** Hershey: Idea Group Inc (IGI)

JANULAITIS, M. V. (2007) **Disaster Recovery - Business Continuity Plan Template: Disaster Recovery Plan Template.** Park City: Janco Associates

JOHNSON, S. (2007) **The IT professional's business and communications guide: a real-world approach to Comp TIA A+ soft skills.** Hoboken: John Wiley and Sons

KAIRAB, S. (2004) **A Practical Guide to Security Assessments.** Boca Raton: Auerbach Publications

KAJAVA, J., ANTTILA, J., VARONEN, R. AND SAVOLA, R. (2006) Senior Executives Commitment to Information Security – from Motivation to Responsibility. **Proceedings of the International Conference on Computational Intelligence and Security, IEEE. 1519-1522**

KAJAVA, J. , ANTTILA, J., VARONEN, R., SAVOLA, R. AND RÖNING, J. (2006) Information Security Standards and Global Business. **Proceedings of the International Conference on Industrial Technology, IEEE. 2091-2095**

KARMIS, M. (2001) **Mine Health and Safety Management.** Littleton: SME

KENDRICK, T. (2003) **Identifying and Managing Project Risk: Essential Tools for Failure-Proofing Your Project.** New York: AMACOM

KENNEDY, J.(2006) Pandemic Business Continuity Planning – Things to Consider. [Online]. Available: http://www.continuitycentral.com/feature0300.htm [Accessed 10 October 2009]

KENT, A. AND WILLIAMS, J. G. (1996) **Encyclopedia of Computer Science and Technology, Volume 34.** New York: Dekker

KOLKOWSKA, E. (2005) Value Sensitive Approach to IS Security - A Socio-Organizational Perspective" (2005). **Proceedings of the Eleventh Americas Conference on Information Systems.** 3310-3317

KRUGER, H. A. AND KEARNEY, W. D. (2006) A Prototype for Assessing Information Security Awareness. **Computers & Security 2 5: 2 8 9 – 2 9 6**

KUEMPEL, E. D., GERACI, C.L. AND SCHULTE, P. A. (2007) Risk Assessment Approaches and Research Needs for Nanomaterials: An examination of Data and Materials from Current Studies. In: Simeonova, P. P., Opopol, N., Luster, M. I. and NATO Science for Peace and Security Programme (eds). **Nanotechnology--toxicological issues and environmental safety**

INTERNATIONAL STANDARDS ORGANISATIONS (ISO) (2010) **ISO/IEC 17799:2005.** [Online]. Available: http://www.iso.org/iso/catalogue_detail?csnumber=39612 [Accessed 12 September 2010]

ISO 27002 DIRECTORY (2008) **Introduction to ISO 27002 (ISO27002).** [Online]. Available: http://www.27000.org/iso-27002.htm [Accessed 10 October 2009]

KADAM, A. W. (2007) Information Security Policy Development and Implementation. **Information Security Journal: A Global Perspective.** 16, 5: 246 – 256

KIZIL, M. (2003) **Virtual Reality Applications in the Australian Mnerals Industry.** [Online]. Available: http://espace.library.uq.edu.au/eserv/UQ:99728/Kizil_2003_Apcom_South_Africa.pdf [Accessed 31 March 2009]

KIZZA, J. M. (2005) **Computer network security.** New York: Springer

KNIGHTS, P.F. AND **Information Technologies in the Minerals industry.** London:

DANESHMEND, L.K. (1998) Taylor & Francis

KOCH, R. (2004) Best Practices in Business Continuity**. Communications News.** 41, 11: 24-25

KONKOLA COPPER MINES (KCM) (2006) **KCM Mines Awarded ISO 14001:2004 Certification** [Online]. Available: http://www.kcm.co.zm/latest_news_full.php?id=6 [Accessed 01 March 2009]

KOVACICH, G. AND HALIBOZEK, E. P. (2003) **The Manager's Handbook For Corporate Security: Establishing And Managing A Successful Assets Protection Program.** Burlington: Butterworth-Heinemann

KREHNKE, D. C. (2007) Corporate Governance. In: Tipton, H. F. and Krause, M. (eds). **Information Security Management Handbook (6e).** Boca Raton: Taylor and Francis group.

KROON, J. (1995) **General Management** (2e). Cape Town: Pearson South Africa

KRUTZ, R. L. (2005) **Securing SCADA systems.** Hoboken: John Wiley and Sons

KRUTZ, R. L. AND VINES, R.D. (2003) **The CISSP® Prep Guide: Gold Edition.** Indianapolis: Wiley Publishing, Inc.

LA FAZIA, T. (2004) Avoid Disaster Through Planning. **Communications News.** 41, 11: 20-25

LAWRENCE, C. (2007) **Adapting Legacy Systems for SOA.** [Online]. Available: http://www.ibm.com/developerworks/webservices/library/ws-soa-adaptleg/ [Accessed 10 October 2009]

LAYTON, T. P. (2006) **Information Security: Design, Implementation, Measurement, And Compliance.** Boca Raton: CRC Press

LAUDON, K. C., AND LAUDON, J. P. (2005) **Essentials of Management Information Systems: Managing the Digital Firm** (6e). New Jersey: Pearson Prentice Hall

LAUDON, K. C., LAUDON, J. P. (1995) **Information Systems – A Problem Solving Approach** (3e). New York: The Dryden Press

LEHTINEN, R, RUSSELL, D. AND GANGEMI, G. T. (2006) **Computer Security Basics** (2e). Sebastopol: O'Reilly Media.

LERBINGER, O. **The Crisis Manager: Facing Risk And Responsibility.** Mahwah:

(1997) Lawrence Erlbaum Associates

LI, W. (2005) **Risk Assessment of Power Systems: Models, Methods, and Applications.** Hoboken: John Wiley and Sons

LINDSTRÖM, J. AND HÄGERFORS, A. (2009) A Model for Explaining Strategic IT- and Information Security to Senior Management. **International Journal of Public Information Systems.** 2009, 1: 17-29

LOWE, J., LASKY, J., GILBERT, D. AND SHEIL, K. (2007) Protecting Industrial Process Control, Automation, and SCADA Systems From Cyber Threats. **SPE Middle East Oil and Gas Show and Conference.** [Online]. Available: http://www.onepetro.org/mslib/servlet/onepetropreview?id=SPE-105696-MS&soc=SPE [Accessed 03 August 2009]

LUCEY, T. (2005) **Management Information Systems** (9e). Boston: Thomson Learning

