IT AUDITS IN SOUTH AFRICAN HIGHER EDUCATION INSTITUTIONS

A thesis submitted in partial fulfilment of the
requirements for the degree of

Master of Science

of

Rhodes University

by

Lynne Angus

December 2012

Abstract

The use of technology for competitive advantage has become a necessity, not only for corporate organisations, but for higher education institutions (HEIs) as well. Consequently, corporate organisations and HEIs alike must be equipped to protect against the pervasive nature of technology. To do this, they implement controls and undergo audits to ensure these controls are implemented correctly. Although HEIs are a different kind of entity to corporate organisations, HEI information technology (IT) audits are based on the same criteria as those for corporate organisations. The primary aim of this research, therefore, was to develop a set of IT control criteria that are relevant to be tested in IT audits for South African HEIs. The research method used was the Delphi technique. Data was collected, analysed, and used as feedback on which to progress to the next round of data collection. Two lists were obtained: a list of the top IT controls relevant to be tested at any organisation, and a list of the top IT controls relevant to be tested at a South African HEI. Comparison of the two lists shows that although there are some differences in the ranking of criteria used to audit corporate organisations as opposed to HEIs, the final two lists of criteria do not differ significantly. Therefore, it was shown that the same broad IT controls are required to be tested in an IT audit for a South African HEI. However, this research suggests that the risk weighting put on particular IT controls should possibly differ for HEIs, as HEIs face differing IT risks. If further studies can be established which cater for more specific controls, then the combined effect of this study and future ones will be a valuable contribution to knowledge for IT audits in a South African higher education context.

Acknowledgements

I would like to thank my employer and fellow colleagues in allowing me the time afforded on this thesis during a very busy period. I acknowledge and appreciate that part-time study puts added pressure on fellow colleagues.

I would like to thank Dr Barry Irwin for his assistance in exploring and identifying various thesis topics.

I would like to thank my supervisor, Dr Karen Bradshaw, for all her guidance throughout the research process and the writing of this thesis. Her assistance and support is greatly appreciated.

Thanks also go to my colleague, Mr Trevor Amos, for his valued knowledge and guidance in the use of the Delphi technique.

My grateful thanks to the twelve professionals who participated so willingly in this study. I realise it took great effort and time out of their busy schedules to respond to each survey over a number of months. I am truly humbled by their efforts and greatly appreciative.

Lastly, I would like to thank my family for their continued support and encouragement.

Table of Contents

List of Tables

List of Figures

Glossary

ASAUDIT – Association of South African University Directors of Information Technology

CFO – Chief Financial Officer

CIO – Chief Information Officer

COBIT – Control Objectives for Information and related Technology

HEI – Higher Education Institution

HEMIS – Higher Education Management Information System

ISACA – Information Systems Audit and Control Association

IT – Information Technology

ITGC – Information Technology Governance Committee

ITIL – Information Technology Infrastructure Library

PDCA – Plan-Do-Check-Act

PPI – Protection of Private Information

SARS – South African Revenue Services

SME – Small-and Medium-Sized Enterprises

US – United States (of America)

Chapter 1 Introduction

Many organisations recognise the potential benefits that technology can yield. Successful organisations, however, understand and manage the risks associated with information technology (IT) (IT Governance Institute, 2000) by carrying out IT audits. IT audits usually follow standards and guidelines for what must be assessed. The question is whether these standards are applicable in all sectors of the economy, and more specifically, to higher education institutions (HEIs). The research area for the proposed study is IT audits in South African higher education institutions.

1.1 Context of the Research

The advent of technology has had a major impact on the way organisations do business. IT has increased the ability to capture, store, analyse, and process huge amounts of data and information, which has in turn empowered the business decision-maker immensely (Gallegos, Manson and Allen-Senft, 1999). Additionally, IT has become the lifeblood of any large organisation in that it does not merely record business transactions, but actually drives the key business processes of the organisation (Sayana, 2002). Further to that, Gallegos et al. (1999) argue that "the increased connectivity and availability of systems and open environments have proven to be the lifelines of most business entities". In these ways and more, the use of IT heavily impacts the organisation's strategy and competitive advantage.

Unfortunately, advancements in technology introduce new problems that must be faced by organisations. Reports of white-collar crime, information theft, computer fraud, information abuse, and other IT concerns that threaten the livelihood of organisations, are now rife. Organisations also have legal obligations to ensure that their IT systems behave appropriately, for example the Protection of Personal Information (PPI) Bill in South Africa (2012) requires that organisations ensure the privacy of its customers' data held in its computer systems. As a result, organisations must be more conscious of the pervasive nature of technology and ensure that IT is adequately governed, and controls are in place to maintain data integrity and manage access to information.

