Information Security Management in a Human Resource Information System of a Selected University of Technology

by

Jerry Bature Ansen
Registration Number: 209251042

SUBMITTED TO

THE FACULTY OF BUSINESS

IN PARTIAL FULFILMENT OF THE REQUIREMENTS

FOR THE DEGREE OF

MASTER OF TECHNOLOGY IN BUSINESS INFORMATION SYSTEMS

AT THE

CAPE PENINSULA UNIVERSITY OF TECHNOLOGY OF SOUTH AFRICA

Supervisor: Michael Twum-Darko (PhD)

April 2014

DECLARATION

I, Jerry Bature Ansen, declare that the contents of this dissertation/thesis represent my own unaided work, and that the dissertation/thesis has not previously been submitted for academic examination towards any qualification. Furthermore, it represents my own opinions and not necessarily those of the Cape Peninsula University of Technology.

Signed **Date**

28th April, 2014

ABSTRACT

The study aimed to determine the information security management challenges in information systems (IS). The human resources department (HRD) of a selected university of technology (UoT) was used as a case study to investigate employee appointment processes data and its security management challenges. The unit of study was the human resource infomation system (HRIS) as a form of IS. An interpretive case-study approach and questionnaires were employed to support data gathering. Information gathered and managed by HRD during and after an employee's appointment is vital to the institution. The rationale for this study therefore eminated from ongoing concerns in respect of ineffective information security in organisations, resulting in substantial losses. From the literature reviewed a conceptual framework was developed and used to guide the data analysis and interpretation of data. The research findings were further used to validate the conceptual framework. This was done to create a general framework, whereby the conclusions and recommendations from the data analysis and information security practices could enhance information security management in human resource systems at a university of technology.

ACKNOWLEDGEMENTS

I would like to thank God for His grace during the study as well as my supervisor, Dr Michael Twum-Darko (Graduate Centre for Management at the Cape Peninsula University of Technology), for his time, guidance, insight and encouragement, without which this dissertation would not have been possible. In addition, I would like to thank my family for their constant support and encouragement.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

APPENDICES

CHAPTER 1: INTRODUCTION

1.1 Background

Securing and managing information systems are crucially important in information-intensive organisations such as universities of technology, as contended by Herath and Rao (2009). Most organisations have long been using information security technologies to safeguard their information assets, but technological devices are insufficient in today's business environment. Herath and Rao (2009) note, "in terms of information security, observing end-user security behaviors is very challenging".

Experience teaches that where there is no proper information security governance implemented, employee data is at risk. Data circulation within a university of technology to active employees and those leaving the organisation raises concerns of information security. One hears of employees who have left their employment and are still paid wages or salaries, and have continued access to their email. The researcher therefore asked questions: Who is responsible for communicating employee information status to key stakeholders? Where are the vulnerabilities for information security management within a university of technology?

Data and information have and will continue to be seen as extremely important assets in today's business environment. Recognizing this, organisations must properly protect and secure these assests (Viljoen, 2008). Unauthorised access to confidential data or information has cost companies and individuals their reputation and good will. Human resource management is a unit within an organisational structure where employees are recruited and their vital information is managed. Failure to secure and prevent unauthorised access by intruders can cost a university and its employees their reputation. As such, a university of technology (UoT) HR department's information systems was selected as the field of study.

Tertiary education institutions in South Africa, especially the former technikons, have undergone developmental phases both administratively and academically, and are still in the process of integrating all their administrative business processes. The Cape Peninsula University of Technology (CPUT) website indicates that "in March 2001, the South Africa minister of education, Kader Asmal, announced the National Plan on Higher Education to change the higher education landscape". In line with the Department of Education's guidelines for mergers and incorporations, "in October 2003 the Minister approved the address and new name, Cape Peninsula University of Technology", and today the institution

is known by its new name, with six geographically dispersed campuses. The human resources department has been integrated and raises the question "how secure is personal data gathered and maintained in the process of employment and terminating employee contracts by the department (CPUT, 2012).

1.2 Terminology used

To avoid any misunderstanding, the terminology used by the researcher is briefly defined below.

Information security: According to Paul Dorey, information security "provides the management processes, technology and assurance to allow business management to ensure business transactions can be trusted; ensure IT services are usable and can appropriately resist and recover from failure due to error, deliberate attacks or disaster; and to ensure critical confidential information is withheld from those who should not have access to it" (IT Governance Institute, 2001).

Information Security policy: For the purpose of this study, this is defined as a document that outlines the rules, laws and practices for computer network access. This document regulates how an organisation will manage, protect and distribute its sensitive information (both corporate and client information) and lays the framework for the computer-network-oriented security of the organisation (Ngobeni and Grobler, 2009:3).

Data protection: Bradley (2013) defines it as "safeguarding of important data from destruction, alteration, or loss. Data protection is achieved through a combination of technology, business processes, and best practices. Core components of a data protection strategy are backup and recovery, remote data movement, storage system security, and Information Lifecycle Management". A business dictionary (2014) also defines data protection as the "use of techniques such as file locking and record locking, database shadowing, disk mirroring, to ensure the availabitity and integrity of the data".

Information leakage: According to the Information Security Forum (ISF) 2007, this "is a loosely defined term used to describe an incident where the confidentiality of information has been compromised, typically as the result of unintentional insider action". Today's

information technology devices, such as portable flash drives, email attachments and cloud computing, make organisations vulnerable to the leaking of vital information.

Personal information: Duggan (2012) explains that this is the "information relating to an identifiable, living, natural person, or an identifiable, existing juristic person. In broad terms, personal information relates to: race, gender, sexual orientation, marital status, etc., medical, financial or criminal history; identifying numbers; contact details; biometric information; personal opinions; private or confidential communications; the views or opinions of others about the person; and the name of the person, in cases where the disclosure of this might reveal information about the person".

Users: In this study, users are defined as the individuals who have authorised access to organisational data. Examples of users are employees, medical aid schemes, pension organisations, and consultants.

Data: A given or fact, which can be a number, statement, or picture. Data in this study refers to the facts collected and stored in a database of a university of technology regarding employees and external partners. The data serves as a base for processing information in an organisation (Business Dictionary, 2014).

Information: quoting from a business dictionary (2014): "information is data that is (1) accurate and timely, (2) specific and organized for a purpose, (3) presented within a context that gives it meaning and relevance, and (4) can lead to an increase in understanding and decrease in uncertainty. Information is valuable because it can affect behavior, a decision, or an outcome. For example, if a manager is told his/her company's net profit decreased in the past month, he/she may use this information as a reason to cut financial spending for the next month. A piece of information is considered valueless if, after receiving it, things remain unchanged".

1.3 Research rationale

The rationale for this study is that users and executive management within a university of technology generally believe that information security is in fact the primary responsibility of the IT experts; however, it should be the responsibility of all indivituals who have access to the organisational data. Viljoen (2008:2) argues that, "every member of the organisation plays a role and shares responsibility for the organisation's information security". This is especially true for managers who are responsible for directing and controlling the assets for which they are answerable. If every member of an organisation is to share responsibility for information security, it follows that every person, and especially managers in the organisation, should have access to relevant management information about that organisation's information security.

This study investigated information security management challenges in the HRIS and data surrounding employees' appointment processes. The study looked at the impact of factors such as personnel information, data protection and compliance with security policy, and information security awareness, in particular during employee appointment and employee termination from the organisation. The motivation for this study comes from the ongoing concern of ineffective information security management in organizations and the issue of information security responsibility problem within organizations resulting in substantial losses.

The main goal of the study was to investigate and identify the vulnerability of data collection, data processes, data access, and data usage, and to recommend information security management standards in terms of:

- protection of organisational records
- information security awareness, education, and training
- technical vulnerability management, and
- management of information security incidents and improvements

The results obtained from the analysis were compiled into a recommendation (see Section 5.3) to minimise the threats that user behaviour poses to the protection of information assets.

1.4 Problem statement

Information insecurity has escalated considerably over recent years and has become a very serious problem that costs governments, organisations and general computer users significant losses annually (Viljoen, 2008). But how do universities of technology manage the challenges and vulnerabilities of information assets in respect of information security? The objective of the research was to investigate and determine the vulnerabilities of data collection, data processes, data access and data usage of personnel information by HRIS in higher education in South Africa through a case study. A university of technology human resources department was used as the unit of study.

1.5 Research questions

The main research question for the study is;

What are the challenges of information security management and vulnerabilities in the human resource information system in respect of employees' data management at a university of technology?

The following research sub-questions were considered to answer the main research question:

a) What knowledge of information security management policies and regulations do human resource personnel have?
b) What are the information security awareness, education and training programmes available for the human resource personnel?
c) How is data being properly managed within the human resource department?

1.6 Delimitation of research

The focus of the study was on a selected university of technology. The human resources department was used as a case study where the unit of study was the human resource system for the fieldwork. The research focused on information security practices such as: protection of organisational records; information security awareness, education, and training; technical vulnerability management; and management of information security incidents. The study did not consider technical information security in respect of access controls, password protection, and encryption.

1.7 Ethical considerations

All data collected during the research were treated confidentially and the anonymity of the respondents was ensured. Respondents were not required to provide any personal details. A covering letter accompanied the instrument, and the purpose of the research was explained. Respondents' views were respected and they were given the option not to respond if they so wished. The ethical statement was a commitment by the researcher to comply with ethical standards and was observed in accordance with the university protocols.

1.8 Research contribution

The research outcome, as proposed seek to recommend a better practice of information security management within the human resources departments to empower individuals who are responsible for data and information management in a university of technology. It is also envisaged that the outcomes will ensure that every university of technology users shares the responsibility for information security. Human resource managers in a University of Technology should have access to relevant management information about that organisation's information security.

1.9 Dissertation overview

The dissertation consists of five chapters, and these chapters are briefly described as follows:

Chapter 1: Introduction

Introduces the dissertation by describing the background of the research, terminology used, and the research rationale. The research problem, research questions, and objectives of the research are further outlined, and the research methodology, scope of the research, and an overview of the research layout are given.

Chapter 2: Literature review

The chapter introduces the relevant literature and the purpose of information security, governance and factors affecting information security in a university of technology. A conceptual framework was developed based on the literature reviewed and was used to guide the data collection and analysis. The chapter further examines literature with regard to information security and the standards that govern information security. In this chapter, the functions of information security in organisations were discussed.

Chapter 3: Research approach

The chapter introduces the methodologies considered for the study and discusses the underpinning philosophy. It further introduces the University of Technology chosen for the fieldwork in the case study used for the research.

Chapter 4: Analysis and interpretation of data

This chapter analyses and interprets data collected through the interviews and questionnaires and discusses possible solutions in respect of the findings. The findings are used to propose a general framework to help govern institutional critical data and to recommend information security practices.

Chapter 5: Recommendations and conclusions

This chapter provides a summary of the research findings, possible recommendations for information security practices, and outlines further studies in terms of future work, as well as conclusions.

CHAPTER 2: LITERATURE REVIEW

2.1 Introduction

Information Security Governance 2004 acknowledges that, "a university of technology does encounter issues of risk, liability, business stability, costs, and national repercussions as universities increasingly move their core activities to the Internet". ISACA (2005) states that information security can be many things to an organisation, since it is the gatekeeper to an enterprise's information assets.

Information assets such as data, information and software have become important assets to an organisation, and improper protection, as noted by Von Solms and Von Solms (2005:1) "could have profound business and legal implications". Von Solms and Von Solms further contend that, "the scope of information security is much wider than just (directly) protecting the data, information and software of a business" (Von Solms and Von Solms, 2005:1). It is therefore arguable that information security is the responsibility of executive management, while executive management sees it as the duty of the security officer in the organisation. To better understand information security management in a university of technology, it was vital to understand what information security entails, and therefore the following areas – information security policy and regulation, human resource systems and infrastructure, and users were reviewed.

2.2 Information security policy and regulation

Herath and Rao (2009: 1) argue that, "although most organizations have long been using information security technologies, it is well known that technology tools alone are not sufficient". Thus, the area of end-user security attitude in organizations has drawn an attention of information security vulnerabilities that this research also intends to validate. Herath and Rao (2009:1) further argue that, observing end-user security behaviours is challenging. However, one should be mindful of Viljoen's (2008:13) argument that, "information security is not the sole responsibility of security experts with technical confidence". Viljoen further argues that every member of the organisation plays a role and shares responsibility for the organisation's information security. If every member of an organisation is to share responsibility for

information security, it should be possible for an organisation to manage its information security (Viljoen, 2008).

According to Herath and Rao (2009:2), “the objective of any organizational policy is to influence and determine employees' course of action. While the defined policies may be crystal clear and detailed, the result may not turn out to be as desired, especially with regard to information security”. Information security governance is and continues to be the responsibility of executive management and each stakeholder within the organisation. The question remains whether this responsibility is exercised, as it should be. As highlighted by Armoni (2002:1), “every organization should be concerned about protecting data against intruders, for the organization's ability to survive depends on the availability, comprehensiveness and reliability of its financial and organizational data”. Failure to acknowledge the danger of losing valuable information assets in today’s business environment causes an organisation to fall prey to unauthorised access to the organisational network systems.

In today’s business environment, governance is about whom makes the decisions, while management has to ensure those decisions are implemented. The vulnerabilities existing between governance and management is who validates, monitors and follows through to affirm that information security governance is in place and functioning. Lack of information security awareness, education and training in an organisation will affect confidentiality, integrity, and availability of information.

Doherty and Fulford (2008) draw on the work of Dhillon & Backhouse (1996) and Garg et al. (2003) and argue that, “information resources could retain their integrity, confidentiality, and availability only if they can be protected from the growing range of threats that is arrayed against them”. Doherty and Fulford (2008) further describe security threats as "circumstances that have the potential to cause loss or harm", which can be both from within and from outside the organisation. They indicate that common internal threats include "mistakes by employees and some categories of computer-based fraud, while attacks by hackers and malwares are the most commonly cited types of external threat”. Hence, "increasing vulnerability of computer-based information systems is underlined by the growing cost of security breaches” (Doherty & Fulford, 2008).

The above literature demonstrates that a paucity of proper information security governance could result in unauthorised access to employee confidential information, which constitutes a considerable threat and potential damage that could affect the institution as a whole. Figure 2.1 below illustrates some potential damage that could affect a university of technology.

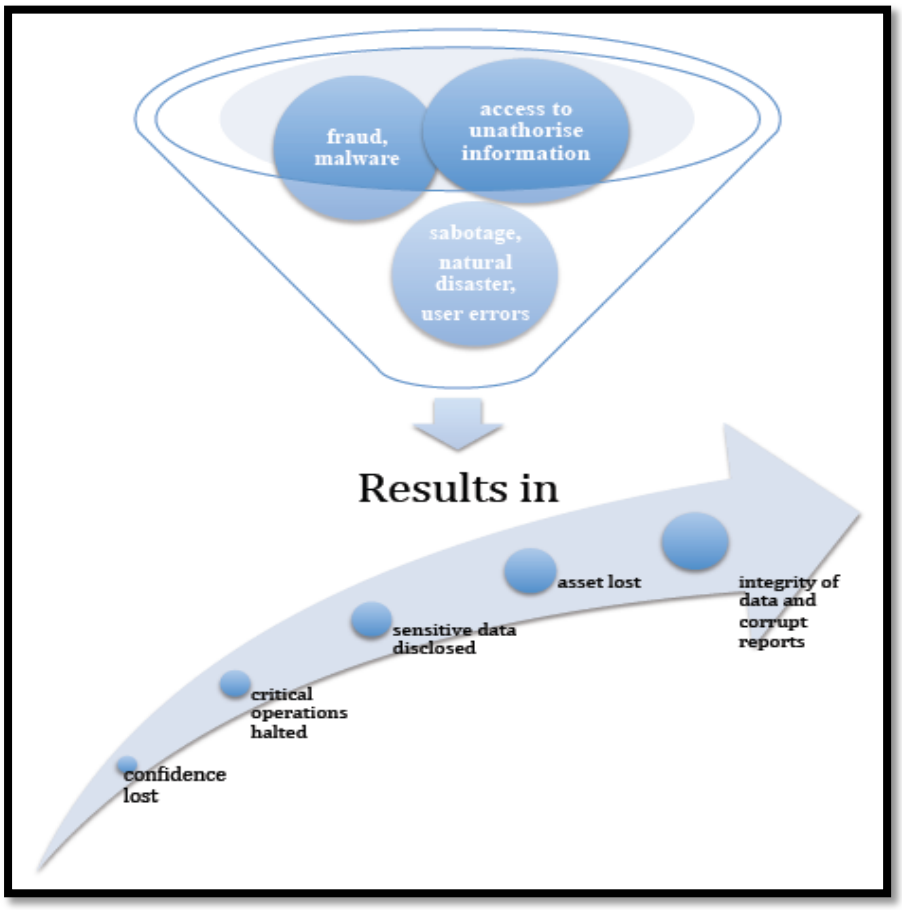


Figure 2.1: Threats and potential risk of tertiary education system vulnerability layout (GAO/AIMD-98-68 Information Security Management)

Figure 2.1 above illustrates the possible threats that could compromise a university of technology's systems by taking advantage of the vulnerabilities. According to the US General Accounting Office (1998), because "systems are interconnected to form networks or are accessible through public telecommunication systems, they are much more vulnerable to anonymous intrusions from remote locations". Lack of contingency plans for events such as fraud, natural disasters, sabotage, and hackers from both inside and outside the institution, and user errors, could cause damage to

the institution's information assets, as illustrated above. This then could cause potential damage such as loss of confidence, sensitive information disclosed to unauthorised persons, critical operations halted and the integrity of the institution's data and reporting corrupted.