MA, Q., JOHNSON, A. C., AND PEARSON, M. J.(2008) Information Security Management Objectives and Practices: a Parsimonious Framework. **Information Management & Computer Security.** 16, 3: 251 – 270

MACKEY, R. (2008) **How to Apply ISO 27002 to PCI DSS Compliance.** [Online]. Available: http://searchsecurity.techtarget.com/tip/0,289483,sid14_gci1295905,00.html [Accessed 10 October 2009]

MANDUCA, A. (2009) **Deloitte 2008 Survey Reveals Growing Information Security Risk.** [Online]. Available: http://www.timesofmalta.com/business/view/20090226/news/deloitte-2008-survey-reveals-growing-information-security-risk [Accessed 17 June 2009]

MARK, H. (2007) **People, Process, Technology.** [Online]. Available: http://www.transactionworld.com/articles/2007/May/security1.asp [Accessed 28 January 2009]

MARLIN-BENNETT, R. (2004) **Knowledge Power: Intellectual Property, Information, And Privacy.** Boulder: Lynne Rienner Publishers

MASLEN, C. (1996) Testing the Plan is More Important than the Plan Itself. **Information Management & Computer Security.** 4, 3: 26–29

MCGAUGHEY JR, R. E., SNYDER, C. A. AND CARR, H. H. (1994) Implementing Information Technology for Competitive Advantage: Risk Management Issues. **Information & Management**. 26: 273-280

MCMILLAN, T. (2007) **Change your Career: Computer Network Security as Your New Profession.** Wokingham: Kaplan Publishing

MCPHEE, D. (2008) Information Security Infrastructure Management Library And Security Overview. In: **Tipton, H. F. and Krause, M.** (eds). Information Security Management Handbook (6e v2). **Boca Raton: Taylor and Francis group**

MEARS, L. AND VON SOLMS, R. (2004) **Corporate Information Security Governance: A Holistic Approach.** [Online]. Available: http://icsa.cs.up.ac.za/issa/2004/Proceedings/Research/041.pdf [Accessed 17 October 2009]

MICROSOFT (2009) **Business Continuity Solutions.** [Online]. Available: http://www.microsoft.com/virtualization/solutions/continuity/default.mspx [Accessed 14 September 2009]

MILES, G. (2001) **Incident Response Part 1.** [Online]. Available: http://www.securityhorizon.com/whitepapersTechnical/IncidentResponsepart1.pdf [Accessed 04 September 2009]

MINING, MINERALS, AND SUSTAINABLE DEVELOPMENT PROJECT (MMSD) (2002) **Breaking New Ground: Mining, Minerals, and Sustainable Development: The Report of the MMSD Project.** London: IIED

MINING NEWS PREMIUM (2007) **Easier GIS for Mining.** [Online]. Available: http://www.miningnewspremium.net/StoryView.asp?StoryID=99546 [Accessed 31 May 2009]

MINING WEEKLY (2009) **Zambia Discovers More Copper in North of Country.** [Online]. Available: http://www.miningweekly.com/article/zambia-discovers-more-copper-in-north-of-country-2009-04-15 [Accessed 09 May 2009]

MINISTRY OF COMMUNICATION AND TRANSPORT (2006) **Zambia National Information and Communication Technology Policy.** [Online]. Available: http://www.mct.gov.zm/pdf/ict.pdf [Accessed 24 March 2009]

MINISTRY OF MINES AND MINERALS DEVELOPMENT (2009) **Mining in Zambia.** [Online]. Available: http://www.zambiamining.co.zm/mininginzambia.htm [Accessed 20 June 2009]

MITROPOULOS, On Incident Handling and Response: A State-Of-The-Art Approach.

S., MITROPOULOS, D. AND DOULIGERIS, C. (2006) **Computers & Security.** 25: 351-370

MONK, E. AND WAGNER, B. (2008) **Concepts in Enterprise Resource Planning**. Boston: Cengage Learning EMEA

MONTANA, P. J. AND CHARNOV, B. H. (2000) **Management.** Hauppauge: Barron's Educational Series

MOREIRA, E., MARTIMIANO, L. A. F., BRANDA˜O, A. J. AND BERNARDES, M. C.(2008) Ontologies for Information Security Management and Governance. **Information Management & Computer Security.** 16, 2: 150-165

MOTWANI, J., SUBRAMANIAN, R. AND GOPALAKRISHNA, P.(2005) Critical Factors for Successful ERP Implementation: Exploratory Findings from Four Case Studies. **Computers in Industry.** 56: 529–544

MOTTOLA, L., LIPSETT, M. AND SCOBLE, M. (2001) **Transforming the Mining Industry Through Electronic Commerce.** [Online]. Available: http://www.hatch.ca/Consulting/Knowledge_Base/Articles/Transforming%20the%20Mining%20Industry%20into%20an%20Electronic%20Business.pdf [Accessed 21 May 2009]

MSN ENCARTA (2009) **Code of Practice.** [Online]. Available: http://encarta.msn.com/encnet/features/dictionary/DictionaryResults.aspx?lextype=3&search=code%20of%20practice [Accessed 14 October 2009]

MUSSON, M. (2007) Business Continuity Strategies for Manufacturing and Logistics. In: Hiles, A. (ed). **The Definitive Handbook of Business Continuity Management.** Chichester: John Wiley & Sons

MYLER, E. AND BROADBENT, G. (2006) ISO 17799: Standard for Security. **Information Management Journal**. 40, 6:43

NATIONAL ASSEMBLY OF ZAMBIA (2009) **The Zambian Parliament.** [Online]. Available: http://www.parliament.gov.zm/index.php?option=com_docman&task=cat_view&gid=115&Itemid=113 [Accessed 10 November 2009]

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) (1995)

NIST SP800-12: An Introduction to Computer Security: The NIST Handbook. [Online]. Available: http://csrc.nist.gov/publications/PubsSPs.html [Accessed 10 November 2009]

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) (1996)

NIST SP800-14: Generally Accepted Principles and Practices for Securing Information Technology Systems. [Online]. Available: http://csrc.nist.gov/publications/PubsSPs.html [Accessed 02 November 2009]

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) (2001)

NIST SP800-33: Underlying Technical Models for Information Technology Security. [Online]. Available: http://csrc.nist.gov/publications/PubsSPs.html [Accessed 02 August 2010]

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) (2002)

NIST SP800-30: Risk Management Guide for Information Technology Systems. [Online]. Available: http://csrc.nist.gov/publications/PubsSPs.html [Accessed 02 November 2009]

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) (2006)

NIST SP800-18: Guide for Developing Security Plans for Federal Information Systems. [Online]. Available: http://csrc.nist.gov/publications/PubsSPs.html [Accessed 02 November 2009]

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) (2008A)

NIST SP800-53 Rev 3: Recommended Security Controls for Federal Information Systems and Organizations. [Online]. Available: http://csrc.nist.gov/publications/PubsSPs.html [Accessed 02 November 2009]

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) (2008B)

NIST SP800-61: Computer Security Incident Handling Guide. [Online]. Available: http://csrc.nist.gov/publications/PubsSPs.html [Accessed 02 November 2009]

NATIONAL INSTITUTE OF

NIST SP800-82: DRAFT Guide to Industrial Control Systems (ICS) Security.