The IT Governance Institute (2007, p. 5) describe IT governance as "the responsibility of executives and the board of directors, and consists of the leadership, organisational structures and processes that ensure that the enterprise's IT sustains and extends the organisation's strategies and objectives". Controls within an IT infrastructure are the policies, procedures and practices which, if implemented correctly, allow for adequate IT governance to be obtained.

Weber (1999) states that "information systems auditing[1] is the process of collecting and evaluating evidence to determine whether a computer system safeguards assets, maintains data integrity, allows organisational goals to be achieved effectively, and uses resources effectively". The organisation's IT infrastructure uses controls to achieve this so the IT audit must ensure that adequate IT controls exist for the organisation. The purpose of the IT audit is to review the IT controls in place for perceived weakness and areas for improvement, and provide feedback, assurance and suggestions (Sayana, 2002).

An IT audit often involves finding and recording observations that are highly technical and such technical depth is required to perform effective IT audits (Sayana, 2002). At the same time it is necessary to translate audit findings into vulnerabilities and businesses impacts to which management can relate (ibid.). Therein lies a main challenge of the IT audit (ibid.). Another challenge is how the auditor knows which controls to audit. IT control frameworks form the basis of IT audits and are used as a guide to know which controls to audit and how to relate findings to business goals. This brings us to the research problem area.

1.2 The Research Problem

IT control frameworks are used in organisations as a guide for implementation of a sound IT infrastructure. These frameworks are also used as a base on which to audit the organisations' IT. More detail on IT controls and how they fit into frameworks is given in Sections 2.2 and 2.3. Frameworks have been created based on IT in corporate organisations, and thus, the use of frameworks to achieve the most out of an organisation's IT and as a means of audit and control is already in place for corporate organisations. However, can the same frameworks be

[1] The term "information systems auditing" is used interchangeably with "IT auditing" in this paper.

applied effectively in a higher education context? Do IT audits carry out relevant testing on HEIs, when based on corporate IT control frameworks? Herein appears to be a gap in current knowledge and thus, the area for this research.

1.3 Objectives of the Research

The primary aim of this research is to develop a set of IT control criteria that are relevant to an IT audit in a South African HEI.

The study is further expanded to include the following research objectives:

- To determine whether there are differences between corporate organisations and HEIs in terms of IT.
- To assess whether it is fitting to use generic IT control criteria to audit an HEI.
- To identify control criteria (including the associated ranking of these criteria) relevant to IT audits in HEIs.

1.4 Research Methodology

The participants in this study were a group of twelve IT professionals in HEIs and IT auditors around the country. Participation was on a voluntary basis and communication was via email. The study made use of a methodology known as the Delphi technique which involved obtaining opinion from experts in the field regarding the research question through the use of email and online surveys, analysing the data, and presenting it back to the participants in further rounds until consensus of opinion had been reached on the IT control criteria to be used to audit an HEI. This iterative process increased the rigour of the study and improved its validity.

1.5 Importance of the Research

The purpose of IT auditing in HEIs is to ensure that the institution is getting the most out of its IT resources and, at the same time, managing risks. It is therefore important for an IT audit to assess the correct controls relative to the context of the organisation. The importance of this study lies in the generation of a model set of IT control criteria that are definitively relevant in a South African higher education context and can be used to audit a South African HEI. By using this model, an HEI can adequately assess and minimise the risks associated with the implementation of IT infrastructure, and in so doing, is better enabled to align IT with strategic goals and compete successfully within the market. This is increasingly important as IT becomes core for organisations and HEIs competing in the market today.

1.6 Feasibility of the Study

A small sample has the capacity to lessen the reliability and validity of a study, and therefore lower its feasibility. It is believed that the use of experts in the field as opposed to a general sample, as well as it being a normal sample size for the use of the Delphi technique, negates the risk of lower feasibility. As stated in Section 1.5, the iterative nature of the Delphi technique lends itself to increased validity in that opinions are confirmed in a number of rounds and there is less opportunity for misinterpretation.

1.7 Limitations and Assumptions

The following two subsections present the limitations and assumptions of this research. A discussion of the consequences thereof is presented in Section 5.2

1.7.1 Limitations

- The data collection process was via email and online survey. This is a static medium and provides less opportunity for discussion between participants.

- The use of questionnaires has its disadvantages, such as possible use of leading questions, or ambiguity and misunderstanding of questions by participants.
- Apart from their interest in the research question, the participants had no incentive to participate. This could introduce less reliable results, and lead to lower response levels and higher attrition rates.
- The attrition rate is further increased by the use of the Delphi technique as its iterative nature requires participants to be open to months of questioning which could become exhaustive and decrease interest, therefore decreasing participation.
- Owing to the range of work experience by participants from the positions they hold to the IT systems they work with, the study could not be too specific in terms of the control criteria. A high-level view could achieve a less reliable result than one that is more specific.