Herath and Rao (2009:2) further note "previous research and field surveys suggested that employees seldomly comply with information security procedures. Policies, especially those involving information securities, are viewed as mere guidelines or general directions to follow rather than hard and fast rules that are specified as standards. Due to the relatively discretionary nature of adherence to these policies, organizations find enforcement of security a critical challenge". In addition to information security policies and regulations being a challenge, the Information Security Forum (ISF) (2007) contributes "information leakage" as another factor that impacts information security in today's environment. Breaches in the confidentiality of information are naturally of concern to the information security professional, and there are a number of particular threats and vulnerabilities that are related to information leakage incidents. Threats include loss of high-capacity storage devices, human error and the actions of malicious third parties (ISF, 2007). Vulnerabilities include inherent weaknesses in storage mechanisms (particularly personal storage) and the ease with which information can be copied between storage formats.

The combination of these threats and vulnerabilities, together with heightened media and regulator attention on the subject of information leakage, has increased the profile of information leakage incidents (ISF, 2007). To consider factors that do affect information security in a university of technology, Yeo et al. (2007) outline some factors in their study, with the following factors having an effect on tertiary education institutions with regard to information security management.

- **Management Support**: An often-cited success factor affecting information security is support from management. Management should ensure that assessment findings result in the implementation of appropriate changes to policy and that controls are continuous, unshakeable and visible.
- **Users' Security Awareness:** A successful information security management programme relies on the awareness and cooperation of users who must follow

procedures and comply with the implemented controls. This requires effective marketing of the information policy to all users to achieve awareness, and providing appropriate and continuous training and education. Established computer security policies within organisations are there to ensure that information resources are secured; however, if employees and end-users of organisational information systems (IS) are not committed or are unenthusiastic in following security policies, these efforts are in vain.

- **Technical Experts**: Yeo et al. (2007:4), citing the General Accounting Office (1999) contend: "Technical experts bring to the risk assessment process an understanding of existing systems designs and vulnerabilities and of the potential benefits, costs and performance impacts associated with new controls being considered." Yeo et al. cited from Torres et al. (2006), noting that "a critical success factor for ensuring security management of information systems is having honest, competent, smart and skilful systems administrators" (Yeo et al. 2007: 4).
- **Accountabilities**: Yeo et al. (2007:4) add that, "executive and line management should be accountable for implementing, monitoring and reporting on information security. Accountabilities and responsibilities should be clearly established for managing risk". They further argue that, "the successful implementation of information security requires the implementation of a measurement system that is used to evaluate performance in information security management". The current rapid growth of information technology tools calls for organisations to pay considerable attention to their vital data.

To affirm the factors mentioned above by Yeo et al. (2007:4), one has to evaluate the impact the factors have on information security management, which this research intends to validate. The impact of these factors on university of technology institutions in South Africa has yet to be examined, which this research intends to redress.

2.3 Human resource systems and infrastructure

2.3.1 Background

Human resource management is a unit within an organisation's structure where the administration of employee recruitment and placement takes place and where employees' personal information is managed. The data and information collected and stored in the department need to be protected from unauthorised access.

However, Gijana (2011: 5) posits that, "human resource management is known and accepted in the broadest sense of the term, as a form of management" that includes "all management decisions and actions that affect the nature of the relationship between the organization and the employees – its human resource". Therefore, human resource management can be difficult, as it comprises all issues that include employees and organisational relationships. Gijana (2011: 5) further argued that, "HR is the most important asset in achieving and sustaining business success", and therefore this makes it a sensitive area for safeguarding personnel information.

2.3.2 Personnel records and data security

The University of California, San Francisco (UCSF) has disclosed that, "proper handling of personnel records or personnel files in departments often raises questions. Organizations may keep only personnel records that are relevant and necessary to the administration of personnel programs. These records should be maintained with accuracy, relevance, timeliness, and completeness and appropriate and reasonable safeguards should be established to ensure security and confidentiality" (University of California, San Francisco, 2013). How this affects a university of technology is yet to be verified and the findings will be used to recommend best practice.

2.4 Users and the institution

The main asset group of any organisation are users; they are responsible for the control of information security (and by implication, insecurity) within the organisation. At same time they can be the most dangerous threats to information security and may help to control the vulnerabilities and accidental inaccuracies in the organisation. There are whole numbers of users within an organisation who may or may not be loyal to the organisation information. Users such as internal users,

external partners, and other stakeholders, for example, investors, are of high risk to the protection of the organisational data and without proper education and awareness of information security policies and procedures, these users may have a harmful effect on the organisation.

A university of technology has many users (such as HR personnel, medical schemes, insurance agencies, finance schemes, pension fund agencies, etc.) who have authorised access to personnel data in the institution. One may wonder how vulnerable employee data is, how secure it is and who maintains it? A preliminary discussion with the HR director of a university of technology elicited that more than 70% of the employees are on contract positions, and the HR director further mentioned that employees who are not full-time workers create a hostile environment and the level of turnover is very high; this creates a lack of trust and inadequate control of data security. The researcher therefore raises the concern of how insecure and vulnerable such a university of technology is with regards to it high employees turnover.

2.5 Information security policy and regulation, human resource systems and users

There are three information security pillars that this research study outlined information security policy and regulation, human resources system infrastructure and users. In an article of (ISO/IEC, 2005) it was argued that organisational "dependence on information systems and services means organisations are more vulnerable to security threats". One could look at current business practices; users are the most vital asset within the organization and play a big role in both organisational information security governance and human resource management systems. Furthermore, ISO 27001 article argues that, "information security management needs participation by all employees in the organisation". Employees and stakeholders of a university community share in the responsibility for protecting the confidentiality and security of data. Despite these issues, little research has been conducted in the area of human resource information security management in a university of technology. Alhough a university of technology may have its own way of managing its information security, particularly within the human resource information domain, it is not clearly understood how institutions manage the vulnerability of information security where

governance, human resource system infrastructure and users to be considered. The study therefore investigated and determined the vulnerability of information security management in a university of technology. Regulatory obligations the institution could consider to help meet the challenges related to information asset protection are also recommended.

2.6 Protection of personal information

Personal information is vital to any individual and governement has regulations protecting such information. Personal information, from Duncan's (2012: 1) perspective, is "information relating to an identifiable, living, natural person, or an identifiable, existing juristic person. In broad terms, personal information relates to: race, gender, sexual orientation, marital status, etc., medical, financial or criminal history; identifying numbers; contact details; biometric information; personal opinions; private or confidential communications; the views or opinions of others about the person; and the name of the person, in cases where the disclosure of this might reveal information about the person".

The *Protection of Personal Information Act, Act No. 4 of 2013*, for the Republic of South Africa seeks "to promote the protection of personal information processed by public and private bodies; to introduce information protection principles so as to establish minimum requirements for the processing of personal information; to provide for the establishment of an Information Regulator; to provide for the issuing of codes of conduct; to provide for the rights of persons regarding unsolicited electronic communications and automated decision making; to regulate the flow of personal information across the borders of the Republic; and to provide for matters connected therewith" (South Africa, 2013:2). The Act requires all organisations handling personal information to handle it with due diligence; such organisations do not exclude universities of technology. Duncan (2012: 3) states that "the Protection of Personal Information Act (POPIA) has huge implications for all institutions or organisations which gather, retain, disseminate and dispose of personal information". The study therefore intended to ascertain whether a selected university of technology does adhere to the requirements of POPIA.

2.7 Information security standards and case study

The objective of this research study was to investigate and determine the vulnerability of data collection, data processes, data access and data usage of personnel information in HRS of a selected higher education institution in South Africa. To understand the complexity around information security management, similarities between information technology standards are discussed and compiled. 'Standards' in this sense, means "a document that provides requirements, specifications, guidelines or characteristics that can be used consistently to ensure that materials, products, processes and services are fit for their purpose" (ISO, n.d.).

2.7.1 Information security standards and best practices

There are several security standards and best practice models available for information security. There seems to be a growing interest among organisations in information security standards and certification, and organisations are increasingly looking to adopt standards. Standards cannot only provide a framework for implementing effective information security practices; they can also ensure that information security and organisational objectives are properly aligned. Furthermore, organisations recognise that standards demonstrate to clients and customers their commitment to good information security practices.

2.7.2 Different information security management standards

Information technology standards are there to govern, support and control how organisations manage their IT business processes and IT system infrastructure, and secure their data and information assets. The IT Governance Institute and Office of Government Commerce (ITGI and OGC) (2008:19) state that, "There is no doubt that effective management policies and procedures help ensure that information technology is managed as a routine part of everyday activities. Adoption of standards and best practices enables quick implementation of good procedures and avoids lengthy delays in creating new approaches when reinventing wheels and agreeing on approvals." The three practices and standards below are taken from ISACA (2005: 6):

- "Information Technology Infrastructure Library (ITIL), published by the UK government to provide best practices for IT service management.

- "Control objective of Information Technology (CoBiT), published by ITGI and positioned as a high-level governance and control framework.
- "ISO/IEC 27002:2005, the latest version of *Information Technology – Security Techniques – Code of Practice for Information Security Management*, to give it its full title, is an internationally accepted standard of good practice for information security."

2.7.3 Practices provided by these standards

Sheikhpour and Modiri (2012:1), state that: "All organizations are dependent on their information technology resources, not only for their survival but also for their growth and expansion in today's highly competitive global markets". Practices such as CoBiT, ITIL and ISO/IEC 27002 can be adopted as the underpinning of a sound information security practice. The standards mentioned earlier are further elaborated as follows:

2.7.3.1 Control objectives of information technology (CoBiT)

According to ISACA (2005), "Business orientation is the main theme of CoBiT". Though CoBiT 5.0 is available and it is in use, the focus of the research makes it immaterial which CoBiT version is relevant. CoBiT, as stated by ITGI and OGC (2008:12) "is designed to be employed not only by users and auditors, but also, and more important, as comprehensive guidance for management and business process owners. Increasingly, business practice involves the full empowerment of business process owners so they have total responsibility for all aspects of the business process. In particular, this includes providing adequate controls".

ITGI and OGC (2008:12) further note "The CoBiT framework provides a tool for the business process owner that facilitates the discharge of the business processes. The framework starts from a simple and pragmatic premise: to provide the information that the organisation needs to achieve its objectives, IT resources need to be managed by a set of naturally grouped processes. The framework continues with a set of 34 high-level control objectives [see Appendix C], one for each of the IT processes, grouped into four domains: Plan and Organise, Acquire and Implement, Deliver and Support, and Monitor. This structure covers all aspects of information and the

technology that supports it." By addressing these 34 high-level control objectives, university of technology business process administrators can ensure that an acceptable control system is provided for the IT environment. Figure 2.2 below illustrates the CoBiT framework and processes.

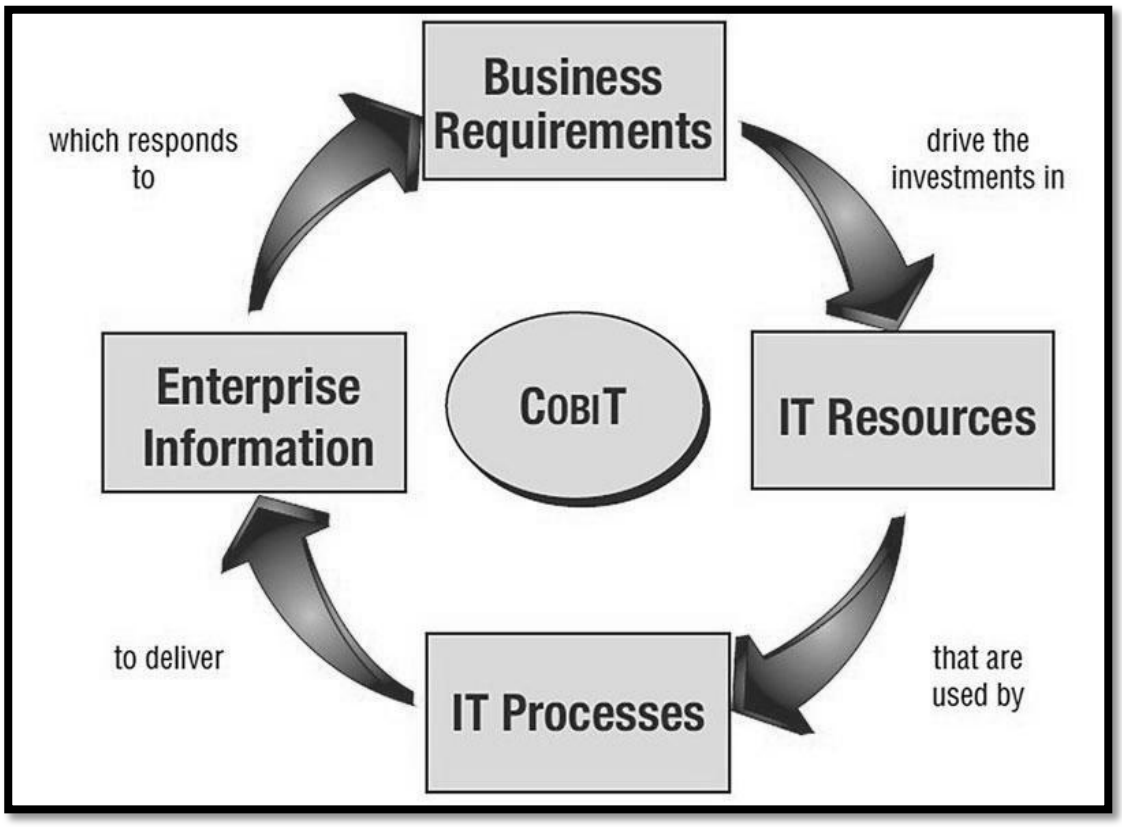


Figure 2.2: CoBiT 4.1 framework (ISACA 2010)

ITGI and OGC (2008:12) further mention that IT governance guidance is also provided in the CoBiT 4.1 framework. "IT governance provides the structure that links IT processes, IT resources and information to enterprise strategies and objectives. IT governance integrates optimal ways of planning and organising, acquiring and implementing, delivering and supporting, and monitoring and evaluating IT performance". Well-implemented CoBiT IT governance can enable a university of technology to take full advantage of its stored information.

2.7.3.2 Information technology infrastructure library (ITIL)

Universities, like the selected university of technology, depend mostly on computer systems to run the day-to-day business activities to fulful their business goals. Based on ISACA (2005:13), "this growing dependency necessitates quality IT services at a

level matched to business needs and user requirements as they emerge. IT service management is concerned with delivering and supporting IT services that are appropriate to the business requirements of the organisation. ITIL provides a comprehensive, consistent and coherent set of best practices for IT service management and related processes, promoting a quality approach for achieving business effectiveness and efficiency in the use of Information Systems".

Further, "ITIL service management processes are intended to underpin, but not dictate, the business processes of an organisation. The generic processes described in ITIL promote best practice and may be used as a basis for achieving the British Standard for IT Service Management (BS 15000), which is currently considered for fast-tracking an international standard—ISO/IEC 27002. The core operational processes of IT service management are described within two ITIL publications: *Service Support* and *Service Delivery*" (ITGI and OGC, 2008:13)

The processes of service support described in ITIL are: "incident management, problem management, configuration management, change management, release management and service desk function. The processes of service delivery described in ITIL are: capacity management, availability management, financial management for IT services, service level management and IT service continuity management" as reported by ISACA (2005:13). These IT service supports and deliveries listed above can help tertiary institutions to enhance or improve the usage of their information technology infrastructure.