STANDARDS AND TECHNOLOGY (NIST) (2008C) [Online]. Available: http://csrc.nist.gov/publications/PubsSPs.html [Accessed 02 November 2009]

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) (2009) **Status of NIST Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems.** [Online]. Available: http://csrc.nist.gov/groups/SMA/fisma/documents/Status-of-NIST-SP-800-26_v2.pdf [Accessed 12 November 2009]

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) (2010) **NIST SP800-34: Contingency Planning Guide for Federal Information Systems.** [Online]. Available: http://csrc.nist.gov/publications/PubsSPs.html [Accessed 02 August 2010]

NETMEDIA (2008) **Online Booking Systems.** [Online]. Available: http://www.netmedia.co.uk/pages/on-line-booking-systems.htm [Accessed 28 May 2009]

NEWMAN, D. P. AND TITTEL, E. (2003) **Cisco Certified Security Professional CSPFA** Exam Cram 2**.** Indianapolis: Que Publishing

NEWMAN, R. C. (2009) **Computer Security: Protecting Digital Resources.** Sudbury: Jones & Bartlett Publishers

NICASTRO, F. (2006) People, Processes and Technology: A Winning Cmbination In: Tipton, H. F. and Krause, M. (eds). **Information Security Management Handbook (5e).** Boca Raton: Taylor and Francis group

O'DONOVAN, G. (2007) A Board Culture of Corporate Governance. **Corporate Governance International Journal.** 6, 3

OLSON, D. L. AND WU, D. D. (2008) **Enterprise Risk Management.** Toh Tuck Link, Singapore**:**World Scientific

PALABORA (2005) **Palabora Mining Company: Human Resources.** [Online]. Available: http://www.palabora.com/Default.aspx?page=109 [Accessed 28 October 2009]

PALADION (2008) **Manufacturing.** [Online]. Available: http://www.paladion.net/Manufacturing.html [Accessed 02 November 2009]

PAQUET, C. (2009) **Implementing Cisco IOS Network Security (IINS).** Indianapolis: Cisco Press

PARAK, C. (2008) **Getting IT Right at the Mining Workplace.** [Online]. Available: http://www.it-online.co.za/content/view/296303/ [Accessed 17 March 2009]

PAVITT, K. (1984) Sectoral Patterns of Technical Change: Towards a Taxonomy and a Theory. **Research Policy.** 13: 343-373

PELTIER, T., PELTIER, J. AND BLACKLEY, J. (2005) **Information Security Fundamentals.** Boca Raton: CRC Press

PELTIER, T.R. (2002) **Information Security, Policies, Procedures, and Standards.** Boca Raton: CRC Press

PELTIER, T. R. (2001) **Information Security Risk Analysis.** Boca Raton: CRC Press

PETERSON, D. J., LATOURRETTE, T. AND BARTIS, J. T. (2001) **New Forces at Work in Mining: Industry Views Of Critical Technologies.** : Rand Corporation

PFLEEGER, S. L. (2003) **Security in Computing** (3e)**.** Upper Saddle River**:** Prentice Hall

PICCOLI, G. (2008) **Information Systems for Managers: Texts and Cases.** Hoboken : John Wiley & Sons Inc.

PILIOURAS, T. C. M. (2004) **Network Design: Management and Technical Perspectives** (2e)**.** Boca Raton: CRC Press

PINCOCK PERSPECTIVES (2005A) **Data Management in the Minerals Industry (Part 1)** [Online]. Available: http://www.pincock.com/perspectives/Issue-72-DataManagement.pdf [Accessed 19 May 2009]

PINCOCK PERSPECTIVES (2005B) **Data Management in the Minerals Industry (Part 2)** [Online]. Available: http://www.pincock.com/perspectives/Issue-73-DataManagement2.pdf [Accessed 19 May 2009]

PIRONTI, J. P. (2008) **Securing Information Infrastructure:Expert Advice on Evaluating the New Risks and Structuring Your Defenses.** [Online]. Available: http://www.iparchitects.com/wp-content/uploads/Securing-Information-Infrastructure.pdf [Accessed

12 October 2009]

PITT, M. AND GOYAL, S. (2004) Business Continuity Planning As A Facilities Management Tool. **Facilities.** 22, 3/4: 87-99

POLAR INERTIA (2003) **Types of Copper Mines.** [Online]. Available: http://www.polarinertia.com/sept03/cuaz00.htm [Accessed 09 May 2009]

POORE, R. S. (2007) Information Security Governance In: Tipton, H. F. and Krause, M. (eds). **Information Security Management Handbook (6e).** Boca Raton: Taylor and Francis group.

PORTER, M. E. (2008) **On Competition** (2e). Boston: Harvard Business Press

PRAXIOM (2009) **ISO IEC 27001.** [Online]. Available: http://www.praxiom.com/iso-27001-intro.htm [Accessed 10 October 2009]

PRICEWATERHOUSE COOPERS (PWC) (2008) **The Global State of Information Security® 2008: Energy and mining security chiefs have advanced in many—but not all—critical security and privacy arenas.** [Online]. Available: http://www.pwc.com/extweb/insights.nsf/docid/A8659F991CA54234852574DB005CFA9E/$File/Global_Info_Survey_Energy.pdf [Accessed 05 March 2009]

PRICEWATERHOUSE COOPERS (PWC) (2009) **Trial by fire* Protected. But under pressure to perform: Key findings from the 2010 Global State of Information Security Survey® Energy & Mining.** [Online]. Available: http://www.pwc.com/en_GX/gx/information-security-survey/pdf/global_info_survey_energy_2010.pdf [Accessed 25 October 2009]

PURSER, S. (2004) **A Practical Guide to Managing Information Security.** Boston: Artech House