1.7.2 Assumptions

- The study required an assumption to be made on the definition of an expert in this field. It was decided that an expert needed to have IT experience as well as experience in IT auditing, either as an auditor or someone who has been part of an audit in an HEI. The job level of the participant was also taken into account. A person at the middle to higher management level was considered appropriate.
- Kendall's coefficient of concordance (described in Section 3.4) was used as a statistical measure to ascertain whether acceptable agreement was obtained by participants in order to progress onto further rounds. The assumption for this research was that a value of 0.5 or greater for this statistic meant agreement.

1.8 Document Structure

Chapter two focuses on the foundations of this study, states the problem area by giving a critical review of the relevant literature and allows for the objectives of this research to be drawn from it.

Chapter three describes the research methodology used. It also gives details of how the participants were selected, the data collection media used, how the data were analysed to progress onto further rounds, and the statistical procedures used to achieve the results.

Chapter four presents the results of the methodology and procedures described in Chapter three, as well as their interpretations. It also provides a comparison of the results to what is presented in related literature discussed in Section 2.7.

Chapter five concludes the research with a summary of the investigation and shows how the outcomes of the study link back to the original research problem. It also provides a critical assessment of the findings with regard to acknowledged limitations. It makes recommendations and consequently suggests areas of further research.

1.9 Summary

This chapter provided a brief summary of the content of this thesis. It stated the research problem, discussed the broad objectives of the research, introduced the research methodology used, explained the importance of the research, acknowledged its limitations and key assumptions, discussed the feasibility of the study and contained a brief outline of what to expect in each of the following chapters.

Chapter 2 Literature Review

2.1 Introduction

A key success factor for any organisation is competitiveness within the market. Abrahams (2003) maintains that competitiveness now extends beyond the corporate world to include educational institutions that build human capital rather than products and materials. As already mentioned, the use of IT to achieve this competitiveness is paramount. Consequently, an adequate IT infrastructure is required by educational institutions in order for them to be competitive within their industry. The adequacy, reliability and effectiveness of an IT infrastructure depends on the IT controls that are in place. To lay the foundation for this research, what follows is a definition of IT controls and the relevant frameworks that revolve around those controls, as well as a discussion of the need for IT audits based on frameworks to assess the effectiveness of those IT controls. The role and importance of IT in higher education is then presented, and because of this importance, the need for audit and control of the IT infrastructure is discussed. Finally, a discussion on the differences between IT in the corporate world and that in higher education, and to what end the corporate frameworks on which audits are based are relevant in a higher education context, is presented based on the literature.

2.2 IT Controls

The Information Systems Audit and Control Association (ISACA[2]) (n.d. (a)) defines controls in a computer information system as the "policies, procedures, practices and organisational structures designed to provide reasonable assurance that objectives will be achieved and undesired events are prevented or detected and corrected". IT controls are, in a sense, the safety net surrounding and within an organisation's IT infrastructure. Controls can be high-level, for example, establishing policies on how to deploy and manage resources to execute the business strategy (IT Governance Institute, 2007), or they could be more specific and technical, for example, data input validation in applications. Nevertheless, they provide a way

[2] www.isaca.org

to protect the organisation from the volatile nature of IT and allow the organisation to use IT in the best way possible to achieve its business goals.

The aforementioned definition of controls states that controls are preventative, detective or corrective in nature. Input validation controls, for example, are preventative in that they prevent harmful user input from being entered via an application. An example of a detective control is the use of anti-malware software. This control ensures that malware is detected on the computer system before damage is done. A disaster recovery plan is a corrective control in that it allows the organisation to undergo corrective action to recover its components to the state that they were before the incident occurred. Ensuring that adequate preventative, detective and corrective controls such as these are in place remains a challenge for any organisation. IT control frameworks have therefore been designed to guide organisations in the implementation of IT controls.

2.3 IT Control Frameworks

Organisations can adopt various IT control frameworks on which to base their IT infrastructure design and implementation. These control frameworks are also used as a base for IT auditing specification. The IT Governance Institute (2000) defines a framework as "the boundaries, a set of principles and guidelines, which provide a vision, a philosophical base and an organisational structure for construction". This allows the organisation to administer its IT controls in a structured manner, providing for a certain standard and consistency within the organisation's IT infrastructure, and ensuring that all bases are covered. If implemented properly it can lead to the organisation realising its business goals through the use of IT. Examples of these frameworks are COBIT (ISACA, n.d. (b)), ITIL (2012), BS 7799 and ISO 27001 (Disterer, 2013). What follows is a discussion of some of the more popular frameworks within the industry.