2.7.3.3 International Organization for Standardization (ISO) 27002

Based on the ITGI and OGC (2008:15) report, "essential parts of ISO 27002 information technology—Code of Practice for Information Security Management were developed and published by the British Standards Institution. The ISO and International Electrotechnical Commission (IEC), which have established a joint technical committee, the ISO/IEC JTC 1, published the international standard. ISO/IEC 27002 provides information to responsible parties for implementing information security within an organisation. It is seen as a basis for developing security standards and management practices within an organisation to improve reliability on information security in inter-organisational relationships. Measures

based on legal requirements include: protection and nondisclosure of personal data, protection of internal information and protection of intellectual property rights. The best practices mentioned are: information security policy, assignment of responsibility for information security, problem escalation and business continuity management". The mind map in Figure 2.3 below outlines the services of ITIL.

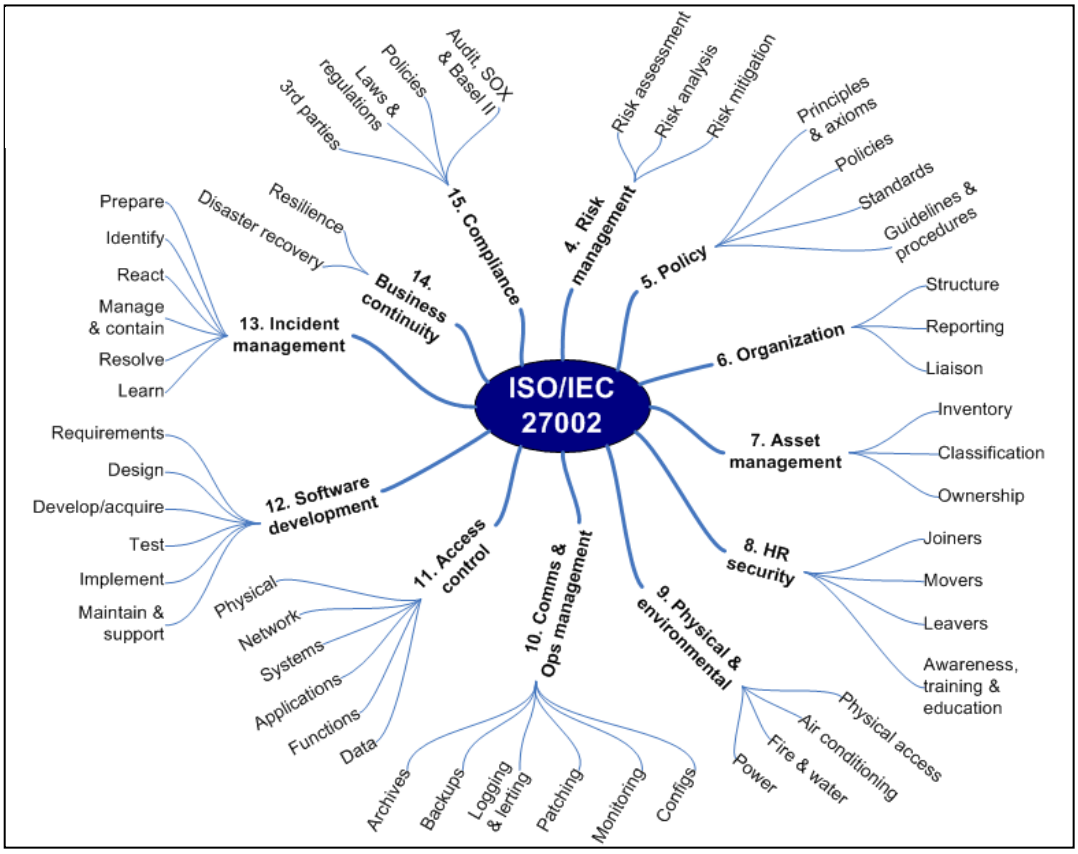


Figure 2.3: ISO Mind Map (source: ISO/IEC 27002, n.d.)

Figure 2.3 above illustrates different sections within the ISO/IEC 27002 mind map. The main focus on this study is on Section 8 in the ISO/IEC 27002 standard, which is human resource security management. The (ISO/IEC 27002:9) standard states that, "the organization should manage system access rights for joiners, movers and leavers, and should undertake suitable security awareness, training and educational activities". Some academic institutions may do this at the beginning, but omit it at the end, meaning when an employee leaves the organisation, he or she is believed to still have access to institutional emails and business application systems for months.

Drawing from the ISO/IEC standard, the follow feature from the mind map is further explained.

"Prior to employment: Security responsibilities should be taken into account when recruiting permanent employees, contractors and temporary staff (e.g. through adequate job descriptions, pre-employment screening) and included in contracts (e.g. terms and conditions of employment and other signed agreements on security roles and responsibilities).

During employment: Management responsibilities regarding information security should be defined. Employees and (if relevant) third party IT users should be made aware, educated and trained in security procedures. A formal disciplinary process is necessary to handle security breaches.

Termination or change of employment: Security aspects of a person's exit from the organization (e.g. the return of corporate assets and removal of access rights) or change of responsibilities should be managed" (ISO/IEC 27002:9).

The study intended to validate whether the university of technology in question does adhere to the practice of information security management with regard to access rights termination when an employee exits the organisation.

2.8 Comparison of ITIL, CoBiT and ISO/IEC 27002

The comparism of the standard is done outlining the main focus areas of the standards and the relevant areas for the research study:

- "ITIL is strong in IT processes, but limited in security and system development. ITIL is based on defining best practice processes for IT service management and support, rather than on defining a broad-based control framework. It focuses on the method and defines a more comprehensive set of processes. ITIL is intended to underpin but not dictate the business processes of an organization. The role of the ITIL framework is to describe approaches, functions, roles and processes, upon which organisations may base their own practices.
- CoBiT is strong in IT controls and IT metrics, but does not say how (i.e. process flows) and not that strong in security. However, COBIT does not include process steps and tasks because, although it is oriented toward IT processes, it is a control and management framework rather than a process framework. CoBiT focuses on what an enterprise needs to do, not how it needs

to do it, and the target audience is senior business management, senior IT management and auditors. CobiT is a globally accepted framework for IT governance based on industry standards and best practices. Once implemented, executives can ensure IT is aligned effectively with business goals and better direct the use of IT for business advantage.

- ISO/IEC 27002 is strong in security controls, but does not say how (i.e. process flows). It is a basis for developing security standards and management practices within an organisation to improve reliability on information security in inter-organisational relationships. It provides information to parties responsible for implementing information security within an organisation" (ITGI & OGC, 2008:17).

The Information Technology Governance Institute and Office of Government Commerce, 2008:19) further note: "There is no doubt that effective management policies and procedures help ensure that IT is managed as a routine part of everyday activities. Adoption of standards and best practices enables quick implementation of good procedures and avoids lengthy delays in creating new approaches when reinventing wheels and agreeing on approaches. However, the best practices adopted have to be consistent with a risk management and control framework, appropriate for the organisation, and integrated with other methods and practices that are being used. Standards and best practices are not a solution; their effectiveness depends on how they have been implemented and kept up to date. They are most useful when applied as a set of principles and as a starting point for tailoring specific procedures. To ensure policies and procedures are effectively utilised, change enablement is required so management and staff understand what to do, how to do it and why it is important. For best practices to be effective, the use of a common language and a standardised approach oriented toward real business requirements is best, as it ensures that everyone follows the same set of objectives, issues and priorities" (ITGI & OGC, 2008:19).

2.9 Information security management in a university of technology

Organisations today need to use IT strategically to gain the benefits and competitive advantage. Information technology as reported by ISACA (2005:9) "has the potential to be a major driver of economic wealth in the 21st century. Information technology being a critical enterprise success, it provides opportunities to obtain a competitive

advantage and offers a means for increasing productivity, it will do all this even more in the future. Though it carries risks, it is clear that in these days of doing business on a global scale around the clock, systems and network downtime have become far too costly for any enterprise to afford. In some industries, IT is a necessary competitive resource to differentiate and provide a competitive advantage, while in many others it determines survival, not just prosperity"(ISACA, 2005:9). Therefore there is a great need for best practices to be adapted in organisations such as universities of technology to provide these institutions with the following benefits based on ITGI and OGC (2008); a well implementation of these practices would;

- reduce dependency on technology experts
- increase the potential to utilise less-experience staff if properly trained
- make it easier to leverage external assistance
- overcome vertical silos and nonconforming behaviour
- reduce risk and errors
- improve quality information security
- improve the ability to manage and monitor information security
- improve trust and confidence from management and partners
- safeguard and prove values of information security

The continuous change of companies' technology and civilisation requires a process of continuously evaluating the effectiveness and efficiency of all security controls and adapting the security system to changing requirements (ITGI & OGC, 2008).

The following section is a conceptual framework developed using knowledge of literature reviewed as far to tease out an information security management in a university of technology.

2.10 Conceptual framework

The proposed framework below will serve as a guide to the data collection process, including the style of interview questions. The framework proposed is to determine the vulnerabilities that might exist in managing the organisational data.

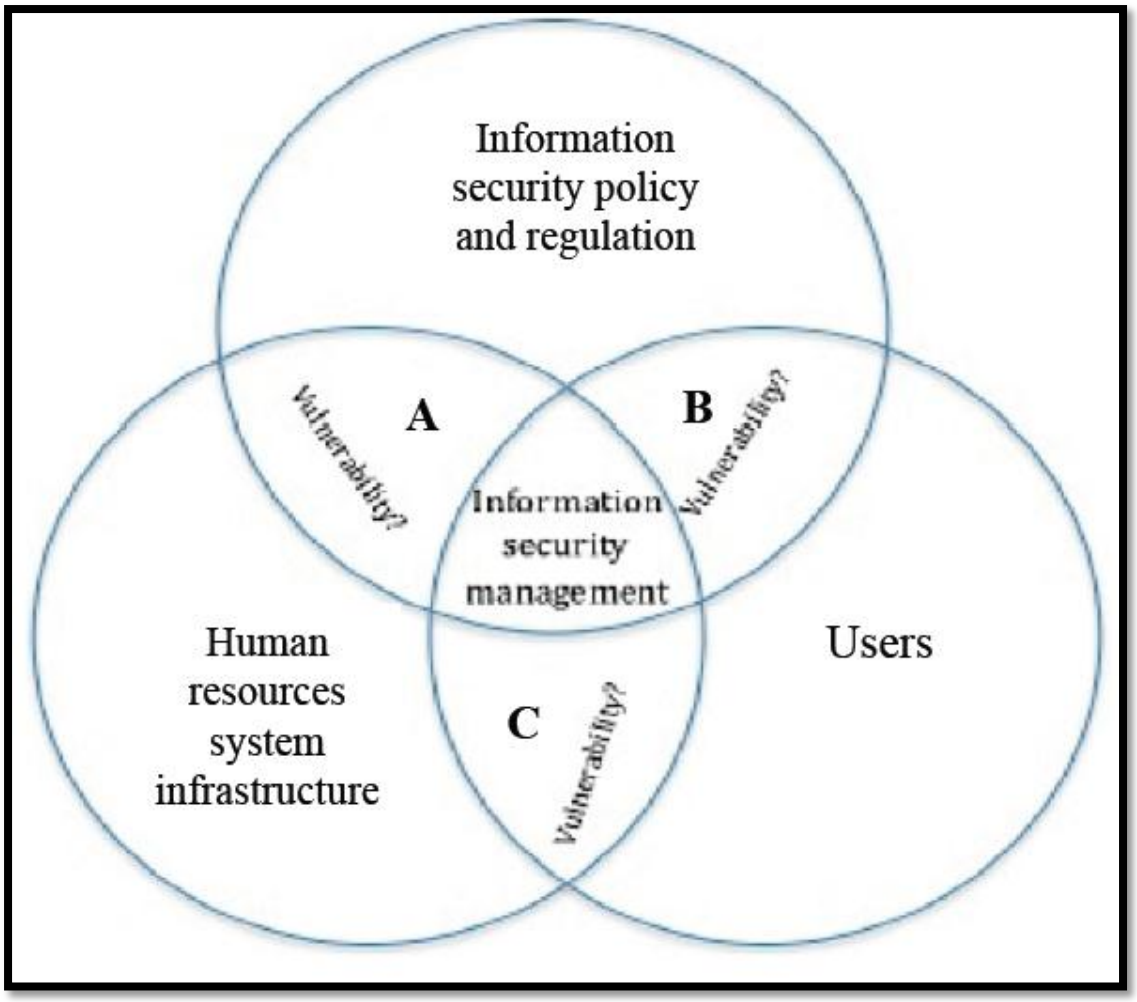


Figure 2.4: Research conceptual framework

Given the above analysis and evaluation of existing scholarly work on information security management and/or lack thereof, a conceptual framework was developed, firstly, to conceptualise the problem as a social phenomenon, and secondly, to guide further understanding and interpretation of this social phenomenon. It was also used for the research design, and in particular, the data collection and analysis. Finally, the proposed framework also served as a guide to develop the techniques deployed in the design of the data-collection instrument. Therefore, the framework proposed above was expected to determine the vulnerabilities A, B and C specified in the framework above that might exist in managing the organisational data.

The above conceptual framework derived from the literature and the conceptualisation of the research problem to understand the research domain and how to interpret the factors contributing to the vulnerability of data through unauthorised access to and use

of the HRS. The compoments influencing information security management are as described below:

The above conceptual framework is further elaborated below:

(i) Policies and regulations – this represents the guidelines to govern users on how they should manage, maintain and use the orgnisational data. These guidelines are made to believe by management that employees adhere to these policies and regulations. The intersections within the conceptual framework demonstrate the relationship that exists between organisational information security policies and regulations, users and the human resource information system.

(ii) Users – these are the internal employees in the HR department and external partners who have authorised access to the organisational data. Users are the central focal point for policies and regulations and the use of the HR system. Users should comply with information security policies and regulations if they are aware of such regulations.

(iii) Human resource systems infrastructure support – represents the data system in place, managing the movement of data within the organisation, and governed by the policies and regulations.

The three conponents illustrated in Figure 2.4 do interact with one another during information (or data) management and represent the complexity of information management. This study used this conceptual framework to investigate the vulnerabilities of information security management within a university of technology HR system to recommend a general framework and information security practices to contribute to the body of knowledge regarding how a university of technology can improve information security management.

2.11 Summary

Information security management is vital to any organisation, irrespective of its business practice. Employee data is regarded as an enterprise information asset because of the valuable information, such as personal details, health, insurance, pension, and banking details, it contains. The chapter introduced the relevant

literature and contribution to the body of knowledge. The purpose of information security and governance, and factors affecting information security in a university of technology were outlined.

The chapter further highlighted some research with regard to information security and standards that govern information. In this chapter the role of information security in organisations was discussed. It was ascertained that information plays a vital role in organisations and protecting information has become crucial for the business continuity of most organisations. It was mentioned that information security should be viewed as a continuous process, and not as a separate set of activities. Furthermore, a range of information security aspects was examined, such as the reliability aspects of information, different security controls, and requirements for a successful security programme. It was disclosed that there are various factors that impose limits on information security, such as security spending that is lagging behind total IT expenditure. Finally, several best practices and standards were addressed. In the next chapter, the research methods used to examine and investigate university of technology information security management are examined. A conceptual framework is developed based on literature reviewed and is used to assist in the data collection and analysis.

The next chapter introduces the research design and approach used in conducting the research findings. It also introduces a case study and the designed business process model illustrating the processes in the human resource management system unit.

CHAPTER 3: RESEARCH APPROACH

3.1 Introduction

This study investigated the vulnerabilities inherent in information security management in an HR system in a selected university of technology. These vulnerabilities were established through a literature review and by interviews conducted at a university of technology. The literature review and developed conceptual framework suggested the appropriateness of the use of interpretive philosophy to tease out the outlined problem. This is because reality, such as the factors contributing to the vulnerability of HR data, is a socially constructed phenomenon. Burrell and Morgan (1979:19) contend that "… the interpretive paradigm is informed by a concern to understand the world as it is, to understand the fundamental nature of the social world at the level of subjective experience. It seeks explanation within the realm of individual consciousness and subjectivity, within the frame of reference of the participant as opposed to the observer of action".