RAKNER, L. (2003) **Political and Economic Liberalisation in Zambia 1991-2001.** Uppsala: Nordic Africa Institute

RAINER R., TURBAN E. AND POTTER R. (2007) **Introduction to Information Systems: Supporting and transforming business.** Hoboken: John Wiley & Sons

RITTINGHOUSE, J., RANSOME, J. (2005) **Business Continuity and Disaster Recovery for InfoSec Managers.** Oxford: Elsevier Digital Press

ROCKWELL (2009) **Security Solutions: Work With Us to Help Mitigate Your Risk.** [Online]. Available: http://www.rockwellautomation.com/solutions/security/

[Accessed 10 August 2010]

ROTHSTEIN, P. J. (2007) **Disaster Recovery Testing: Exercising Your Contingency Plan.** Brookfield: Rothstein Associates

ROZANSKY, I. (2009) **Disaster Recovery & Business Continuity. [Online]. Available:** http://www.apogeestrategies.com/Documents/apogee_crisis_management_wp.pdf [Accessed 19 November 2009]

RUSSELL, D. AND GANGEMI, G. T. (1991) **Computer Security Basics.** Sebastopol: O'Reilly Media

SADGROVE, K. (2005) **The Complete Guide To Business Risk Management** (2e). Hants: Gower Publishing, Ltd

SAMUELLE, T. J. (2008) **Mike Meyers' CompTIA Security+ Certification Passport** (2e)**.** New York: McGraw Hill Professional

SANS (2002) **The Legal System and Ethics in Information Security**. [Online]. Available: http://www.sans.org/reading_room/whitepapers/legal/the_legal_system_and_ethics_in_information_security_54?show=54.php&cat=legal [Accessed 10 November 2009]

SANS 17799-2: (2003) **South African National Standard : Information Security Management Systems - Part 2: Specification with guidance for use**

SAP (2009) **Security - Protecting Your Data – And Your Business.** [Online]. Available: http://www.sap.com/solutions/security/index.epx [Accessed 01 September 2009]

SATENSTEIN, L. (2008) **How the Mining Industry Benefits from ERP Systems** [Online]. Available: http://www.technologyevaluation.com/en/Research/ResearchHighlights/ERP/2008/03/research_notes/TU_ER_LS_03_26_08_14.asp [Accessed 12 May 2009]

SAVAGE, M. (2002) Business Continuity Planning. **Work study.** 51, 5: 254-261

SAWADA, K. (2004) Mining Information and Mining Policy. **Journal of the Mining and Materials Processing Institute of Japan:** 120, 9: 532-534

SCHEIN, E. (2004) **Organizational Culture and Leadership** (3e). San Francisco: John Wiley and Sons

SCHIESSER, R. (2003) — **Eight Key Steps to Business Continuity.** [Online]. Available: icsa.cs.up.ac.za/issa/2003/Publications/Schiesser_EightKeySteps.ppt [Accessed 12 September 2009]

SCHUMACHER, M. (2006) — **Security Patterns Integrating Security & Systems Engineering.** New Delhi: Wiley-India

SCHWALBE, K. (2009) — **Information Technology Project Management** (6e). Boston: Course Technology

SELDON, A. (2009) — You Cannot Use it if it is Gone. **Hi-Tech Security Solutions: The Industry Journal for Security & Business Professionals**. [Online]. Available: http://securitysa.com/article.aspx?pklArticleId=5621&pklCategoryId=106 [Accessed 12 September 2009]

SHELLY, G. B. AND ROSENBLATT, H. J. (2009) — **Systems Analysis and Design** (8e). Boston: Cengage Learning

SHELTON, R. (2009) — **An Integrated Approach to Legacy IT Modernization.** [Online] Available: http://www.acs-inc.com/assets/0/24/818/824/eb1056b2-9058-4170-82cf-696257083213.pdf [Accessed 01 September, 2009]

SHIM, J. K., SIEGEL, J. G (2005) — **The Vest Pocket Guide to Information Technology** (2e)**.** Hoboken: John Wiley and Sons

SIPIOR, J. C. AND WARD, B. T. (2008) — A Framework for Information Security Management Based on Guiding Standards: A United States Perspective. In: Cohen, E. (ed). **Setting Knowledge Free: The Journal of Issues in Informing Science and Information Technology, Volume 5. Santa Rosa**: Informing Science

SLADE, R. (2006) — The Controls Matrix. In: **Tipton, H. F. and Krause, M. (eds). Information Security Management Handbook (5e v3).** Boca Raton: Taylor and Francis group

SODIYA, A. S., ONASHOGA, S. A. AND OLADUNJOYE, B. A. (2007) — Threat Modelling using Fuzzy Logic Paradigm. In: Cohen, E. (ed). **Information and Beyond: Part 1. The Journal of Issues in Informing Science and Information Technology, Volume 4.** Santa Rosa: Informing Science

SRINIVAS, K. AND MALIK, S. A. (2009) — **Business Ethics For Excellence In Action: A View.** Journal of Education Administration and Policy Studies. 1, 2: 23-27

STACEY, T. (2006) **Contingency Planning Best Practices and Program Maturity. In:** In: Tipton, H. F. and Krause, M. (eds). **Information Security Management Handbook (5e).** Boca Raton: Taylor and Francis group

STAIR, R., REYNOLDS, G. AND REYNOLDS, G. W. (2008) **Principles of Information Security** (9e). Boston: Cengage Learning

STAKE, R. E. (1995) **The Art of Case Study Research.** Thousand Oaks: Sage Publications

STANTON, J. (2006) **The Visible Employee: Using Workplace Monitoring and Surveillance to Protect Information Assets--Without Compromising Employee Privacy or Trust.** Medford: Information Today, Inc.

STARKE L. (2002) **Breaking New Ground: Mining, Minerals, and Sustainable Development - The Report of the MMSD Project.** London: Earthscan

STEWART, J. M. (2004) **Security+ Fastpass.** Alameda: Sybex

STEWART, M. J., TITTEL, E., AND CHAPPLE, M. (2005) **CISSP: Certified Information Systems Security Professional: study guide** (3e). Indianapolis: Wiley Publishing, Inc.