2.3.1 COBIT

The purpose of the COBIT framework (standing for Control Objectives for Information and related Technology), as defined by ISACA, is to "provide management and business owners with an IT governance model that helps in delivering value from IT and understanding and

managing risks associated with IT" (ISACA, n.d. (b)). COBIT is made up of control objectives based on IT governance best practices and is one of the most widely-used frameworks. It facilitates the definition of an organisation's most vulnerable assets and defines a level of control over these assets to mitigate losses in the event of a security incident (Council, 2006). The COBIT mission is to "research, develop, publicise and promote an authoritative, up-to-date, international set of generally accepted information technology control objectives for day-to-day use by business managers and auditors" (IT Governance Institute, 2000, p. 1). COBIT is intended for use not only for business and IT management, but for IT audit and assurance professionals as well, as it bridges the gap between technical controls and business risks (ISACA, 2010). Much of the literature presented later in this chapter bears reference to the COBIT framework (Council, 2006; Viljoen, 2005; Sayana, 2002), so what follows is a fairly detailed discussion of COBIT's core principles.

As presented in the COBIT 4.1 release by the IT Governance Institute (2007), the COBIT framework contributes to the success of IT in delivering against business requirements by encompassing four concepts. These four concepts are a) creating a link to the business requirements, b) organising IT activities into a generally accepted process model, c) identifying the IT resources to be leveraged, and d) defining the management control objectives to be considered. The process model "subdivides IT into four domains and 34 processes in line with the responsibility areas of plan, build, run and monitor, providing an end-to-end view of IT" (IT Governance Institute, 2007, p. 5). These domains are listed below and discussed thereafter.

The four domains of COBIT 4.1 are:

- Plan and Organise
- Acquire and Implement
- Deliver and Support
- Monitor and Evaluate

The Plan and Organise domain involves strategic thinking around alignment of IT to business goals. COBIT documents ten processes that an organisation can put in place to achieve success in this domain. These processes include definition of a strategic IT plan, and management of IT human resources, for example. COBIT expands on each of the processes

to guide the implementation of the framework within each domain. The Acquire and Implement domain involves realising the strategy identified in the Plan and Organise domain, and includes the design of IT controls and services to ensure its success. This domain is divided into seven processes; for example, identify automated solutions to realise functional business requirements, and manage changes to applications such as implementing version control procedures. The Deliver and Support domain is concerned with delivery of those IT services and maintenance of the IT controls put in place to ensure continued realisation of the business strategy; for example, determining whether adequate confidentiality, integrity and availability controls are in place for information security, or managing the physical environment, are two of the thirteen processes in this domain. The Monitor and Evaluate domain involves the regular assessment of all IT processes for quality, and compliance with control requirements. These processes typically involve auditing and IT governance. Although COBIT provides for 34 processes across these four domains, it in no way requires that each and every one be implemented as the COBIT framework is merely a guide for good practices to best achieve success through the use of IT. (IT Governance Institute, 2007)

It must be mentioned that not only is COBIT process-driven, but it also provides tools for measuring the status of an organisation's IT by way of maturity models. Using these models, an organisation can assess the maturity of its IT and better manage the resources and costs involved. Maturity models also provide an ideal way of benchmarking an organisation against others in the market, which allows for movement toward and achievement of a competitive edge. (IT Governance Institute, 2007)

The researcher is aware that COBIT 5 has recently been released but information regarding this version is limited at this time. ISACA (n.d., (c)) however states that COBIT 5 incorporates the latest thinking by ISACA professionals and builds on COBIT 4.1 by "integrating other major frameworks, standards and resources, including ISACA's Val IT and Risk IT, Information Technology Infrastructure Library (ITIL) and related standards from the International Organization for Standardization (ISO)". COBIT 5 allows organisations making use of previous versions of COBIT to build on what they already have in place as the fundamental concepts of this framework have not changed. It is this constant revising of the framework between experts in the field that has lead to COBIT becoming one of the most popular, stable and reliable frameworks in use today.

2.3.2 ITIL

Another popular framework is the IT Infrastructure Library (ITIL). This was developed as "a set of comprehensive and inter-related codes of practice in achieving the efficient support and delivery of high quality, cost effective IT services" (Hewlett-Packard Development Company, 2006, p. 9). ITIL has a narrower focus than COBIT in that it largely focusses on service delivery; but, like COBIT, it was designed to capture industry best practice. The official ITIL site (2012) states that ITIL "provides a practical, no-nonsense framework for identifying, planning, delivering and supporting IT services to the business". Hewlett-Packard Development Company (2006) maintains that ITIL is scalable and platform independent, and advises organisations to adopt and adapt it, rather than applying it as-is. Adaptability is the key to any good IT framework as one size does not fit all across the range of business contexts. Because of its narrow focus, ITIL is often implemented at the core of many control frameworks, one of which is COBIT 5.

2.3.3 BS 7799 and ISO 27001

Whereas COBIT focuses[3] on IT governance and ITIL focuses[3] on IT service management, the aforementioned BS 7799 and ISO 27001 focus solely on information security (Susanto et al., 2011). In fact, ISO 27001 was adapted from BS 7799 and therefore has similar characteristics (ibid.). Both of these are referred to as security standards rather than all-encompassing frameworks and "can be used as a guideline to develop and maintain" adequate information security (Disterer, 2013).