According to Vessey et al. (2002), an interpretive approach has been used to add greater richness to the interpretation of the information systems phenomena. Furthermore, Burrell and Morgan (1979:20) argue that "interpretive philosophers and sociologists seek to understand the very basis and source of social reality which in the context of research the researcher seeks to tease out" – in this case, the social reality of information security management. Therefore the interpretive research method was employed to gather data for analysis and to compile suggestions and recommendations to enhance information security management in a university of technology human resource information system.

3.2 Methodology

There are different types of research methodology available for research, depending on the nature of the study. Wisker (2014:1) argues that, *"*one's research will dictate the kinds of research methodologies one will use to underpin one's work and methods one will use in order to collect data. If one wishes to collect quantitative data one is probably measuring variables and verifying existing theories or hypotheses or questioning them. Data is often used to generate new hypotheses based on the results of data collected about different variables*"*.

Based on the interpretive assumption made, a qualitative approach was used. In support of the approach, Wisker (2014:1) mentions that, *"*qualitative research methods are carried out when one wishes to understand meanings, look at, describe and understand experience, ideas, beliefs and values, intangibles such as these*"*. Wisker further argues that, *"*using interviews enables face-to-face discussion with human subjects, and the researcher has to determine the interview schedule of questions to use which can be either closed or open questions, or a mixture. However, often collections of statistics and number crunching are not the answer to understanding meanings, beliefs and experience, which are better understood through qualitative data. In a quantitative data analysis, data must be remembered, and also collected in accordance with certain research vehicles and underlying research questions. Even the production of numbers is guided by the kinds of questions asked of the subjects, so is essentially subjective, although it appears less so than qualitative research data" (Wisker, 2014:1).

The study attempted to analyse the management of information security within the HR system in an organisation, and in particular at a university of technology, to determine the factors contributing to the protection of information assets. The results obtained from the analysis were used to compile a recommendation to minimise the threats that users' behaviour poses to the protection of information assets.

3.3 Case study of a university of technology

A university of technology (UoT) HR department's information systems were selected as the field of study. Tertiary education institutions in South Africa, especially the former technikons, have undergone developmental phases both administratively and academically, and are still in the process of integrating all their administrative business processes. In March 2001, the South Africa Minister of Education, Kader Asmal, announced the National Plan on Higher Education to change the higher education landscape (CPUT, 2012).

In line with the Department of Education's Guidelines for Mergers and Incorporations, in October 2003 the Minister approved the address and new name, Cape Peninsula University of Technology, and today the institution is known by its

new name with six geographically dispersed campuses. It has more than 30 000 students and 1 200 staff. The human resource departments of the two previous technikons (Cape Technikon and Peninsula Technikon) were integrated (CPUT 2012), and this raises the question: How securely is personal data gathered and maintained in the process of employing and terminating employee contracts by the department? Figure 3.1 below illustrates the structure of CPUT and some functions within its human resources department.

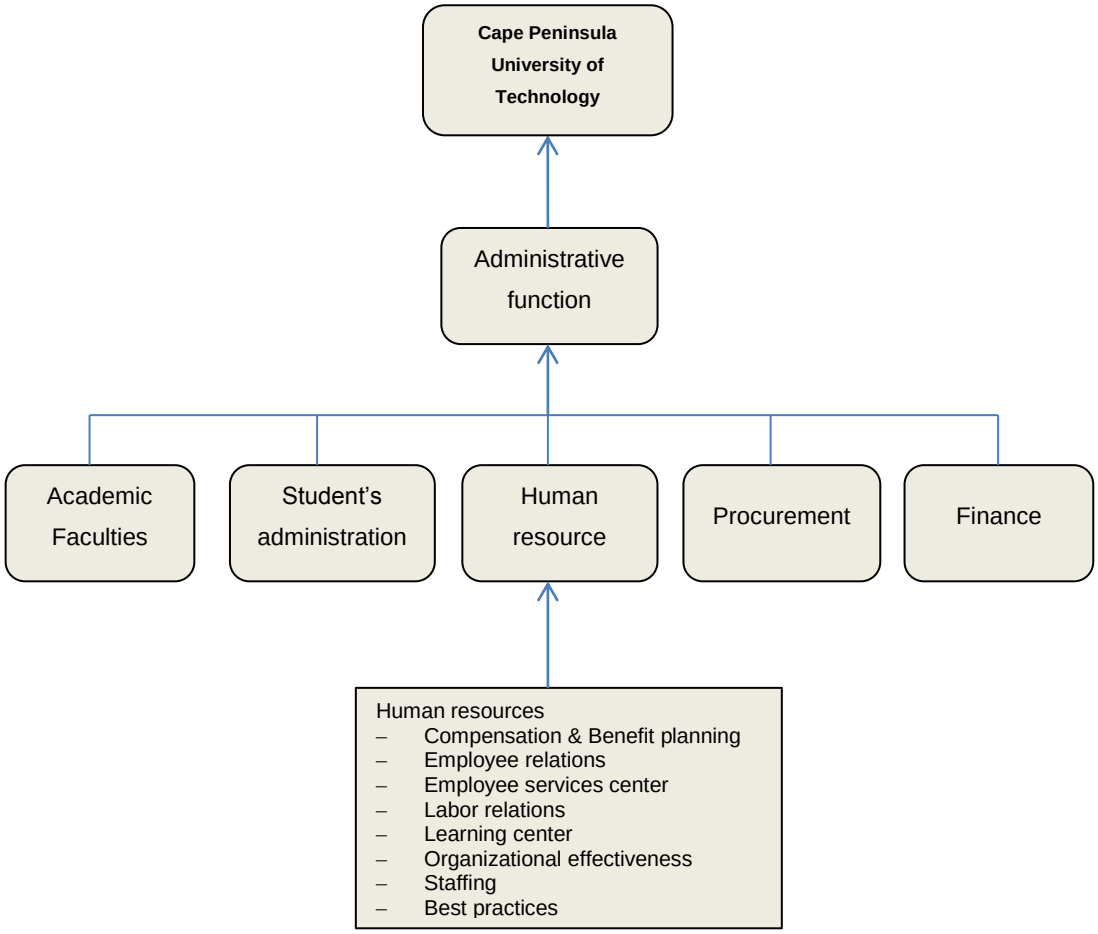


Figure 3.1: Organisational structure and some human resources functions of the Cape Peninsula University of Technology

3.3.1 Human resources process of appointment: Case study

Human resource management is a unit within an organisational structure where employees are recruited and their vital information is managed. The current recruitment process for CPUT takes approximately 90 days. It begins, when a head of department (HOD) requires a position to be filled.

1. The HOD must complete a requisition and send it to the Human Resources (HR) Department. HR reviews and assigns a number to the requisition, and returns it to the HOD for approval. He/she approves it, obtains the appropriate signatures, and then returns it to HR.
2. Next, HR creates a job position and announces the position internally, first through the company's intranet and bulletin boards.
3. HR also solicits résumés from external sources by advertising. HR pre-screens résumés and forwards the names of qualified candidates to the HOD forreview. The HOD notifies HR of candidates to interview.
4. The HOD also conducts phone screening. If the phone screening is promising, HR coordinates and schedules an on-site interview. The HOD interviews the candidates, with an HR representative present at the interview. HR records the interviews in an applicant flow log.
5. Once a candidate is selected for hire, HR and the HOD prepare an offer, and a background check is initiated.
6. The HOD then must approve the offer and obtain the required signatures on an internal associate data/change form. Subsequently, the HOD must extend the offer to the candidate, while HR sends the written offer, including a start date for work.
7. Once the applicant accepts the offer, the person signs the offer letter and returns it to HR. HR notifies the HOD of the acceptance. Finally, the "new hire" receives orientation on the date hired.

Figure 3.2 below illustrates a process flow of the appointment process within a university of technology human resources department, using the case study above.

Appointment process flow

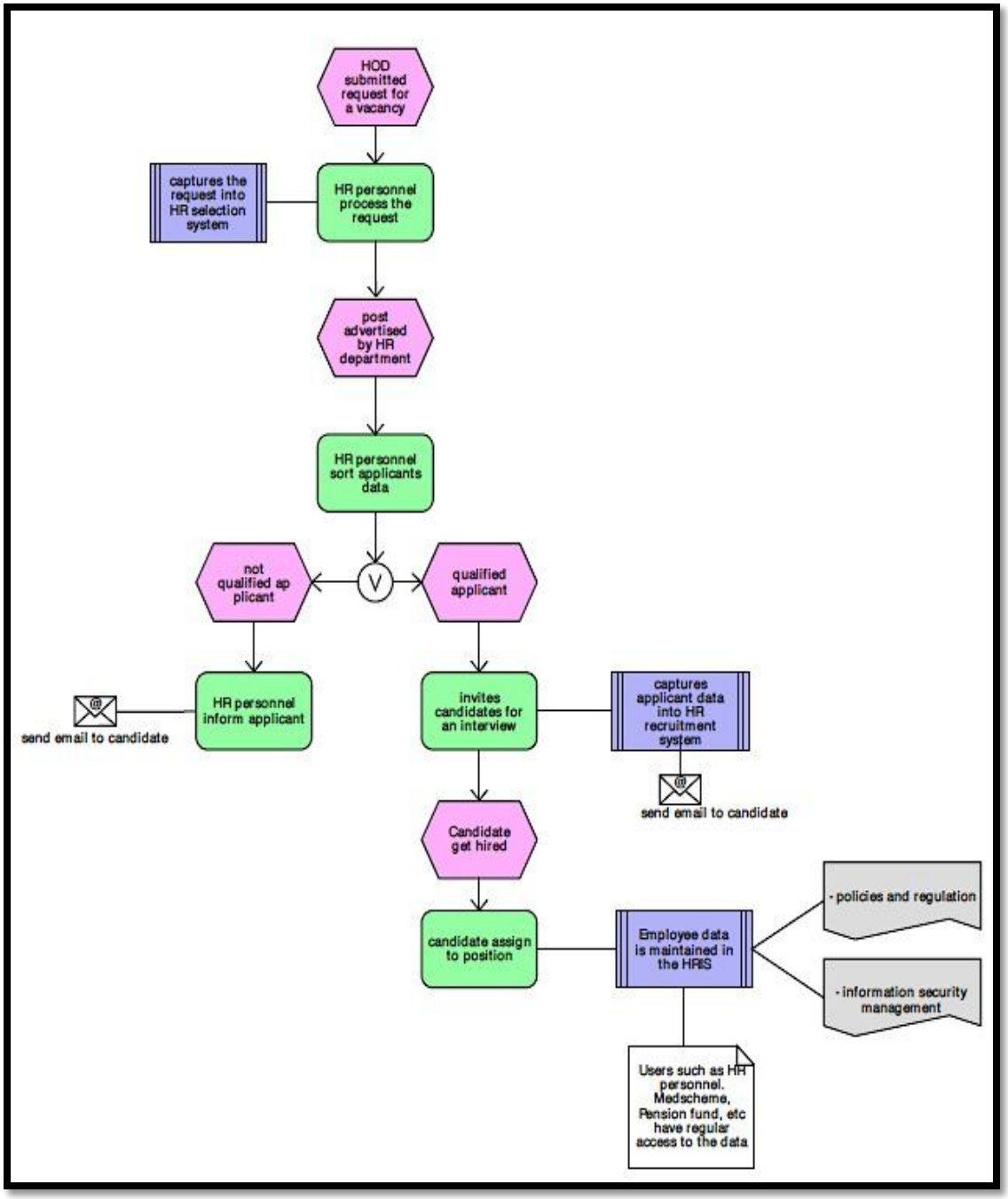


Figure 3.2: A university of technology human resources appointment business process

The above business process diagram illustrates the process that the HR Department goes through to appoint an employee into the organisation (see Appendix B for detailed HR business process). Data collected in each of the process areas are stored in a centralised database for easy access and maintainance. The Cape Peninsula University of Technology uses Integrated Tertiary Software (ITS) to manage its employee data, where

HR personnel are able to store and make changes to the data in real time. The institutional data policies, and how users manage HRIS, could determine the university's vulnerability.

3.4 Summary

The chapter introduced the objective of the research study and the methodologies considered for the study. It further introduced the University of Technology chosen for the field study and a case study used for the research. The next chapter analyses and dicusses the responses received from the research questions.

CHAPTER 4: ANALYSIS AND INTERPRETATION OF DATA

4.1 Introduction

This chapter presents an analysis of the qualitative data collected for this study. The fieldwork was based at a university of technology and the unit of analysis was the management of information security in the institution's HR information systems. The analysis centred on how employee data is maintained and the vulnerabilities associated with its maintenance. A general framework based on the conceptual framework was recommended to improve compliance with information security standards.

The data collected through interview-questionaires with participants from the CPUT HR department was analysed and interpreted within the research analysis framework. The outcome of the analysis guided the development of the general framework. It is envisaged that this should guide HR executive management, HR officers and other stakeholders to improve the management of data security within the HR department.

The selection of participants was done in the light of their position within the institution, and involvement in data capture, data usage and information security management processes within their department. Closed-interview questions were used to collect data, but individual participants were at times engaged to share their personal experiences with regard to the research topic. These discussions were recorded and transcribed in the data analysis and interpretation. Thirty research interview questionnaires were distributed and 20 responses were returned. A brief description of the participants follows:

Table 4.1: A brief description of the participants

Code	Position	Number of responedents	Responsibilities	Reason for the interview
DHR	Director Human Resources	1	Manages and works on the human resource information system daily	To understand the practice of information security and how it is implemented within the HR department

HRO	Human resources officers	19	Work on the human resource information system daily	Ascertain information security practice, awareness and training, management commitment to information security and involvement of information security specialist in the HR department

The research questions were answered by analysing the responses from the participants. Although the selected case study focused on information security management in HRIS, the study did not aim at implementing information security measures, but rather explored the relationship between implementation, effectiveness of measures and the practice and awareness of and training in information security.

4.2 Research instrument

Research instrument used to collect data for analysis and interpretation was interview-questionaires in this research to help the researcher to develop a more detailed view of the factors and issues affecting information security management in the HRIS.

Interviews are of three types: structured interviews, semi-structured interviews and unstructured interviews. Structured interviews use a formally structured schedule of interview questions, with each participant given the same set of questions. Semi-structured interviews use predetermined questions with questions asked in a systematic and consistent order. On the other hand, unstructured interviews do not employ a standard schedule of questions; rather questions are designed, based on the interviewee responses as the interview continues. Therefore, qualitative semi-structured interviews were employed as the primary data collection method.

4.3 Data analysis and interpretation of data

This section presents an analysis of the qualitative data collected for the study. The research conceptual model (see Figure 2.4, Chapter 2) is presented here to provide a focus for the case practices and issues.