SYSOPTIMA (2005) **Functional Modules of ERP Software.** [Online]. Available: http://sysoptima.com/erp/erp_modules.php [Accessed 14 may 2009]

SZYMANSKI, R., SZYMANSKI, D. AND PULSCHEN, D. (1995) **Computers and Information Systems.** Upper Saddle River: Prentice-Hall

TANSER, J. D. (2003) **Simulation of a Slope Stability Radar for Opencast Mining.** [Online]. Available: http://rrsg.uct.ac.za/theses/msc_theses/dtanser_thesis.pdf [Accessed 02 June 2009]

TARANTINO, A. (2008) **Governance, Risk, and Compliance Handbook: Technology, Finance, Environmental, and International Guidance and Best Practices.** Hoboken: John Wiley and Sons

TAYLOR, M. (2008) **Continuity Strategy – The Global View.** [Online]. Available: http://www.thebci.org/articlesept2007.pdf

[Accessed 04 March 2009]

TCHANKOVA, L. (2002) Risk Identification – Basic Stage in Risk Management. **Environmental Management and Health.** 13, 3: 290-297

TESELEANU, G., MAGHEAR, T., AND ANDRAS, A. (2006) **The Need for Innovation and Technology Transfer in Mineral Industry.** [Online]. Available: http://opi4.opi.org.pl/repository/41fa6dc088dd71307f6cbcd93a3ca1b6Ot9EO9.pdf [Accessed 06 May 2009]

THOMSON, K. AND VON SOLMS, R. (2004) Towards Corporate Information Security Obedience. In: Deswarte, Y., Cuppens, F., Jajodia, S. and Wang, L. (eds). **Information Security Management, Education And Privacy.** Norwell: Kluwer Academic Publishers

THOMPSON, M. (2006) **Business Continuity Management: The Nine Deadly Sins.** [Online]. Available: http://www.continuitycentral.com/feature0320.htm [Accessed 04 September, 2009]

THORLEY, U. AND BLACKWELL, G. (2009) **Geographic Information Systems for Mine Development.** [Online]. Available: http://www.accessscience.com/content.aspx?id=YB090001 [Accessed 13 May 2009]

THURAISINGHA M, B. M. (1997) **Data management systems: evolution and interoperation.** Boca Raton: CRC Press

TILLEY, K. (1995) Work Area Recovery Planning: The Key to Corporate Survival. **Facilities.** 13, 9/10: 49–53

TIPPETT, P. (2007) Computer Ethics. In: Tipton, H. F. and Krause, M. (eds). **Information Security Management Handbook (6e).** Boca Raton: Taylor and Francis group.

TOMLINSON, R. F. (2007) **Thinking About GIS: Geographic Information System Planning For Managers (3e).** Redlands: ESRI, Inc.

TREGEAR, J. (2001) Risk Assessment. **Information Security Technical Report.** 6, 3: 19-27

TUDOR, K. J. (2006) **Information Security Architecture: An Integrated Approach to Security in the Organization** (2e). Boca Raton: CRC Press

TURBAN, E., MCLEAN E., WETHERBE J., BOLLOJU N. AND DAVISON R. (2002) **Information Technology for Management:** Transforming Business in the Digital Economy**. New York:** John Wiley and Sons

TUSUBIRA, F. F. AND MULIRA, N. (2004) **Integration of ICT in Organisations: Challenges and Best Practice Recommendations Based on the Experience of Makerere University and Other Organizations.** [Online]. Available: http://www.fftusubira.com/publications/Integration_of_ict.pdf [Accessed 29 November 2009]

UPFOLD, C. (2005) **An Investigation of Information Security in Small and Medium Enterprises (SME's).** Unpublished MCom Thesis. Grahamstown: Rhodes University

UPSTILL, G. AND HALL, P. (2007) Innovation in the Minerals Industry: Australia in a Global Context. **Resources Policy**. 31, 3: 137-145

VALLABHANENI, R. (2008) **Corporate Management, Governance, and Ethics Best Practices.** Hoboken: John Wiley and Sons

VAN HOLSBECK, M. AND JOHNSON, J. Z. (2004) **Security in an ERP World.** [Online]. Available: http://www.net-security.org/article.php?id=691 [Accessed 21 June 2009]

VANCOPPENOLL E, G. (2008) What Are We Planning For? In: Hiles, A. (ed). **The Definitive Handbook of Business Continuity Management.** Chichester: John Wiley & Sons

VASUDEVAN, V. (2008) **Application Security in the ISO27001 Environment.** Ely: IT Governance

VELLANI, K. H. (2006) **Strategic Security Management: A Risk Assessment Guide for Decision Makers.** Burlington: Butterworth- Heinemann

VON SOLMS, B. AND VON SOLMS, R. (2004) The 10 Deadly Sins of Information Security Management. **Computers & Security.** 23: 371-376

VON SOLMS, R. AND VON SOLMS, S. H. (2009) **Information Security Governance.** New York: Springer

VON SOLMS, R. AND VON SOLMS, S. H. (2006) Information Security Governance: A model based on the Direct–Control Cycle. **Computers & Security**. 25, 6: 408-412

VON SOLMS, R. (1999) Information Security Management: Why Standards are Important. **Information Management and Computer Security.** 7,1: 50-57

VON SOLMS, S. H. AND HERTENBERGER, M. P. (2005) — ERPSEC - A Reference Framework to Enhance Security in ERP Systems. **IFIP Advances in Information and Communication Technology.** 181: 79-94

WAGNER, H. AND FETTWEIS, G. B. L. (2001) — About Science and Technology in the Field of Mining in the Western World at the Beginning of the New Century. **Resources Policy**. 27, 3: 157-168

WANG, G. (2005) — **Strategies and Influence for Information Security.** [Online]. Available: http://www.isaca.org/Template.cfm?Section=Home&Template=/ContentManagement/ContentDisplay.cfm&ContentID=23548 [Accessed 28 October 2009]

WANG, S. X. AND TARATORIN, A. M. (1999) — **Magnetic Information Storage Technology.** San Diego: Academic Press

WARNER, D. (2007) — **Disaster Recovery Solutions for Business Continuity within the Manufacturing Industry.** [Online]. Available: http://www.plasticsbusinessmag.com/wp/?p=35 [Accessed 13 September 2009]

WARD, P. AND DAFOULAS, G. (2006) — **Database Management Systems.** Boston: Cengage Learning EMEA

WELANDER, P. (2007) — **10 Control System Security Threats.** [Online]. Available: http://www.controleng.com/article/269570-10_Control_System_Security_Threats.php **[Accessed 10 August 2009]**

WELANDER, P. (2009) — **Securing Legacy Control Systems.** [Online]. Available: http://www.controleng.com/index.php?id=483&cHash=081010&tx_ttnews[tt_news]=866 [Accessed 10 October 2009]