The BS 7799 standard titled "IT – Security Techniques – Code of Practice for Information Security Management" was released in 1995 by the British Standards Institute. This standard was adopted and "harmonised" with other standards by the International Organisation for Standardisation (ISO) to produce the ISO 27001 which was released in 2005. Organisations have since certified their systems and processes against this international standard. (Disterer, 2013).

The ISO 27001 standard "aims to provide an approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving" information security (Sharma

[3] Although this includes aspects of information security as well, it is not the sole focus.

and Dash, 2012). It is based on the Plan-Do-Check-Act (PDCA) concept, which is similar to the four domains of COBIT described in Section 2.3.1. The PDCA process is a "widely accepted system to drive continual improvement" (Sharma and Dash, 2012) and starts with an attempt to define the requirements for protecting the information and the information systems. It then identifies and evaluates risks, develops suitable procedures and measures for reducing those risks, implements these, and continuously monitors operations to drive their improvement (Disterer, 2013).

Disterer (2013) describes ISO 27001 as providing "control objectives, specific controls, requirements and guidelines, with which the company can achieve adequate information security". It does this by outlining 39 control objectives across 11 domains[4]. These domains are security policy, organisation of information security, asset management, human resources security, physical and environmental security, communications and operations management, access control, information systems management, information security incident management, business continuity management, and compliance. It is up to the organisation to assess how the control objectives across these domains should be implemented in accordance with the type of business and culture of the organisation to minimise its information security risks.

A research study by Barlette and Fomin (2008) explored the suitability of information security standards to type and size of business, particularly small- and medium-sized enterprises (SME). They found that the applicability of the ISO 27001 was low in SMEs and stated that real business environment requirements for uniform standards will differ depending on the "specific organizational context and type of information being processed". Additionally, Sharma and Dash (2012) promoted the ISO 27001 as a "management standard", not a "security standard" and argued that it provides a framework for the management of security within an organization, but does not provide a "one size fits all" for information security. Disterer (2013) supports this view by saying that concrete measures for the fulfilment of requirements must not be stipulated by the standard but rather be developed and implemented on a company-specific basis.

This argument over applicability of frameworks and standards, and whether or not they can be tailored to the organisation's needs is the underlying notion of this research and is the

[4] This is the 2005 version which has since been revised but the revision is still in drafting phase.

main reason that no particular standard was used as a basis for this study. This is explained further in Section 3.4.1 regarding control selection.

2.3.4 King III

A discussion of IT control frameworks and IT governance cannot be complete without mention of King III. The King III report on governance for South Africa was developed in 1993 in response to the end of Apartheid and the need for organisations to adapt to a free economy (Stewart, 2010). It documents the principles of good corporate governance that organisations should adhere to and includes a set of principles for IT governance best practice. The Companies Act of South Africa requires that the policies and procedures presented in King III be covered in the governance of the organisation so it is in the organisation's best interest to apply King III (Institute of Directors in Southern Africa and the King Committee on Governance, 2009). However, King III allows for an "apply or explain" approach rather than the "comply or else" approach of the USA's corporate governance code, the Sarbanes-Oxley Act (Sarbanes and Oxley, 2002). (It must be noted however, that the Sarbanes-Oxley Act applies to listed corporations raising money in the USA and not HEIs).

The application of frameworks such as COBIT or ITIL can be used to satisfy the principles of King III. In addition, to ensure that an organisation is applying these frameworks correctly, an IT audit can be carried out. IT audits are an important aspect of IT governance in that they assure the IT steering committee that adequate IT controls are in place to protect the organisation's information assets and to realise its business strategy through the use of IT. What follows is a discussion of the IT audit concept.

2.4 IT Audits

An IT audit uses frameworks and other measuring means to assess the IT controls within an organisation's IT infrastructure to ensure that risks are managed and accounted for. Weber (1999) introduces several major reasons why organisations must establish a function for examining its IT controls. The first is the costs of data loss. "Data makes up a critical resource necessary for an organisation's continuing operations … data provides the organisation with an image of itself, its environment, its history, and its future. If this image

is accurate, the organisation increases its abilities to adapt and survive in a changing environment. If this image is inaccurate or lost, the organisation can incur substantial losses" (ibid.). The second reason, related to the first, is incorrect decision-making. The quality of decisions depends on the quality of data and if the data is inaccurate then so too will be the decision-making. Bad decisions based on poor data can have devastating consequences for the organisation. The third reason is the costs of computer abuse. Weber (1999) argues that "the major stimulus for development of the IT audit function within organisations often seems to be computer abuse". Computer abuse can take the form of hacking, viruses, illegal physical access, or abuse of privileges, amongst others. Another reason for establishing a function to examine IT controls is the value of hardware, software and personnel, which are critical organisational resources that can be negatively affected by the absence of adequate IT controls. There are also high costs associated with computer error as computers perform functions automatically and there are consequences if these functions are unreliable. Maintenance of privacy is another reason stated by Weber (1999) for establishing a function for ensuring adequate IT controls, as previously mentioned in Section 1.1 (with reference to the PPI Bill in South Africa). All these concerns make it important to monitor controls in the way of IT auditing (Gallegos et al., 1999). Therefore the function that must be established is the IT audit.