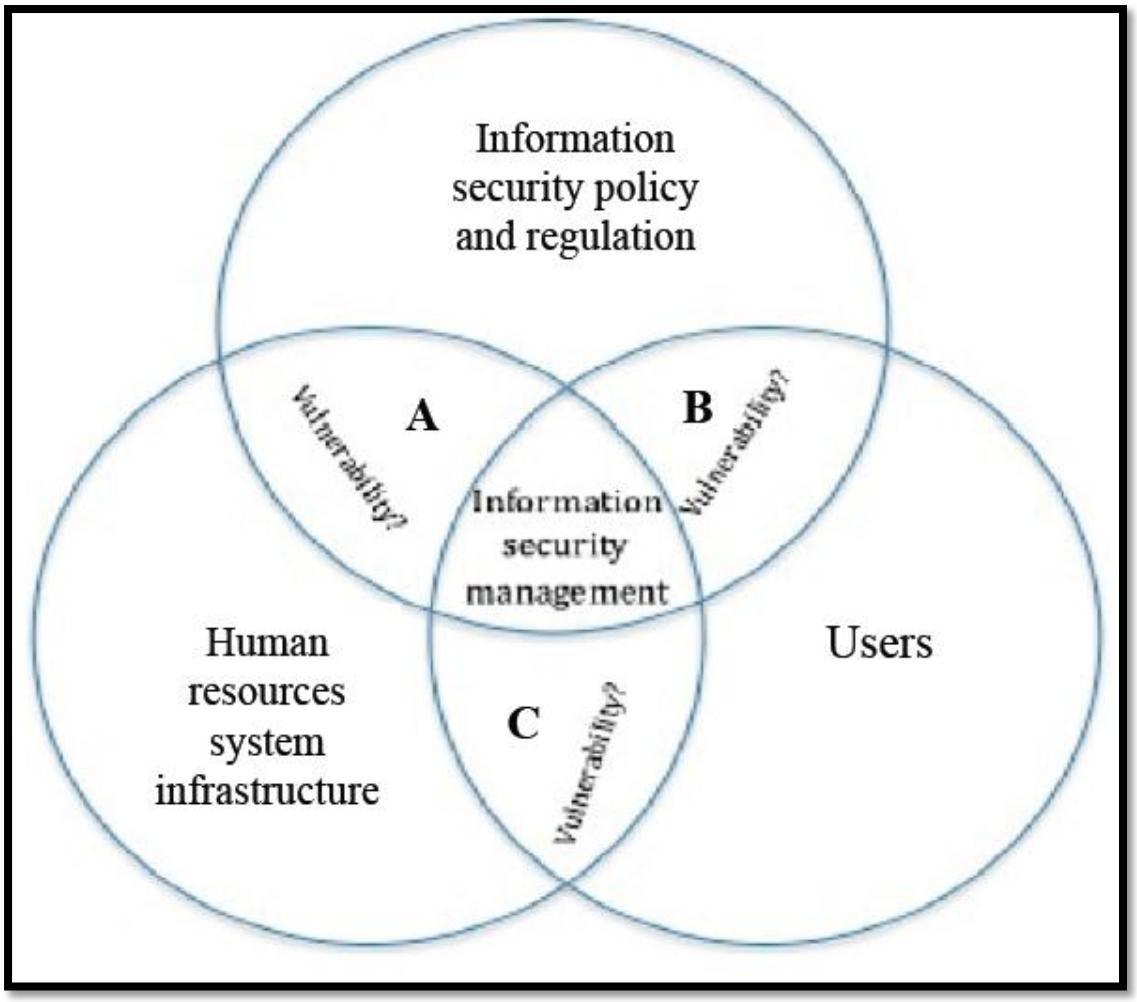


Figure 4.1: Research conceptual framework

The research questions were divided into two parts: the first was to collect data about the current position of the participants and to understand what individuals consider to be the main causes of information security incidents and the barriers to achieving improved security compliance within the department. The second was to assess the institutional and departmental aspects of information security management.

The data collected in Part 1 (see Appendix D), demonstrates their knowledge, and what the participants considered to be the three main causes of information security incidents, such as malware, cyber or internally based attacks and user error or non-compliance with information security in the HR department. These assertions affirm the literature of the Information Security Forum (2007), where information leakage was addressed and some of the factors reported as security threats were human error, malware and an insider. The participants for this study also considered lack of information security

awareness and training programmes, lack of adequate technology and lack of management involvement in security issues to be the three main barriers to improved security compliance.

Notably, the participants appeared to share a similar understanding of the main causes of information security incidents. Nevertheless, this understanding seemed not to be linked with the overall departmental strategy development of the employees' awareness of information security. The majority of participants indicated that top management did not regard information security as a big issue within the department, and as such seemed to influence the HR officers' lack of commitment to information security programmes.

The second part of the data collection was to understand and to determine information security practices in the HR department.

4.3.1 Management commitment

To a large extent, the lack of HR management commitment to information security within the HR department is clearly illustrated in Figure 4.2 below. Participants happened to share the same understanding that information security management practices might exist, but were not enforced or fully implemented by top HR management. Most participants responded that little was done to identify threats and vulnerabilities, and also to conduct risk assessment to support information security programmes (see Figure 4.2 below). Some participants noted that:

> "There hasn't been a seminar or directives from management to enforce information security."

> "I am a human resource officer, not an information technology professional."

A question was asked by the Human Resource Director, and is trancribed below:

> "Do we have a person called information security manager or profesional in this institution? If there is, I will [*sic*] like to meet such an individual" (HRD, Table 4.1).

During the time of data collection, the researcher had the opportunity to meet an IT manager and two questions were addressed to him: Do you expect HR management and HR officers to know about information security practices? He responded:

> "We don't expect them to know everything about security but at least [they] should know their responsibility with regard to information management."

The second question was: Is there any information security management training offered to executive management? He responded:

> "No information security management training at the moment is given to them but [we] do inform them of security issues as it arises [sic]."

Figure 4.2 below demonstrates the partial commitment of HR management's involvement in information security. Probably not much education and training are given to HR management to be able to manage and enforce security policy and regulation. However, researchers and information security standards continuously affirm that executive management in organisations are the custodians for the control and protection of organisational information assets.

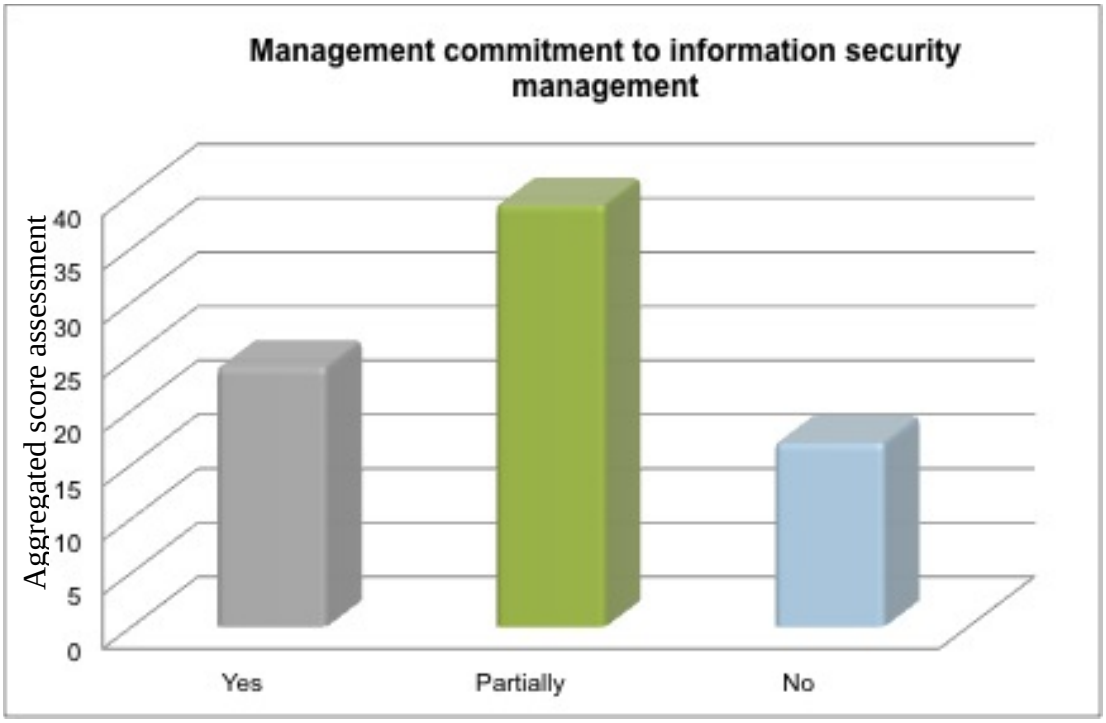


Figure 4.2: Commitment of HR top management to information security

This level of commitment appears to be the practice among HR officers, resulting in inconsistent information security policies and regulations. Referring to Viljoen's (2008:13) argument, executive management seem to believe that "information security is the responsibility of the information security professional", which one might contend is common knowledge, but it should be every member of executive management's responsibility to enforce it.

4.3.2 Security compliance

Participants were asked to respond to issues pertaining to the violation of organisational security policy and regulations, password sharing among users, and regular information security audits to verify information misuse or intrusion attempts. It was apparent that not much was done to comply with information security standards or practices, owing to the lack of commitment from HR executive management. When the participants were asked about any clear procedures in place to discipline members who violated organisational information security policies and regulations, the majority responded partially. Respondents made the following observation:

> "Not aware of any measures or formal procedures in place to discipline members who does [*sic*] not comply to [*sic*] information security regulations, especially in the case where we are not even aware of any existing security regulations."

> "It is quite surprising that there are no information security compliance regulations tabled in any of our meetings, especially looking at the devices available to leak valuable data to the public" (HRO, Table 4.1).

> "There are no clear procedures and guidelines related to information security isues and it is taken for granted that managers and individuals will do the right thing, but unfortunately, this is not always the case."

Another respondent admitted that:

> "Password sharing is really an issue here in the department; we do not tolerate or share passwords among ourselves, but IT professionals are responsible for the maintenance of passwords."

This indicates that low enforcement appears to be an issue in the HR department, even though the password policy was practised within the department. Most participants were not aware of information security standards available for the department, and they believed information technology professionals were the custodians of security issues. Figure 4.3 below illustrates the responses from participants with regard to security compliance.

Figure 4.3: Human resource department information security compliance

In general, participants indicated that compliance with information security standards was not fully implemented and enforced by management (see Appendix A). One thing that the respondents highlighted as of high concern to HR management was password sharing among users. With reference to the conceptual framework in Figure 4.1, it is clearly seen that there are vulnerabilities between information security policies and regulations, users, and human resource systems. Thus, there are no clear communication structures of information security responsibilities within the HR department. This research will recommend possible solutions to bridge the gap that currently exists within the structures.

4.3.3 Awareness

HR officers rely heavily on computer and telecommunication services (CTS) professionals whose responsibilities are to monitor and maintain computer networks and security issues, such as a malware outbreak, or unauthorised access to the institutional network, etc. Respondents commented:

"We get to be notified by email of any information security incident that does occur. I don't even know who is the responsible person. These emails get sent to us without any detailed explanation" (HRO, Table 4.1).

"I'm sure numerous warning security emails sent from CTS department, does [*sic*] not get noticed by many or taken serious [*sic*]."

Other respondents noted:

"I'm not sure of any awareness programme organised to properly inform us of the security responsibilities and how to safeguard institutional vital data" (HRO, Table 4.1).

"As a manager, it is my responsibility to manage the people. I leave the security issues to the CTS department."

Figure 4.4 below illustrates the responses from the respondents regarding awareness programmes.

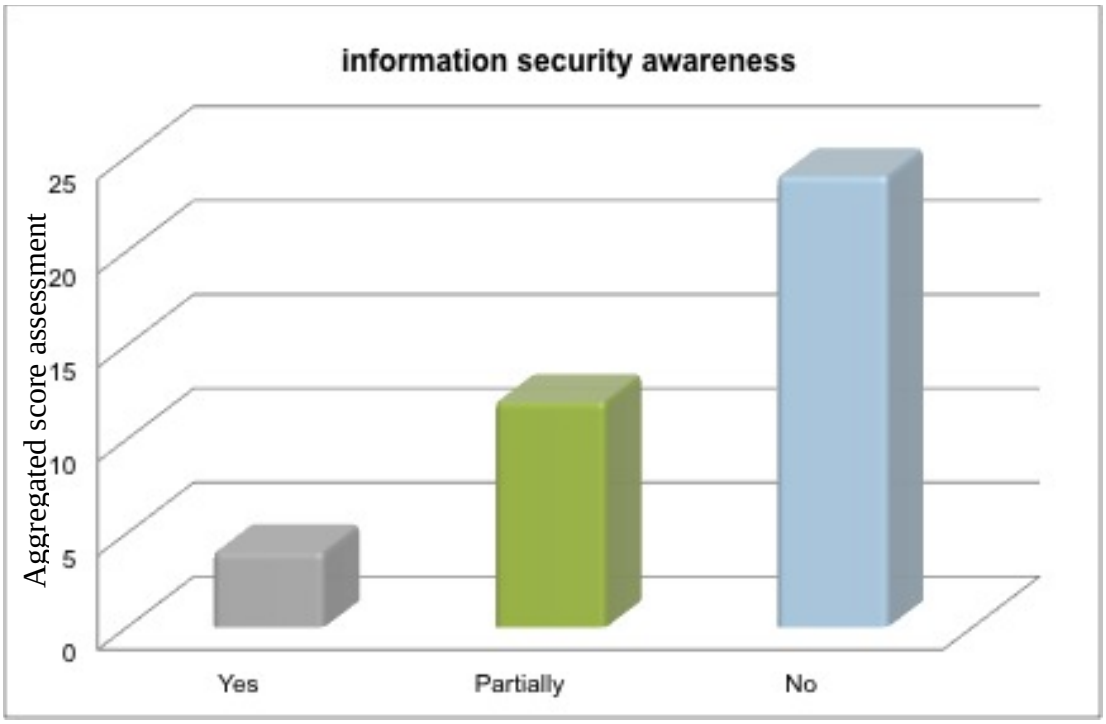


Figure 4.4: Awareness of information security

As apparent from Figure 4.4 above, one of the blockages of information security practice within the HR department is information security awareness.

4.3.4 Skills and training

Participants indicated that there had not been any structured training programmes with regard to information security. The majority of the participants were not even aware of any information security expert within the institution to support services such as day-to-day business processing.

In a meeting with the HR director on the issue of information security management, she mentioned:

> "Since I have been in the institution, I have not seen or been visited by an information security manager to discuss matters regarding information security education and training, which I believe are very important" (DHR, Table 4.1).

> "We depend solely on CTS to protect the data we're working on."

Another respondent commented that:

> "Due to today's current storage devices on the market, one has to be trained to know how to manage organisational data."

The statement made by the director clearly affirms Viljoen's (2008:13) argument that "information security management is believed to be the responsibility of information security officers or professionals". Figure 4.5 below indicates the lack of information security skills and training among HR executives and officers.

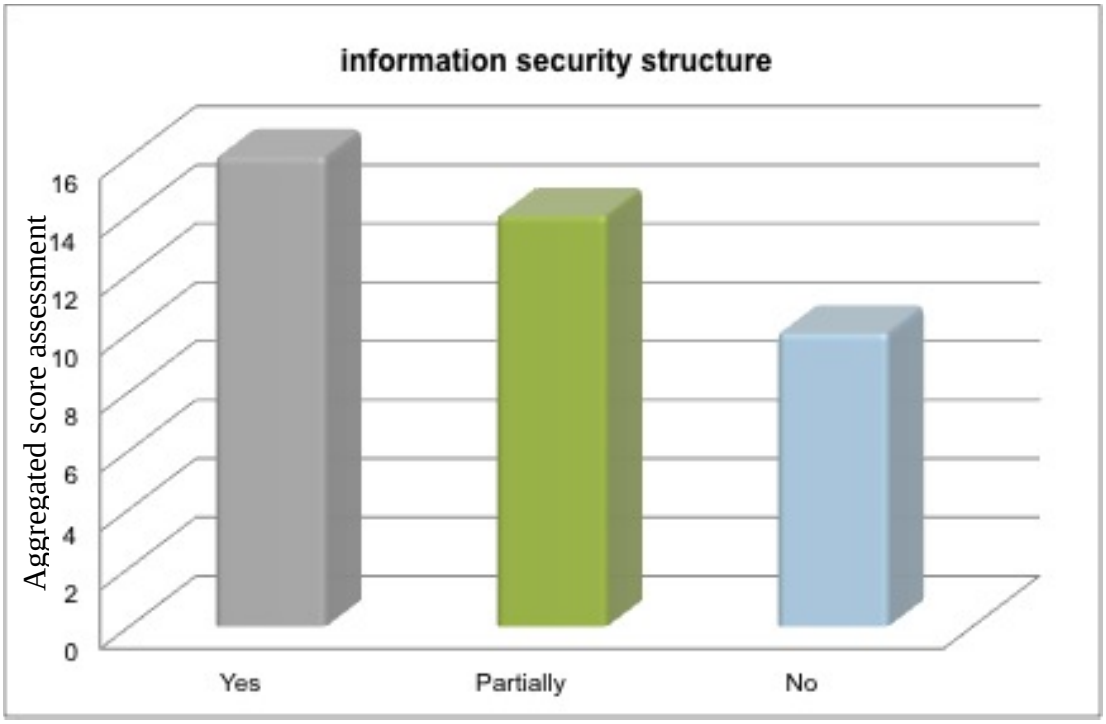


Figure 4.5: Information security skills and training

Figure 4.5 above indicates that the majority of the participants identified a lack of skills and training to be one of the major barriers to improved information security management.

4.3.5 Information security structure

In this section, participants responded that the HR department did have a strong hierarchical structure and the department relied mostly on CTS for authorised decisions relating to information security issues. Respondents noted:

> "We depend totally on CTS personnel with regard to information security issues, hardware and network security" (HRO, Table 4.1).

Figure 4.6 below illustrates the participants' responses with regard to information security structure.

Figure 4.6: Information security structure

It appears from the comments (as Figure 4.6 above illustrates), that all employees consider the CTS department and IT professionals responsible for information security standards and ensuring compliance with those standards.