WELMAN, C., KRUGER, F. AND MITCHELL, B. (2005) — **Research Methodology** (3e). Cape Town: Oxford University Press Southern Africa

WESSELS, P. L., GROBBELAAR, E., MC GEE, A. AND PRINSLOO, G.T.M. (2007) — **Information Systems in a Business Environment** (4e). Durban: Lexis Nexis

WHITMAN, M. E. AND MATTORD, H. J. (2010) **Management of Information Security** (3e). Boston: Thomson Course Technology

WHITMAN, M. E. AND MATTORD, H. J. (2004) **Management of Information Security**. Boston: Thomson Course Technology

WHITMAN, M. E. AND MATTORD, H. J.(2009) **Principles of Information Security** (3e). Boston: Course Technology

WILLIAMS, P. A. (2001) Information Security Governance. **Information Security Technical Report**. 6, 3: 60-70

WORLD INTELLECTUAL PROPERTY ORGANISATION (WIPO) (2009) **What is WIPO?** [Online]. Available: http://www.wipo.int/about-wipo/en/what_is_wipo.html [Accessed 25 October 2009]

WORLD BANK, THE (1992) **Strategy for African Mining.** Washington, D.C.: World Bank Publications

WORLD HEALTH ORGANISATION (WHO) (2009) **Pandemic Influenza Preparedness and Response.** Geneva: World Health Organisation

WORLD STONEX (2006) **Information Technology In Mining Industry.** [Online]. Available: http://www.worldstonex.com/en/InfoItem.asp?ICat=2&ArticleID=251 [Accessed 01 April 2009]

YACHIR, F. (1988) **Mining in Africa Today: Strategies and Prospects.** Avon: United Nations University Press

YAKOVLEVA, N. (2005) Corporate Social Responsibility In The Mining Industries**.** Aldershot: Ashgate Publishing

YIN, R. (2003) **Case Study Research: Design and Methods.** Thousand Oaks: SAGE

ZHANG, R. (2009) **Steps for Achieving Proper Mobile Security Governance** [Online]. Available: http://www.computerworld.com/s/article/9133117/Steps_for_Achieving_Proper_Mobile_Security_Governance?taxonomyId=&intsrc=kc_feat&taxonomyName= [Accessed 19 October 2009]

ZHANG, R., XIE, H., ZHAO, S., LIU, Z., WANG, S., LIU, A Decision Support System Of Open Pit Mining And Its Application. In: **Computer Applications In The Minerals Industries. Xie, H., Wang, Y. and Jiang, Y. (eds).** Lisse: Swets and

A., WANG, C. AND ZHANG, G. (2001) Zeitlinger

ZELKOWITZ, M.V. (1997) **Advances in Computers.** Orlando: Academic Press

ZOUFALY, F. (2009) **Issues and Challenges Facing Legacy Systems.** [Online]. Available: http://www.developer.com/mgmt/article.php/11085_1492531_1 [Accessed 01 September 2009]

Appendix A

Leadership Perception Questionnaire - Part A

Appendix A

Information Security Practices in Zambian Mining Organisations

Dear Respondent,

The following questionnaire is part of an MSc. Information Systems dissertation on Information Security practices in Zambian copper mining organisations. The purpose of this questionnaire is to explore leadership perceptions surrounding Information Security practices in these mining organisations. It is intended for completion by a member of the board of directors or by a senior management position holder within the organisation. Please indicate your response by placing a tick (✓) in the appropriate column and provide comments where necessary.

1. The organisation's Information Security governance framework:

(Please indicate the **existence**, YES, NO or PARTIAL of each information security governance pillar listed below by placing a tick (✓) in the appropriate column).

Information Security Governance Pillars	**Yes**	**No**	**Partial**
Information Security Policies			
Ethics (privacy, accuracy, property and accessibility)			
Accountability and Responsibility for information security (by board of directors and senior executives)			
Information Security Risk Management			
Employee Education, Training, and Awareness			
Information Sharing (with other organisations and regulatory bodies)			
Information Security Resource Allocation			
Best Practice Information Security Standards (e.g. ISO 27002, ITIL, COBIT)			
Compliance with legal requirements			

Comments:……..……

……...……

…….....

2. Information Security Policy

2.1 The organisation has an Information Security Policy

Yes	No	Partial

(If response to question 2.1 is NO, please skip to Question 3)

2.2 The organisation's Information Security policy adequately caters for organisational security requirements, business objectives and changing business requirements.

(Please indicate with a tick (✓) in the appropriate column, the level of adequacy of the information security policy.

	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Information Security Requirements					
Business Objectives					
Business Requirements					

Comments:……..….....

.....……

…..…….....

3. Information security is integrated into employment policies and practices.

Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree

Comments:……

……

……

4. **The organisation adheres to all information security regulatory requirements.**

Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree

Comments:……

……

…….....

5. **Organisational information is disclosed and/or disseminated only to the appropriate stakeholders.**

(Stakeholders include shareholders, customers, employees, financial institutions, communities, media, government, etc)

Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree

Comments:……

……

……

6. **We have established an enterprise-wide Business Continuity planning process in which our organisation's information security requirements are catered for.**

Appendix A

Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree

Comments:……

……

……

THANK YOU!!

Appendix B

Leadership Perception Questionnaire - Part B

Appendix B

Information Security Practices in Zambian Mining Organisations

Dear Respondent,

The following questionnaire is part of an MSc. Information Systems dissertation on Information Security practices in Zambian copper mining organisations The purpose of this questionnaire is to explore leadership perceptions surrounding Information Security practices in these mining organisations. It is intended for completion by the overall Head of Information Technology. Please indicate your response by placing a tick (✓) in the appropriate column and provide comments where necessary.

1. Formal information security procedures that cater for all information system processes have been established.

Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree

Comments:……
……
…….....

2. Legacy systems receive the appropriate level of protection as other systems.

Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree

Comments:……
……
…….....

3. Cultural clashes exist between younger and older IT staff over legacy and modern systems.

(Younger IT staff have been trained on modern systems which creates a gap for the support of legacy systems).

Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree

Comments:……

……

…….....

4. Software patches are regularly applied, thereby improving information security and eliminating security weaknesses.

Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree

Comments:……

……

……

5. Formal change management procedures have been established to control changes to information systems.

Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree

Comments:……

……

……

6. Measures have been put in place to protect information processing equipment from environmental threats.

Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree

Comments:……

……

……

7. Information systems are protected from accidental or deliberate human error.

(e.g. social engineering)

Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree

Comments:……

……

……

8. Crisis management procedures have been clearly defined.

Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree

Comments:……

……

…….....