The IT auditor is concerned with availability, confidentiality, and integrity of the IT infrastructure, which are a major focus of the ISO 27001 (Sharma and Dash, 2012). This supports the notion that frameworks and standards should form the basis of IT audits. Sayana (2002) states that the following questions for each concern apply:

> *"Availability – Will the IT systems on which the business is heavily dependent be available for the business at all times when required? Are the systems well protected against all types of losses and disasters?*
>
> *Confidentiality – Will the information in the systems be disclosed only to those who have a need to see and use it and not to anyone else?*
>
> *Integrity – Will the information provided by the systems always be accurate, reliable and timely? What ensures that no unauthorized modification can be made to the data or the software in the systems?"*

Additional concerns for auditing are whether the system uses resources efficiently and can perform its functions effectively.

The controls that are reviewed in a full IT audit fall under the following broad classifications: physical controls, system administration, application software, network security, business continuity, and data integrity controls. A physical controls review assesses controls associated with physical security, power supply, and air conditioning, amongst others. A system administration review includes controls in operating systems, database management systems, all system administration procedures and compliance. A review of the controls in place in application software includes assessment of access control and authentication, input validation, error and exception handling, amongst others. The application software provides the front-end access to the organisation's data-related assets. This review also includes assessment of the procedures around development and implementation of new systems and the maintenance of existing systems, for example, whether version control for release of application code is used. The network security review assesses controls around the internal and external connections to the system, perimeter security, firewalls, and intrusion detection, amongst others. A review of business continuity confirms the existence of backup procedures and storage as well as a documented and tested disaster recovery plan. Data integrity reviews can be performed using generalised audit software, which investigates live data to verify adequacy of controls and impact of weaknesses of controls identified in the previous reviews. (Sayana, 2002)

Sayana (2002) argues that all the elements of an IT audit described above must be addressed and presented to management for a clear assessment of the system. For example, "application software may be well designed and implemented with all the security features, but the default super-user password in the operating system used on the server may not have been changed" (ibid.), thereby allowing someone direct access to the data files. Such a situation negates whatever security is built into the application and an audit of the application software will reveal no indication that the operating system on which it runs fails the security check (ibid.).

A discussion on IT audits is incomplete without a distinction being made between internal and external audits. Normally, the purpose of an external audit, which is carried out by an independent organisation, is to assess the systems that underlie the financials of the organisation. On the other hand, the purpose of an internal audit is broader, encompassing full assessment of the IT infrastructure, and is carried out internally within the organisation. In this study, a holistic view of the IT audit is adopted in order to focus on the betterment of information security in the IT infrastructure as a whole. Section 4.3, however, shows that

participants in this study distinguish between internal and external audits in order to support their claims.

In conclusion, we have discussed the importance of IT controls for an adequate IT infrastructure and the use of IT control frameworks to maintain a structured approach to the implementation of these IT controls. We have also proposed the use of IT audits based on the IT control frameworks to assure the organisation that the IT controls have been implemented correctly. For purposes of this research, it is now time to focus this general discussion more specifically on IT in the higher education context.

2.5 The Role of IT in Higher Education

Two core missions of an HEI are to provide outstanding education as well as research. Access to the Internet, digital libraries, email, threaded discussions and related technologies have become a necessity towards achieving this mission. Productive research has been argued to require massive processing power and very fast networks, such that "higher education now supports some of the world's largest collections of networked resources and maintains high-speed links to similar organisations around the world" (EDUCAUSE[5], 2002, p. 9). In addition, the HEI requires adequate IT for the administrative functions that support the education and research goals of the institution. (EDUCAUSE, 2002)

Glenn (2008) suggests that technology in higher education will become a core differentiator in attracting students and corporate partners. He states that the more advanced the HEI is in terms of its use of IT, the closer it moves towards its goals. For example, the concept of e-learning is gaining a firm foothold in universities around the world (Glenn, 2008). Laurillard (2006) defines e-learning to be the use of various technologies for learning or learner support. This covers a broad range of capabilities including Internet access to digital versions of materials unavailable locally; interactive customisable tutorials; personalised web environments, which allow participation in class discussion forums; and the ability to model real-world systems and create an environment in which students can explore, experiment and learn. Many of these capabilities are often consolidated into a learning management system,

[5] EDUCAUSE is a non-profit organisation whose focus is to advance higher education through the use of technology. See http://www.educause.edu/.

which provides a framework upon which to plan, deliver and manage online content for students. Laurillard (2006, p. 10) states that "e-learning has been used very effectively in university teaching for enhancing the traditional forms of teaching and administration". This is important in that, if administered properly, it can have a significant impact on how learners learn, how quickly they master the skill, how easy it is to study and the overall enjoyment of the learning process (Laurillard, 2006).