4.3.6 Summary of data analysis and interpretation of data

The analysis of the information security management in the university of technology human resource information systems proves that commitment to information security issues is lacking from HR management. There is no information security awareness in the HR department, and as such, users have no idea of information security compliance regulations and policies. HR executive management's partial commitment to information security issues, indicated in Appendix A, Table 4.2, results in the slackness of information security awareness and training adoption, and minimal compliance with any information security management standards within the department.

The general impression from this analysis is that HR executive management depend solely on IT professionals with regard to information security issues. Although there is an information security structure within the university of technology, it also appears that there is a communication issue with regard to information security responsibilities.

4.4 Questions addressed in this study

This research set out to address the following question:

What are the challenges of information security management and vulnerabilities in the human resource information system in respect of employees' data management at a university of technology?

The following research sub-questions were considered:

a) *What knowledge of information security management policies and regulations do human resource personnel have*?

In response to this sub-question, interview-questions were used and respondants acknowledge the fact that, there were not aware of information security management policies and regulations and information security was seen as the responsibility of information security professional. As mentioned in chapter 4.3.4, information security practices were not properly articulated to the users and as such were not taking the responsibility to safeguard the information asset.

It was therefore recommended that, HR management at a university of technology could adopt the IT security learning scale as proposed by Wilson and Hash (2003:7) in Figure 4.7 below. Wilson and Hash declare that for data to be protected, an effective IT security programme should entail:

> *1) developing IT security policy that reflects business needs tempered by known risks; 2) informing users of their IT security responsibilities, as documented in agency security policy and procedures; and*
>
> *3) establishing processes for monitoring and reviewing the program.*

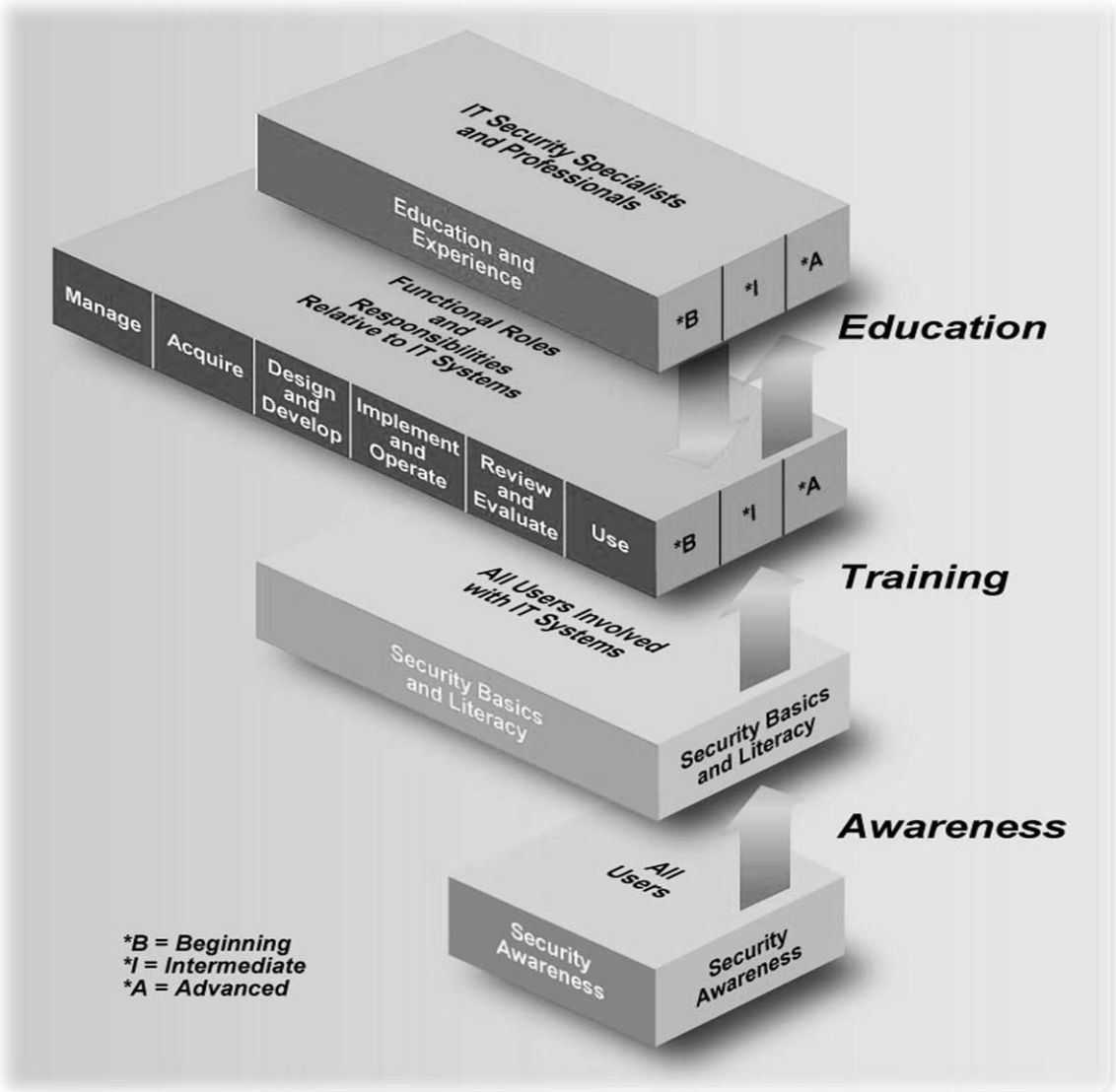


Figure 4.7: IT security learning continuum (Wilson & Hash, 2003:8)

Based on the literature and findings, a general framework was proposed to properly implement a clear information security policy and to educate users to practice information security management.

b) *What are the information security awareness, education and training programmes available for the human resource personnel?*

In response to this question, it was identified based on literature and analysis that, a university of technology needs to develop information security awareness and training programme to focus on the HR department's entire body of users. The researcher concurs with Wilson and Hash's argument that states: "Management should set the example for proper IT security behavior within an organization. An awareness program should begin with an effort that can be deployed and implemented in various ways and is aimed at all levels of the organization including senior and executive managers. The effectiveness of this effort will usually determine the effectiveness of the awareness and training program" (Wilson & Hash, 2003:7).

An awareness and training program is crucial in that it is *the* vehicle for disseminating information that users, including managers, need in order to do their jobs. In the case of an IT security program, it is *the* vehicle to be used to communicate security requirements across the enterprise.

For a university of technology to have an effective information technology security awareness and training program, proper rules of behavior for the use of a university of technology IT systems and information need to be implemented. Users first should be informed of the expectations with regards to information security practices, but accountability must be derived from a fully informed, well-trained, and aware workforce (Wilson & Hash, 2003:7).

c) How is data being properly managed within the human resource department?

In order to understand the data management within the HRIS in a university of technology, literature review from various perspectives was conducted and also analysis was done using interview-questionaires. The outcome was then used to propose the

general framework at section 5.3 in figure 5.1 to help improve data management within the HR department.

4.5 Summary

The chapter discussed the details of the research methodology used in the study. A brief outline of the participants' responses was given, and the collected data was analysed. A brief discussion of the participants' responses followed. The researcher also summarised the data analysis and gave an interpretation of the results.

CHAPTER 5: CONCLUSIONS AND RECOMMENDATIONS

5.1 Conclusions

This study investigated information security management challenges and vulnerabilities in the HRIS of data in respect of employees' data management at a university of technology. Generally, the objective of information security management in HRIS is to ensure that users (including contractors and any user of sensitive data) are aware of and understand their roles and responsibilities in accessing and using sensitive employee data of an organisation.

The objective of the study was to analyse and determine the vulnerability of data collection, data processes, data access, and data usage, and to recommend information security management standards in terms of:

- protection of organisational records;
- information security awareness, education, and training;
- technical vulnerability management; and
- management of information security incidents and improvements.

A further objective was to recommend a general information security framework to guide HR line managers, HR executives, and HR officers to better manage vital organisational data.

Sheikhpour and Modiri (2012:27) contend that, "Information security plays an important role in protecting the assets of an organization." Human resource management at a university of technology could adopt an implementation approach recommended by the researcher to use ITGI and OGC's (2008:21-22) Governance Implementation Guide (ref: Appendix E) to develop a policy to help manage and maintain data quality.

5.2 Research contribution

This section reviews the theoretical, methodological and practical contributions of the research.

5.2.1 Theoretical contribution

- In terms of theory formation, relevant literature was studied and a conceptual framework was developed to assist in data collection and analysis. This research

study explains human resources personnel's awareness and knowledge of information security issues with regard to data management. The outcomes identify a lack of the required skills, as well as accountability by management, with regard to information security with the HR department. Furthermore, to address the skills gap within the human resource department, a general framework is proposed to bridge the skills gap relating to information security.

- From a theoretical perspective, the study adds to the body of knowledge in respect of the practices and attitudes towards information security within an HR department in a university of technology.

5.2.2 Methodological contribution

- With regard to research methodology, the study also illustrates that qualitative methods, especially the case study method, were found to be valuable in exploring new insights.
- It is recommended that HR executive management employ an information security specialist within the HR department to manage information security issues by creating awareness, through training, and by educating the users.
- Furthermore, a university of technology information security professional should adopt the framework of CoBiT and ISO/IEC 27002 to increase the value of information technology, and to enable alignment and good practice for information technology control throughout the HR department.

5.2.3 Practical contribution

The present study highlights several managerial loopholes with regard to information security. HR management needs to be able to develop and deploy information security practice within the department. The key practical contributions relating to information security practices for the body of knowledge are presented below. HR management needs to ensure that:

- information security education and training is provided to all HR executive management and HR officers;
- attention is paid to users' information security awareness and training programmes;
- periodic monitoring and evaluation of the security programmes are done;

- there are ongoing presentations and feedback from users and managers with regard to the impact of the security programme.

5.3 Recommendation

The vulnerabilities that existed between information security management, users, and human resource business processes in the conceptual framework in this study was demonstrated and identified as information awareness, information security education and training and data quality as shown in Figure 5.1 below. The study further identified a paucity of research in the area of information security management in a human resources information system at a university of technology.

The recommendation of this study is redolent of the research done by Wilson and Hash (2003) and Yeo et al. (2007). The uniqueness of this study is that it focused on a specific department and how information security management is practised within the department. Previous researchers on information security management have targeted the entire organisational practices of information security.

The study therefore recommends a general framework, based on the conceptual framework used to help collect data, and the data analysis, to support HR management to embrace information security management as part of their core business strategy for data quality and data security. Figure 5.1 below illustrates a proposed general framework to be adopted by all members of executive management within a university of technology to manage vital institutional information.

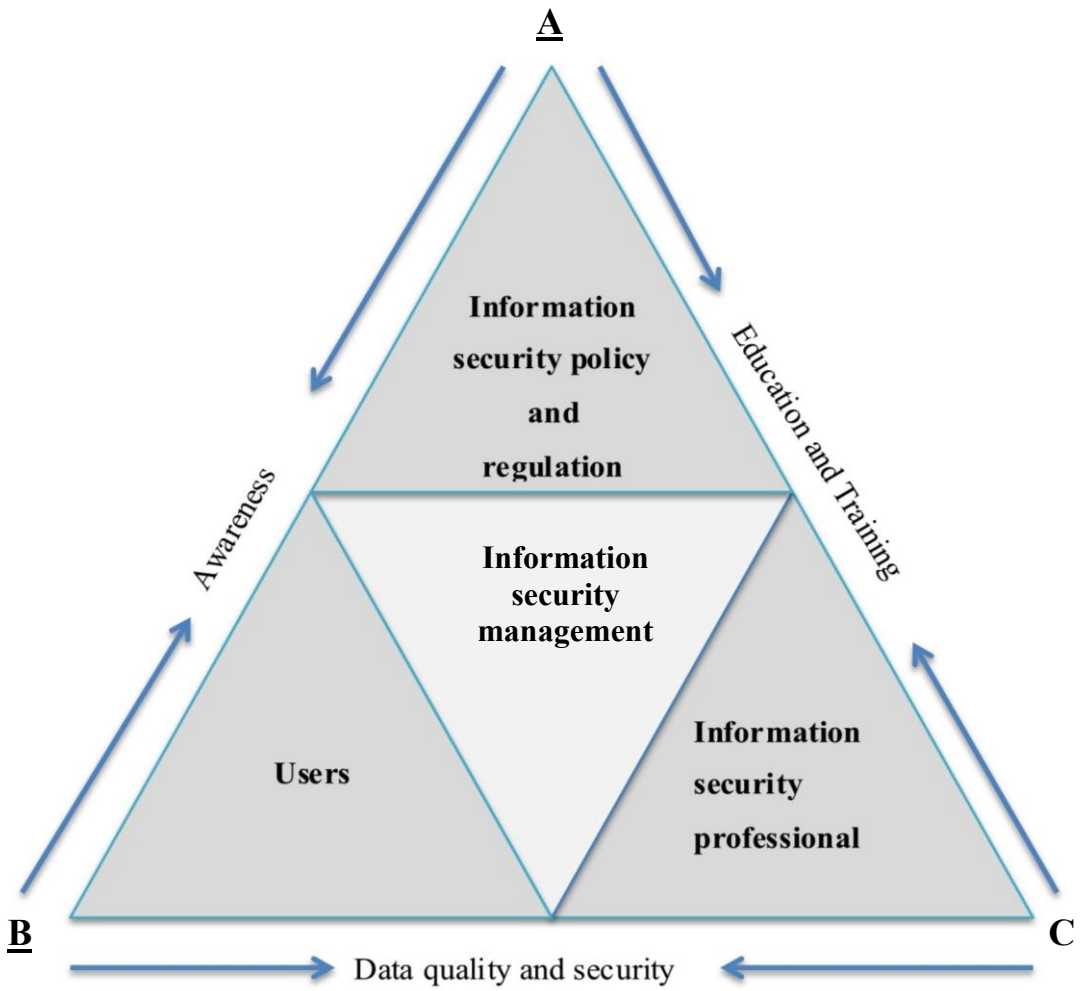


Figure 5.1: A proposed general information security management framework

The general framework above is further explained below:

5.3.1 Awareness

Information Security awareness should be focused on to improve the attitude of HR personnel towards information security as highlighted by Wilson and Hash (2003) in previous chapters. The direction of the arrows on side A and B proposes that users informed of information security policy and regulations build a strong foundation for information security compliance within a university of technology. The effectiveness of most security measures depends largely on the behaviour of the users affected by those measures. HR management should put in place an information security awareness programme to motivate HR officers and external users with regard to information security issues and their responsibilities. In addition, it is advisable for the HR management to reinforce institutional security values over time to maintain security awareness.

5.3.2 Education and training

HR officers should be aware of security issues and need to be educated and trained for their role with regard to security concerns and solutions; they should also understand their role in making security measures effective. A and C on Figure 5.1 proposes that HR management needs to integrate an information security professional into the HR department to facilitate information security education and training issues within the department. Such an information security professional would then motivate users to adhere to the information security policies and regulations, and enforce compliance with these. HR management needs to investigate education and training as an investment for data quality and data security.

5.3.3 Data quality and data security

A well-implemented information security awareness programme, information security education, and training (Figure 5.1), will lead to quality data and secure data within HR information systems. This proposed general information security management framework for a university of technology human resource information system should help bridge the gap that exists between information security policies and regulations, users and HR officers in their day-to-day data management.

5.4. Summary

This chapter concludes the disertation and outlines the research contributions. The chapter has also recommended a general information security framework to improve information security within the HR department at a university of technolgy.

5.5 Summary of dissertation

The rationale for this research study emanated from the ongoing concern that information security should not be the exclusive responsibility of information security experts with technical expertise or of executive management. It is the responsibility of *all* an organisation's employees to manage and maintain institutional data securely.

Chapter 1 of the study introduced the dissertation by describing the background of the research, terminology used, and rationale for the research. The research problem and the objectives of the research were further outlined, and the research methodology, scope of the research and an overview of the research layout were discussed.

Chapter 2 introduced the relevant literature and the purpose of information security, governance and factors affecting information security at a university of technology. A conceptual framework was developed based on the literature reviewed and was used to assist in the data collection and analysis. The chapter further highlighted prior research with regard to information security and standards that govern information security. In this chapter, the role of information security in organisations was discussed.

Chapter 3 gave an overview of the objectives of the research study and the methodologies considered for the study. It further introduced the university of technology chosen for the field study and the case study used for the research. The main data collection tools employed was interview-questionnaires, and face to face observation. Questionnaires were important in that they allowed the researcher to elicit the responses of HR staff within the university of technology.