9. All staff are given adequate and appropriate information security education, training and awareness.

Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree

Comments:……

……

……

10. All assets used for information processing can be identified and located.

Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree

Comments:……

……

……

11. Adequate electronic mail management policies and procedures have been implemented.

Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree

Comments:……

……

…….....

12. Electronic communication has been protected against both external and internal threats. (Threats include viruses, spam, phishing, etc)

Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree

Comments:……

……

……

13. Information security incident reporting responsibilities and channels have been defined.

Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree

Comments:……

……

…….....

14. Information security requirements are emphasised during the procurement and development of application software.

Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree

Comments:……

……

……

15. Adequate access control procedures have been established and they meet the organisation's security requirements. (Access control includes physical and logical access controls)

(Please indicate with a tick (✓**)** the current state of access control procedures)

	Yes	**No**	**Partial**
Access control procedures have been established			
Access control procedures meet the organisation's security requirements			

Comments:……

……

……

16. Mobile security governance measures have been put in place to address mobile computing and communications.

Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree

Comments:……

……

……

17. We have detailed Business Continuity Plans (BCPs) in place, which specify the actions to be taken to keep the organisation functioning in the event of a disaster.

Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree

Comments:……

……

……

18. All organisational data and information has been consolidated and can be accounted for.

Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree

Comments:……

……

……

19. Policies and procedures that cater for control systems are in place.

Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree

Comments:……

……

……

20. Contingency plans to deal with systems failures have been established and are regularly tested and reviewed.

(These plans include business impact analyses, incident response plans, disaster recovery plans, and business continuity plans)

Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree

Comments:……

……

……

21. Information security risks are regularly assessed and managed.

Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree

Comments:……

……

……

22. User access privileges to all systems are restricted and controlled.

Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree

Comments:……

……

……

THANK YOU!!

Appendix C

Praxiom ISO/IEC 27002 Information Security Audit Tool

Questionnaire 1 of 11

Appendix C

5.1 ESTABLISH AN INFORMATION SECURITY POLICY						
1	**GOAL**	Have you established an information security policy?	YES	NO	N/A	
2	**GOAL**	Does your information security policy provide clear direction for your information security program?	YES	NO	N/A	
3	**GOAL**	Does your information security policy show that your management is committed to information security?	YES	NO	N/A	
4	**GOAL**	Does your management support your organization's information security policy?	YES	NO	N/A	
5	**GOAL**	Does your information security policy show that your management is prepared to support an ongoing commitment to information security?	YES	NO	N/A	
6	**GOAL**	Is your information security policy consistent with your organization's business objectives?	YES	NO	N/A	
7	**GOAL**	Does your information security policy meet your organization's business requirements?	YES	NO	N/A	
8	**GOAL**	Does your information security policy comply with all relevant laws and regulations?	YES	NO	N/A	
5.1.1 DEVELOP AN INFORMATION SECURITY POLICY DOCUMENT						
9	**CTRL**	Did you document your information security policy?	YES	NO	N/A	
10	**CTRL**	Has your information security policy document been formally approved by your management?	YES	NO	N/A	
11	**CTRL**	Do you communicate your security policy to all employees?	YES	NO	N/A	
12	**CTRL**	Do you communicate your policy to relevant external parties?	YES	NO	N/A	
13	GUIDE	Are your organization's information security policy communications easy for users to understand?	YES	NO	N/A	
14	GUIDE	Are your security policy communications relevant to your users' needs and expectations?	YES	NO	N/A	
15	GUIDE	Does your security policy document state that your management is committed to information security?	YES	NO	N/A	
16	GUIDE	Does your policy document state that your management supports your organization's information security goals and principles?	YES	NO	N/A	
17	GUIDE	Is your statement of support for information security consistent with your organization's business strategy and objectives?	YES	NO	N/A	

18	GUIDE	Does your security policy document provide a definition of information security?	YES	NO	N/A	
19	GUIDE	Does your policy document clarify the scope of your organization's commitment to information security?	YES	NO	N/A	
20	GUIDE	Does your information policy document define your organization's information security objectives?	YES	NO	N/A	
21	GUIDE	Does your information policy document explain how your organization's information security program will facilitate information sharing?	YES	NO	N/A	
22	GUIDE	Does your information security policy document describe your organization's approach to the management of information security?	YES	NO	N/A	
23	GUIDE	Does your information security policy document describe a framework that you can use to establish your organization's security objectives and controls?	YES	NO	N/A	
24	GUIDE	Does your information security policy document describe your organization's general approach to risk assessment and risk management?	YES	NO	N/A	
25	GUIDE	Does your information security policy document briefly explain the information security policies that are especially important to your organization?	YES	NO	N/A	
26	GUIDE	Does your information security policy document briefly explain the information security principles that are especially important to your organization?	YES	NO	N/A	
27	GUIDE	Does your information security policy document briefly explain the information security standards that are especially important to your organization?	YES	NO	N/A	
28	GUIDE	Does your information security policy document briefly explain the information security compliance requirements that are especially important to your organization?	YES	NO	N/A	
29	GUIDE	Does your information security policy briefly explain the legislative compliance requirements that are especially important to your organization?	YES	NO	N/A	
30	GUIDE	Does your information security policy explain the regulatory compliance requirements that are especially important to your organization?	YES	NO	N/A	
31	GUIDE	Does your information security policy explain the contractual compliance requirements that are especially important to your organization?	YES	NO	N/A	
32	GUIDE	Does your information security policy explain	YES	NO	N/A	

		the educational requirements that are especially important to your organization?				
33	GUIDE	Does your information security policy explain the security training requirements that are especially important to your organization?	YES	NO	N/A	
34	GUIDE	Does your information security policy explain the security awareness requirements that are especially important to your organization?	YES	NO	N/A	
35	GUIDE	Does your information security policy explain the business continuity management requirements that are especially important to your organization?	YES	NO	N/A	
36	GUIDE	Does your information security policy document explain what could happen if your information security policy is violated or ignored?	YES	NO	N/A	
37	GUIDE	Does your information security policy document define both general and specific information security management responsibilities?	YES	NO	N/A	
38	GUIDE	Does your security policy define information security incident reporting responsibilities?	YES	NO	N/A	
39	GUIDE	Does your security policy refer to other documents that support your information security policy?	YES	NO	N/A	
40	GUIDE	Does your security policy document refer to other more detailed security policies and procedures for specific information systems?	YES	NO	N/A	
41	GUIDE	Does your security policy document refer to security rules that all users should comply with?	YES	NO	N/A	
42	NOTE	Did you create a standalone information security policy document or make it part of a larger general policy document?	YES	NO	N/A	
43	NOTE	Have you ensured that you don't accidentally disclose sensitive information if you distribute your security policy document to persons outside of your organization?	YES	NO	N/A	
5.1.2 REVIEW YOUR INFORMATION SECURITY POLICY						
44	**CTRL**	Do you carry out information security policy reviews?	YES	NO	N/A	
45	**CTRL**	Do you carry out security policy reviews at planned intervals?	YES	NO	N/A	
46	**CTRL**	Do you carry out a security policy review whenever your organization's security risks change?	YES	NO	N/A	
47	**CTRL**	Do your security policy reviews evaluate the ongoing suitability of your information security policy?	YES	NO	N/A	