Included in the concept of e-learning is virtual classrooms. The definition and value achieved from the virtual classroom is illustrated by the following study. Schutte (2002) carried out an experiment on a class of 33 students, half of which were taught using the traditional method and the other half using the virtual classroom. While the traditional class underwent traditional lectures and submitted assignments in class, the virtual class underwent email collaboration, submission of assignments via email, online discussion forums, and completed homework via forms online. It was found that the virtual class scored an average of 20% higher on examinations than the traditional class and the virtual method was perceived to be more flexible and understandable with more peer contact and more time spent on work. This research shows that the use of technology in teaching is beneficial.

It is evident that the main advantage of e-learning is that it provides flexibility and customisation in the learning process. This leads to a more student-centred approach to learning in that learning can be customised to the individual as opposed to the traditional way of reducing the student to a stereotype in the form of a lecturer giving a one dimensional lecture to a classroom of students. E-learning allows for the emphasis to be removed from the teacher and to be focussed more on the student as the student is not required so much to listen anymore but to "do" (Wilson, 2001). This can enhance the learning experience. Having said that, Wilson (2001) argues that technology by itself neither guarantees nor inhibits quality. It is the design and delivery of the educational experience that is the critical factor. The ability to reliably provide this new medium of learning will increase the HEI's competitive advantage in the market.

In terms of the second core mission of HEIs, Wilson (2001, p. 9) states that "technology can break down the barriers of distance and allow cross-cultural collaboration in spite of geographic isolation", which allows for more efficient and effective research collaboration in the form of globalisation of knowledge. All in all, technology allows institutions to share

courses, research experiences, and cross cultural experiences without regard to geography (Wilson, 2001).

In conclusion, IT is indeed important in higher education, but as mentioned previously, along with advancements in technology come new challenges. E-learning requires long session lengths, high levels of file sharing, and the need for rapid response-times with large numbers of widely-distributed users (Viljoen, 2005). These challenges, coupled with the fact that any interruption in the service can result in complete shutdown of the virtual university, highlight the need for good controls (ibid.). HEIs competing in the education industry of our times therefore also need to enforce controls to protect their information assets and provide a function for assessing those controls.

2.6 The HEI – a unique entity

Having said that HEIs must also provide the means to protect and audit their IT infrastructure, an HEI has complexities that set it apart from the corporate world. Academic freedom has a long history in higher education as a set of rights and responsibilities that enables enquiry, debate and the pursuit of knowledge in new directions (EDUCAUSE, 2002). This academic freedom leads to diversity in thinking and rejection of formal structures in favour of flexibility. This concept makes implementing rigid IT controls difficult within the dynamics of the HEI and a balance between academic freedom and security must be maintained (ibid.). The management style in an HEI is decentralised and any one decision must be passed through a number of channels before implementation. Price and Officer (2005) argue that this leads to a lack of accountability of individuals within the institution and thoughts about information security are lax. It has always been insisted on that a "university is not a business" (Naudé, 2011) and that HEIs are mission-driven as opposed to profit-driven (Price and Officer, 2005). This has a major impact on how a university sees the need for securing its technology. Budgets are tight, and many of the benefits of increased security are often perceived to have little return on investment for the institution itself (EDUCAUSE, 2002).

HEIs are set apart from the corporate world not only in the soft managerial issues discussed above but also with regard to technical issues. A single campus network may host an array of dissimilar systems from a supercomputer cluster involved in international research to student-owned laptops (EDUCAUSE, 2002). Student computers are generally connected directly to the same network infrastructure as administrative, research and instructional systems and they can easily represent the largest number of computers making use of campus resources, but at the same time they are the most difficult to standardise and control (EDUCAUSE, 2002). HEIs are subject to the same security flaws that affect companies the world over, but owing to the diversity of computers and users, these flaws often impact the institution disproportionately (EDUCAUSE, 2002). Other technical issues that an HEI must deal with are: workstations dedicated to more than one user (Viljoen, 2005), students having specialised IT skills and mischievous "script kiddie" tendencies to undermine the security of campus IT systems, and a continuous inflow of technically-unsophisticated students with enquiring minds who like to fiddle.