Chapter 4 reflected on the analysis and interpretation of the data collected through the interview-questionnaires. The results obtained from the questionaires were particularly important in highlighting the information security management commitment levels of HR managers and HR officers. In the next chapter, the findings were used to propose a general framework to help govern institutional essential data and to recommend information security practices.

Chapter 5 concluded the dissertation and outlined the research contributions. The chapter also recommended a general information security framework to improve information security within the HR department at the university of technolgy, and finally recommended future research that could be done.

5.6. Future research

The study was able to provide a theoretical framework for information security management, while gaps between theory and practice were observed within the university of technology in question. The gaps that require attention are in respect of integrating various information security management mechanisms that may exist within the organisation and raising the awareness and understanding of the concept of information security among executives.

There are a number of research limitations that should be acknowledged. First, the research model is theoretical and as such could be further developed. It should be noted that:

- The research could be replicated with a wider sample of organisations to provide more refined results and potential for generalisation within the university sector.
- The research participants of this study were the HR director and HR officers of the organisation who are the key personnel in the HR department.
- Further studies could also focus on CIOs/IT – their characteristics, what they do, how they do it and especially how they influence IT governance performance.

REFERENCES

Armoni, A. 2002. Data security management in distributed computer systems. *Informing Science Journal: The International Journal of an Emerging Transdiscipline*, 5(1):19-27.

Bradley, T. 2013. Data protection and information lifestyle management. Chapter 1: Introduction to data protection. http://netsecurity.about.com/od/chapterexcerpts/a/aaexc_datailm.htm [20 October 2013].

Burrell, G. & Morgan, G. 1979. *Sociological paradigms and organisational analysis: elements of the sociology of corporate life.* London: Heinemann.

BusinessDictionary.com. 2014. http://www.businessdictionary.com/definition/data.html [24 April 2014].

Cape Peninsula University of Technology. 2012. History of Cape Peninsula University of Technology. http://www.cput.ac.za/history [12 September 2012].

Doherty, N.F. & Fulford, H. 2008. Do information security policies reduce the incidence of security breaches? An exploratory analysis. In Nemati, H. (ed.). *Information security and ethics: concepts, methodologies, tools, and applications.* Hershey, PA: Information Science Reference: 964-980.

Duncan, J-A. 2012. The Protection of Personal Information Bill: safeguarding privacy or permitting secrecy? http://www.archivalplatform.org/blog/entry/popia/
[3 December 2013].

Gijana, A.P. 2011. Assessing challenges in public appointments and recruitment processes in Chris Hani District Municipality: a case study of human resource department in Lukhanji Municipality (2008–2010). Unpublished MPA thesis, University of Fort Hare, South Africa.

Herath, T. & Rao, H.R. 2009. Encouraging information security behaviors in organizations: role of penalties, pressures and perceived effectiveness. *Decision Support*

Systems, 47(2):154-165, May.

Information Security Forum. 2007. Information leakage. *ISF Briefing*, (4), October.

Information Systems Audit and Control Association. 2005. Critical elements of information security program success. http://www.isaca.org/Knowledge-Center/Research/Documents/Critical-Elements-of-Information-Security-Program-Success_res_Eng_0105.pdf [13 October 2013].

International Organization for Standardization. n.d. Standards. http://www.iso.org/iso/home/standards.htm [17 April 2014].
ISACA *see* Information Systems Audit and Control Association.

ISO/IEC 27002:2005. Information technology — Security techniques — Code of practice for information security management.

IT Governance Institute. 2001. Information security governance: guidance for boards of directors and executive management. Rolling Meadows, IL: ITGI. http://citadel-information.com/wp-content/uploads/2010/12/isaca-information-security-governance-guidance-for-boards-of-directors-and-executive-management-2001.pdf [19 January 2014].

IT Governance Institute and Office of Government Commerce. 2008. Aligning CoBiT®, ITIL® and ISO/IEC 27002 for business benefit. Management summary. A management briefing from ITGI and OGC. http://www.onuva.com/wp-content/uploads/2013/04/Aligning_COBITITILV3ISO27002_Bus_Benefit_9Nov08_Research.pdf [16 February 2014].

Ngobeni, S.J & Grobler, M.M. 2009. Information Security policies for Governmental Organisations, the minimum criteria. Information Security South Africa (ISSA2009) Conference, University of Johannesburg, Gauteng, South Africa, 6 - 8 July, 2009.http://icsa.cs.up.ac.za/issa/2009/Proceedings/Research/50.pdf [24 February 2013]

Sheikhpour, R. & Modiri, N. 2012. An approach to map COBIT processes to ISO/IEC information security management controls. International Journal of Security and its Applications, 6(2):13-28, April.

South Africa. 2013. Protection of Personal Information Act, Act No. 4 of 2013. *Government Gazette*, 581(37067), 26 November 2013. http://www.justice.gov.za/legislation/acts/2013-004.pdf [20 November 2013].

University of California, San Francisco. n.d. Guide to managing human resources: a resource for managers and supervisors. http://ucsfhr.ucsf.edu/index.php/pubs/hrguidearticle/chapter-1-employment/ [21 October 2013].

US General Accounting Office. 1998. Executive guide. Information security management. Learning for leading organizations. Washington, DC: US General Accounting Office. GAO/AIMD-98-68. http://www.gao.gov/assets/80/76396.pdf [12 November 2013].

Vessey, I., Ramesh, V. & Glass, R.L. 2002. Research in information systems: an empirical study of diversity in the discipline and its journals. *Journal of Management Information Systems*, 19(2):129-174, Fall.

Viljoen, M. 2008. A framework towards effective control in information security governance. Unpublished MTech: IT thesis, Nelson Mandela Metropolitan University, Port Elizabeth, South Africa.

Von Solms, B. & Von Solms, R. 2005. From information security to … business security. *Computers & Security*, 24(4):271-273, June.

Wilson, M. & Hash, J. 2003. Building an information technology security awareness and training program. Recommendations of the National Institute of Standards and Technology. 1st Draft, July 2002. Washington, DC: US Government Printing Office. NIST Special Publication 800-50.

http://www.iwar.org.uk/comsec/resources/nist/draft800-50.pdf [20 January 2013].

Wisker, G. 2014. Choosing appropriate research methodologies and methods. http://www.palgrave.com/skills4study/studentlife/postgraduate/choosing.asp [16 April 2014].

Yeo, A.C., Ramin, M.M. & Miri, L. 2007. Understanding factors affecting success of information security risk assessment: the case of an Australian higher educational institution. *Proceedings of the Pacific Asia Conference on Information Systems (PACIS) 2007, Auckland, New Zealand, 4 – 6 July 2007*. Paper 74. http://aisel.aisnet.org/pacis2007/74 [19 February 2013].

APPENDIX A

A summary of participants' interview questions responses.

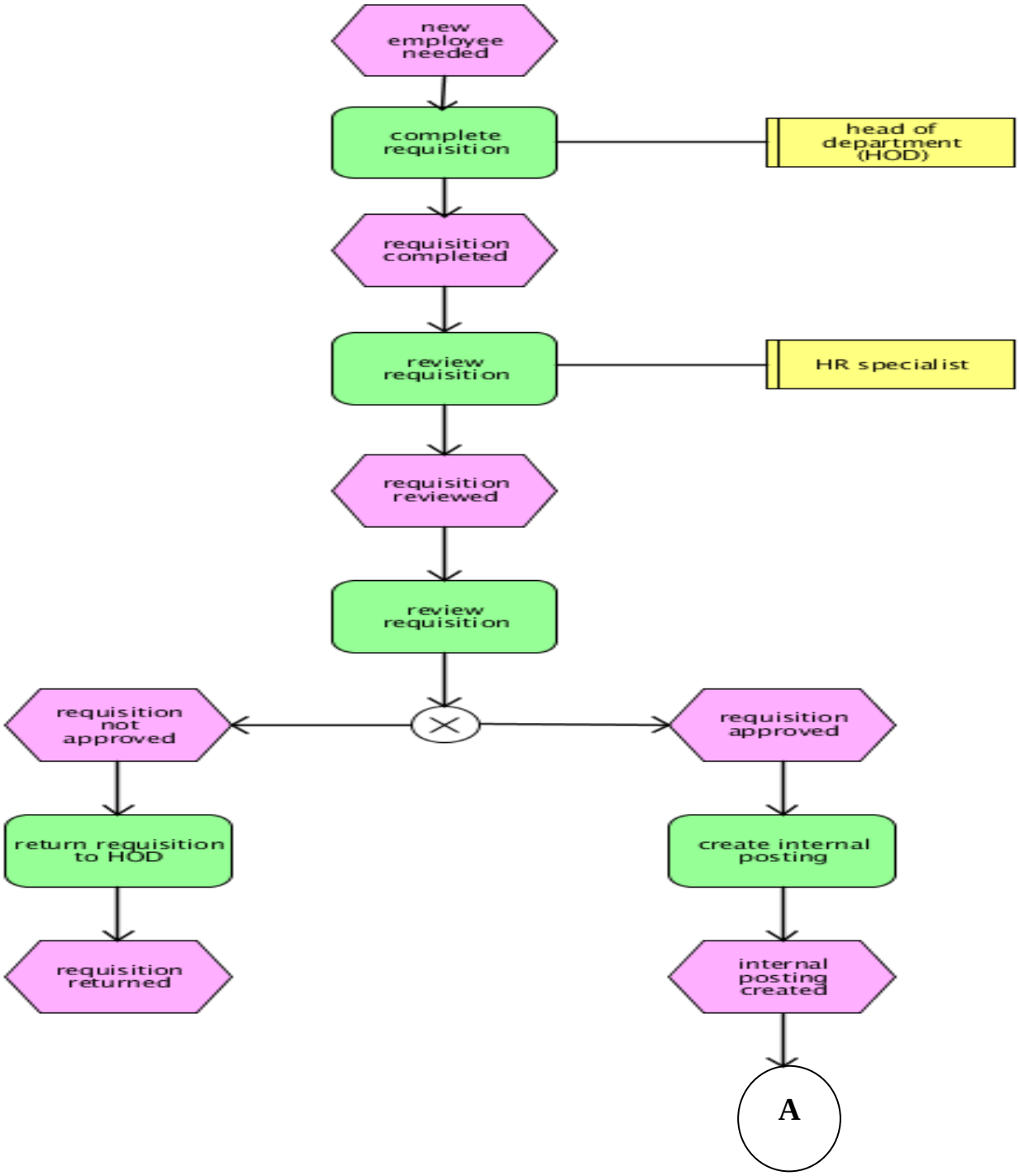
Management commitment:	Yes	Partially	No
HR top management considers information security an important organisational priority.	[7]	[8]	[5]
HR executives give strong and consistent support to security programme.	[7]	[9]	[4]
Management has identified information security threats and vulnerabilities associated with each of the critical assets and functions within the department.	[4]	[12]	[4]
The department conducts risk assessment to identify the key objectives that need to be supported by information security programme.	[6]	[10]	[4]
Score	**24**	**39**	**17**
Security compliance			
There is a clear procedure to discipline members who violate organizational security policy and regulations.	[6]	[14]	[0]
Information security rules are enforced by all HR managers.	[7]	[13]	[0]
Password sharing among users is an issue in the department.	[8]	[4]	[8]
The department routinely conducts information security audits and maintains historical records/data of information misuse or intrusion attempts.	[4]	[12]	[4]
Score	**25**	**43**	**12**
Awareness:	Yes	Partially	No
There are appropriate awareness programmes to ensure that members of the department are aware of their security responsibilities (e.g. training sessions/workshops on security organised).	[4]	[6]	[10]
Members of the department take information security courses as part their education.	[0]	[6]	[14]
Score	**4**	**12**	**24**
Skills and training:			
There is a regular and structured training programme for all	[0]	[6]	[14]

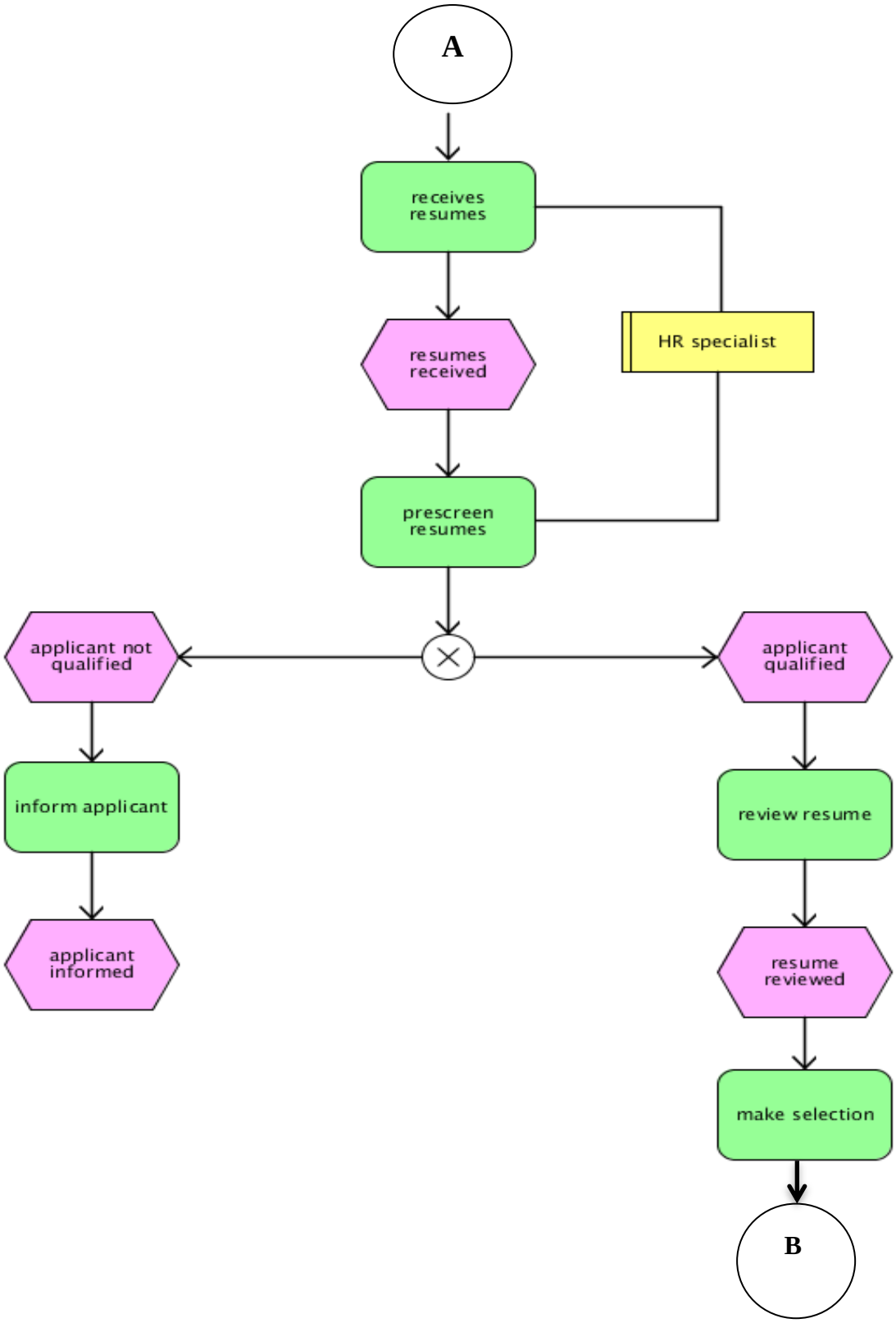
members on information security.			
There is adequate in-house information security expertise for all supported services, devices and technologies.	[6]	[5]	[9]
Score	**6**	**11**	**23**
Information security structure:			
The department has a strong hierarchical structure.	[8]	[6]	[6]
IT staff are authorised to make important decisions related to information security issues.	[8]	[8]	[4]
Score	**16**	**14**	**10**