48	CTRL	Do your security policy reviews evaluate the ongoing adequacy of your information security policy?	YES	NO	N/A	
49	CTRL	Do your security policy reviews evaluate the ongoing effectiveness of your information security policy?	YES	NO	N/A	
50	GUIDE	Do your security policy reviews examine opportunities to improve your information security policy?	YES	NO	N/A	
51	GUIDE	Do your security policy reviews examine opportunities to improve your organization's approach to information security?	YES	NO	N/A	
52	GUIDE	Do your security policy reviews assess the impact that changes in your organizational environment have on your organization's information security policy?	YES	NO	N/A	
53	GUIDE	Do your security policy reviews assess the impact that changes in your technical environment have on your organization's information security policy?	YES	NO	N/A	
54	GUIDE	Do your security policy reviews assess the impact that changes in your organization's business circumstances have on your information security policy?	YES	NO	N/A	
55	GUIDE	Do your security policy reviews assess the impact that changes in your organization's legal conditions have on your information security policy?	YES	NO	N/A	
56	GUIDE	Have you clarified who owns your information security policy?	YES	NO	N/A	
57	GUIDE	Is your security policy owner responsible for the development of your information security policy?	YES	NO	N/A	
58	GUIDE	Is your security policy owner responsible for the review of your information security policy?	YES	NO	N/A	
59	GUIDE	Is your security policy owner responsible for the evaluation of your information security policy?	YES	NO	N/A	
60	GUIDE	Have you defined a *management review* procedure to evaluate your organization's information security policy?	YES	NO	N/A	
61	GUIDE	Have you established a security policy review schedule?	YES	NO	N/A	
62	GUIDE	Have you identified *inputs* that your security policy owner can use to review your information security policy?	YES	NO	N/A	
63	GUIDE	Do you examine feedback (input) from interested parties that can be used to review your information security policy?	YES	NO	N/A	
64	GUIDE	Do you examine results (inputs) of independent reviews?	YES	NO	N/A	
65	GUIDE	Do you examine status (inputs) of preventive actions?	YES	NO	N/A	
66	GUIDE	Do you examine status (inputs) of corrective actions?	YES	NO	N/A	

67	GUIDE	Do you examine the results (inputs) of previous reviews?	YES	NO	N/A	
68	GUIDE	Do you examine security policy compliance data (inputs)?	YES	NO	N/A	
69	GUIDE	Do you examine changes (inputs) that could affect how your organization manages information security?	YES	NO	N/A	
70	GUIDE	Do you examine changes (inputs) to your organization's environment and do you evaluate how these changes influence your approach to information security?	YES	NO	N/A	
71	GUIDE	Do you examine changes (inputs) to your organization's contractual environment and do you evaluate how these changes influence your approach to information security?	YES	NO	N/A	
72	GUIDE	Do you examine changes (inputs) to your organization's regulatory environment and do you evaluate how these changes influence your approach to information security?	YES	NO	N/A	
73	GUIDE	Do you examine changes (inputs) to your organization's legal environment and do you evaluate how these changes influence your approach to information security?	YES	NO	N/A	
74	GUIDE	Do you examine changes (inputs) to your organization's technical environment and do you evaluate how these changes influence your approach to information security?	YES	NO	N/A	
75	GUIDE	Do you examine changes (inputs) to your organization's business circumstances and do you evaluate how these changes influence your approach to information security?	YES	NO	N/A	
76	GUIDE	Do you examine changes (inputs) to your organization's resource availability and do you evaluate how these changes influence your approach to information security?	YES	NO	N/A	
77	GUIDE	Do you examine threat trends (inputs) that could influence your organization's approach to information security?	YES	NO	N/A	
78	GUIDE	Do you examine vulnerabilities (inputs) that could influence your organization's approach to information security?	YES	NO	N/A	
79	GUIDE	Do you examine reported information security incidents (inputs) that could influence your approach to security?	YES	NO	N/A	
80	GUIDE	Do you examine recommendations (inputs), made by relevant authorities, that could influence your approach to information security?	YES	NO	N/A	
81	GUIDE	Have you identified *outputs* that your information security *management reviews* should generate?	YES	NO	N/A	
82	GUIDE	Do your information security management reviews generate decisions and actions (outputs)?	YES	NO	N/A	
83	GUIDE	Do you generate decisions and actions that will improve	YES	NO	N/A	

		your approach to managing information security?				
84	GUIDE	Do you generate decisions and actions that will improve your information security management processes?	YES	NO	N/A	
85	GUIDE	Do you generate decisions and actions that will improve your organization's information security control objectives?	YES	NO	N/A	
86	GUIDE	Do you generate decisions and actions that will improve your organization's information security controls?	YES	NO	N/A	
87	GUIDE	Do you generate decisions and actions that will improve the allocation of your organization's resources?	YES	NO	N/A	
88	GUIDE	Do you generate decisions and actions that will improve the allocation of your organization's responsibilities?	YES	NO	N/A	
89	GUIDE	Do you maintain a record of your organization's information security management reviews?	YES	NO	N/A	
90	GUIDE	Do all information security policy revisions receive management approval?	YES	NO	N/A	

Answer each of the above questions. Three answers are possible: YES, NO, and N/A. YES means you're in compliance, NO means you're not in compliance, while N/A means that the question is not applicable in your case. YES answers and N/A answers require no further action, while NO answers point to security practices that need to be implemented and actions that need to be taken. Also, please use the column on the right to record your notes and comments.

In the spaces below, enter the name and location of your organization, who completed this page, who reviewed it, and the dates.