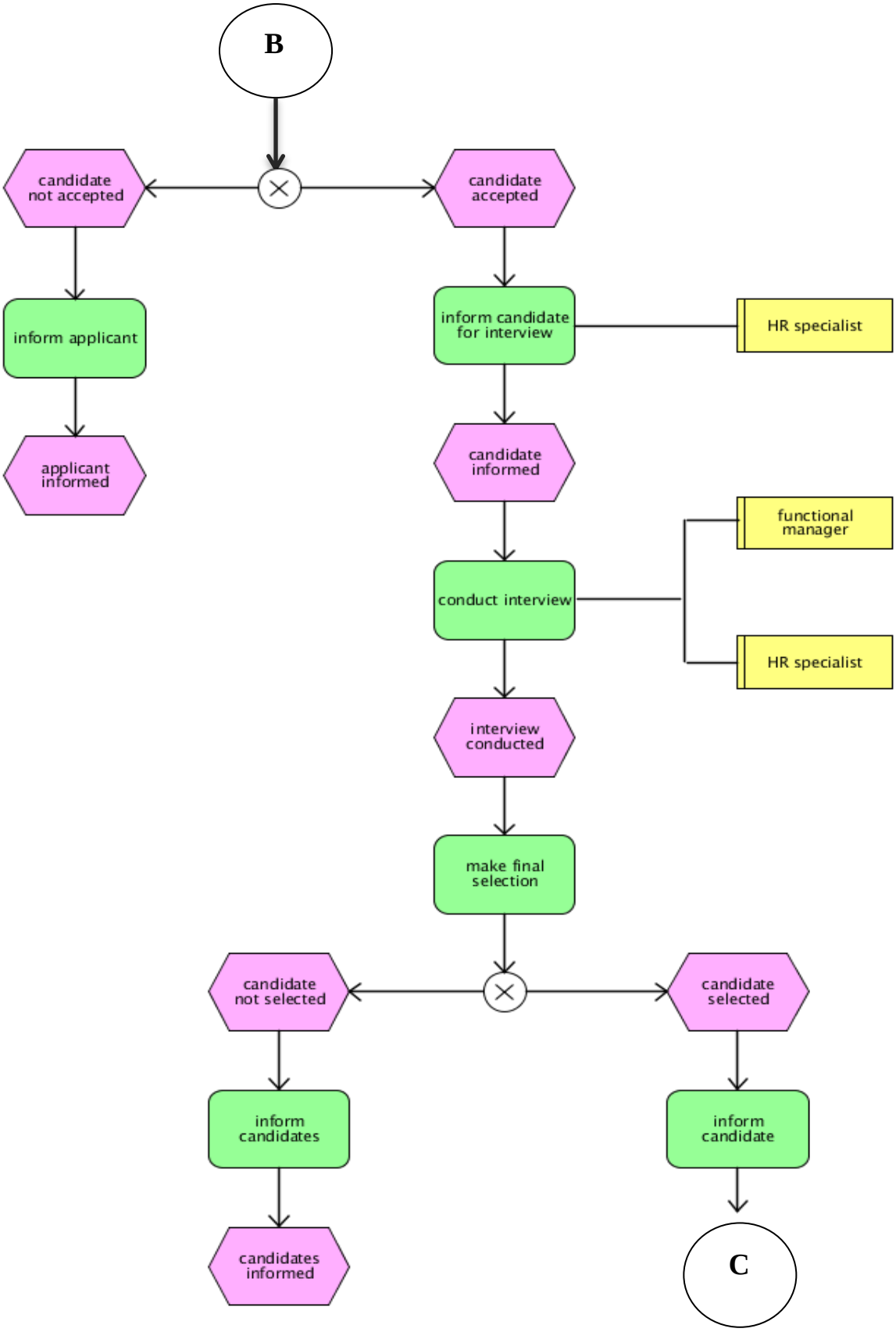
Analysis of the research data

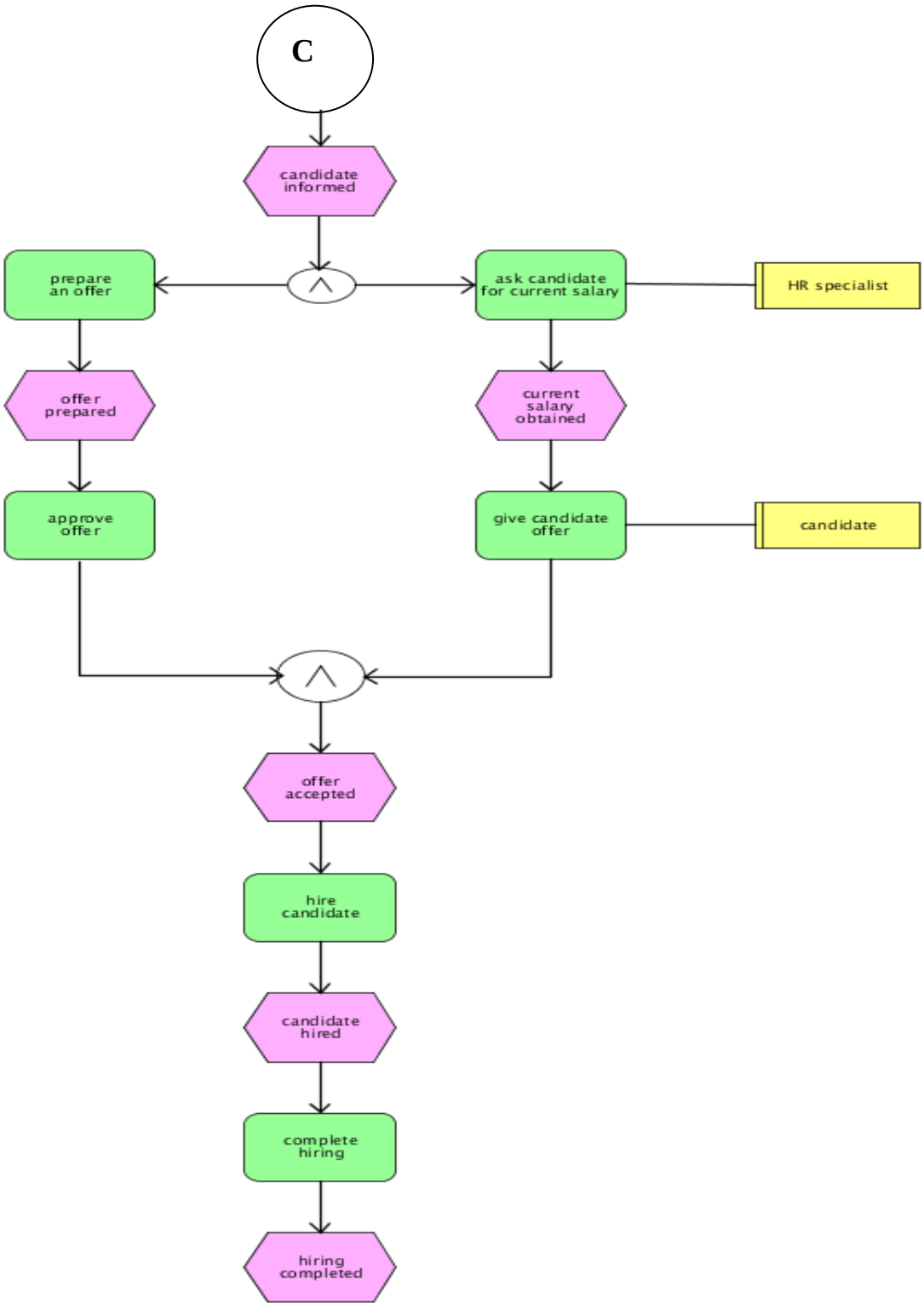
APPENDIX B

Detailed human resources business processes



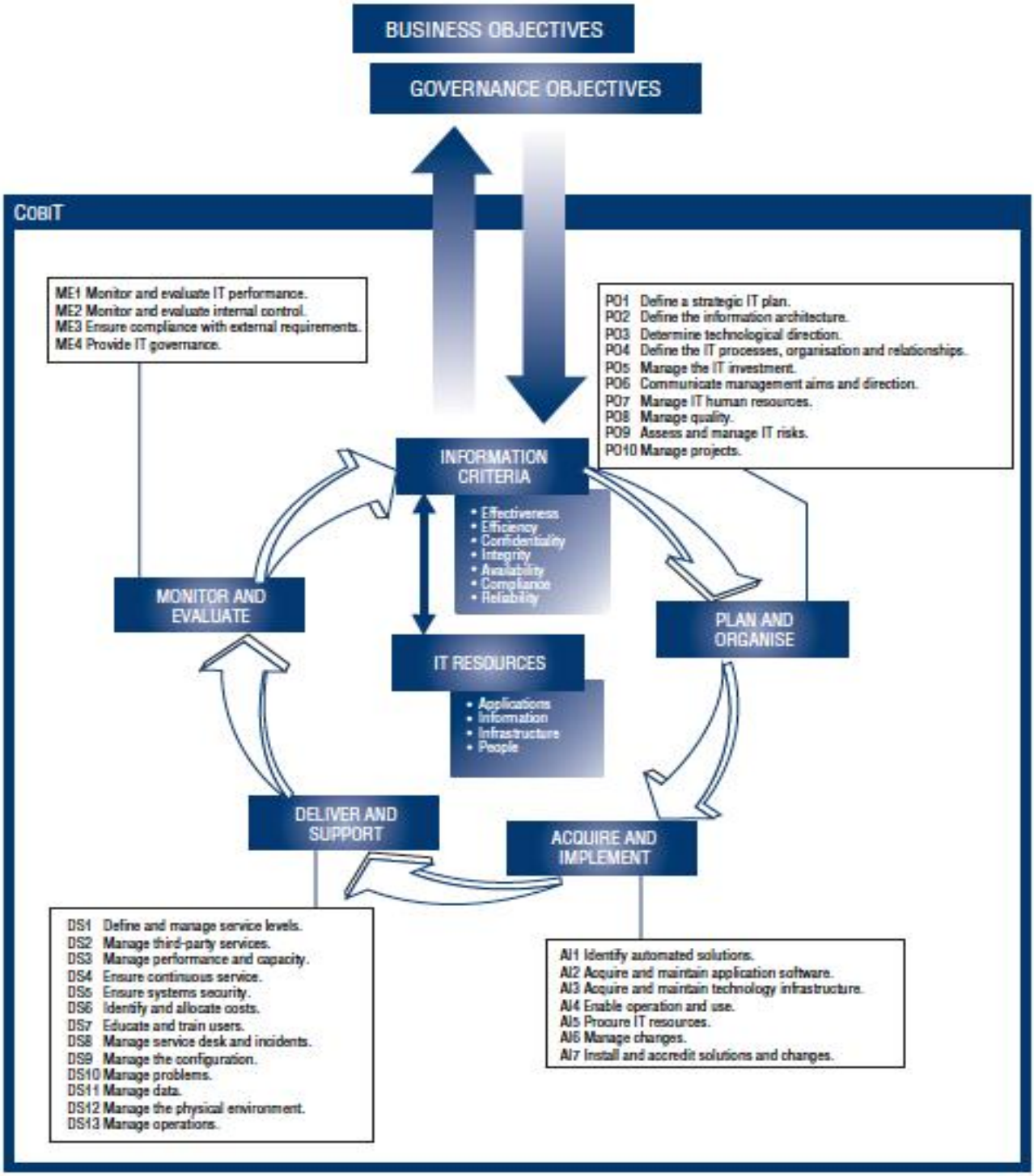

A
receives resumes
resumes received
HR specialist
prescreen resumes
applicant not qualified
applicant qualified
inform applicant
review resume
applicant informed
resume reviewed
make selection
B


B
candidate not accepted
candidate accepted
inform applicant
inform candidate for interview
HR specialist
applicant informed
candidate informed
functional manager
conduct interview
HR specialist
interview conducted
make final selection
candidate not selected
candidate selected
inform candidates
inform candidate
candidates informed
C


C
candidate informed
prepare an offer
ask candidate for current salary
HR specialist
offer prepared
current salary obtained
approve offer
give candidate offer
candidate
offer accepted
hire candidate
candidate hired
complete hiring
hiring completed

APPENDIX C

CoBiT 34 high-level control objectives



Source: Information Systems and Audit and Control Association, 2005

APPENDIX D

PART 1

---

1. Please state your job function in the HR department

……

2. What do you consider to be the top three main causes of information security incidents in your department? *Please select three.*

- Malwares
- System or software errors
- Cyber or internal-based attacks
- User error or non-compliance
- Hardware failure
- Third parties
- Other (*please specify)* ……..

3. In your view, what do you consider to be the top three barriers or obstacles to achieving improved security compliance? *Please select three.*

- Lack of information security awareness and training programmes
- Lack of adequate technology
- Lack of clear direction in security procedures and roles
- Lack of motivation programmes
- Lack of management involvement in security issues

PART 2

Please choose the answer that best reflects your opinion about the department you work for.

Yes – indicates the practice is implemented

Partially – indicates that part of the practices is implemented

No – indicates the practice is not implemented at all

This section assesses the HR department aspects of the information security programme:

Management commitment:	Yes	Partially	No
HR top management considers information security an important organisational priority.	[ ]	[ ]	[ ]
HR executives give strong and consistent support to security programme.	[ ]	[ ]	[ ]
Management has identified information security threats and vulnerabilities associated with each of the critical assets and functions within the department.	[ ]	[ ]	[ ]
The department conducts risk assessment to identify the key objectives that need to be supported by information security programme.	[ ]	[ ]	[ ]
Security compliance:			
There is a clear procedure to discipline members who violate organisational security policy and regulations.	[ ]	[ ]	[ ]
Information security rules are enforced by all HR managers.	[ ]	[ ]	[ ]
Password sharing among users is an issue in the department.	[ ]	[ ]	[ ]
The department routinely conducts information security audits and maintains historical records/data of information misuse or intrusion attempts.	[ ]	[ ]	[ ]
Awareness:	Yes	Partially	No

There are appropriate awareness programmes to ensure that members of the department are aware of their security responsibilities (e.g. training sessions/workshops on security organised).	[ ] [ ] [ ]
Members of the department take information security courses as part their education.	[ ] [ ] [ ]
Skills and training:	
There is a regular and structured training programme for all members on information security.	[ ] [ ] [ ]
There is adequate in-house information security expertise for all supported services, devices and technologies.	[ ] [ ] [ ]
Information security structure:	
The department has a strong hierarchical structure.	[ ] [ ] [ ]
IT staff are authorised to make important decisions related to information security issues.	[ ] [ ] [ ]

APPENDIX E

ITGI and OGC's IT Governance Implementation Guide (ITGI & OGC, 2008)

1. Set up an organisational framework (ideally as part of an overall IT governance initiative), with clear responsibilities and objectives and participation from all interested parties who will take implementation forward and own it as an initiative.
2. Align IT strategy with business goals. In which current business objectives does IT have a significant contribution? Obtain a good understanding of the business environment, risk appetite and business strategy as they relate to IT. CobiT's management guidelines (specifically the goals and metrics) help define IT objectives. Used in conjunction with ITIL, services and service level agreements (SLAs) can be defined in end-user terms.
3. Understand and define the risks. Given the business objectives, what are the risks relating to IT's ability to deliver against these objectives? Consider:
    - Previous history and patterns of performance
    - Current IT organisational factors
    - Complexity and size/scope of the existing or planned IT environment
    - Inherent vulnerability of the current and planned IT environment
    - Nature of the IT initiatives being considered, e.g., new systems projects, outsourcing considerations, architectural changes
4. Define target areas and identify the process areas in IT that are critical to delivering value and managing these risk areas. The CobiT process framework can be used as the basis, underpinned by ITIL's definition of key service delivery processes and ISO/IEC 27002 security objectives. OGC's publication, *Management of Risk: Guidance for Practitioners* can also be of assistance in assessing and managing risks at any of the four main levels, i.e., strategic, programme, project or operational
5. Analyse current capability, and identify gaps. Perform a maturity capability assessment to find out where improvements are needed most. The CobiT maturity models provide a basis supported in more detail by ITIL and ISO/IEC 27002 best practices.
6. Develop improvement strategies, and decide which are the highest priority projects that will help improve the management and governance of these

significant areas. This decision should be based on the potential benefit and ease of implementation, with a focus on important IT processes and core competencies. Specific improvement projects as part of a continuous improvement initiative should be outlined. The CobiT control objectives and control practices can be supported by more detailed ITIL and ISO/IEC 27002 guidance.

7. Measure results, establish a scorecard mechanism for measuring current performance and monitor the results of new improvements considering, as a minimum, the following key questions:
   - Will the organisational structures support strategy implementation?
   - Are responsibilities for risk management embedded in the organisation?
   - Do infrastructures exist that will facilitate and support the creation and sharing of vital business information?
   - Have strategies and goals been communicated effectively to everyone who needs to know within the organisation?
8. Repeat steps 2 through 7 on a regular basis.