2.7 Relevance of IT Frameworks and IT Audits in Higher Education

The frameworks for IT control discussed earlier form the basis for IT audits. There has been some research on the relevance of frameworks and their control criteria in higher education (Council, 2006; Viljoen, 2005; Sayana, 2002). There has also been research on the top IT controls in areas other than the corporate world (Busta, Portz, Strong and Lewis, 2006). What follows is a presentation of this literature and its claims. There has not been as much research with regard to the relevance of control criteria for IT audits in higher education as there has been in determining relevance of implementation of IT governance frameworks in higher education. However, as audit control criteria are based on the controls and standards specified in the frameworks, both areas of research are considered relevant to determine what control criteria are most significant to audit, a claim supported by Maria and Haryani (2011).

The purpose of a case study involving an "academic information system" at Satya Wacana Christian University in Indonesia by Maria and Haryani (2011) was to develop an audit model to measure the performance of an academic IT system. Based on COBIT, the developed model provided a basic framework that could be used to audit an academic IT

system. Maria and Haryani (2011) argue that higher education in Indonesia lacks specific models for IT implementation and audit. Since the focus of the study was limited to system performance in delivery and support, only that aspect of the COBIT framework was used to establish the audit model. The authors identified four critical success factors with regard to achieving adequate service delivery and support from their IT system and attempted to align them to the COBIT controls in order to develop a model of the most significant controls to audit to ensure that the system achieves its function (in this case delivery and support). The COBIT controls identified to be directly aligned with the critical success factors were: ensure continuous service, manage performance and capacity, ensure systems security, educate and train users, amongst a few others. COBIT defines "ensure continuous service" as making sure that IT services are available as required to ensure minimum business impact in the event of a major disruption (IT Governance Institute, 2000). This is enabled by "having an operational and tested IT continuity plan which is in line with the overall business continuity plan and its related business requirements" (IT Governance Institute, 2000, p. 138). This is indeed necessary in higher education where the various stakeholders of the institution require IT systems to be available at any time of the day. This control objective, along with the others that were identified, were found to be directly aligned to adequate delivery and support of IT systems in the academic information system at Satya Wacana. A COBIT control that was not identified as relevant was "identify and allocate costs". COBIT defines this control objective as "correct awareness of the costs attributable to IT services and is enabled by a cost accounting system which ensures that costs are recorded, calculated and allocated to the required level of detail and to the appropriate service offering". This objective seems to be more suited to the corporate world, which is more profit-driven than mission-driven higher education, as mentioned earlier. This research highlights the fact that different controls are relevant to different sectors of the economy.

On a national front, a study on IT governance in higher education was carried out by a Masters student at Nelson Mandela Metropolitan University in Port Elizabeth, South Africa (Viljoen, 2005). The primary objective was to propose suitable IT governance frameworks (for example COBIT) for use by HEIs in South Africa. In the study, the need for IT governance in higher education was determined, followed by the identification of criteria for the selection of suitable IT governance frameworks for use in higher education in South Africa. As a result, several widely-used frameworks were identified, although these frameworks "generally do not make a distinction between corporations and not-for-profit

organisations[6]" (Viljoen, 2005, p. 134). The author argued that some adaptations would be appropriate. The study found that several of the frameworks identified could make a significant contribution towards improving the level of IT governance in HEIs, but a clear conclusion was that "COBIT addresses all the most important requirements for a high level IT governance framework, and that it is suitable for implementation in a higher education IT governance environment" (Viljoen, 2005, p. 158).

A study conducted in Louisiana USA investigated the difficulty of implementing COBIT in an IT governance programme at South Louisiana Community College (SLCC) (Council, 2006). The implementation was limited to COBIT's delivery and support process which focuses on ensuring network security. Through the implementation of COBIT in a higher education environment, it was found that COBIT generally matched the environment at SLCC, with a few exceptions. It was argued, however, that no single IT organisational structure or governance programme is applicable to all organisations, because the organisation must respond to its own unique environment (Council, 2006). Some changes were necessary to make the tool more applicable to SLCC. For example, the DS5-8 control objective of COBIT states "gain the ability to detect, record, analyse significance, report, and act upon security incidents when they do occur, while minimising the probability of occurrence by applying intrusion testing and active monitoring" (Council, 2006, p. 13). This objective was found not to be applicable at SLCC because the cost in terms of man-hours and equipment expense outweighed the perceived risks. This is applicable to higher education institutions in general who typically have tight budgets and small IT teams. The study concluded by stating that "SLCC has demonstrated that medium-sized institutions of higher learning can benefit from the implementation of an IT governance security programme" (Council, 2006, p. 189). The IT governance programme assisted in improving the performance of the IT infrastructure relative to the goals of the institution and formed a base on which its IT could be audited, with a few minor changes for its application in a higher education context.

Another study was carried out by Busta et al. (2006) on the top IT controls for small businesses. Small businesses, like HEIs, were identified as being different to corporate organisations. Busta et al. (2006) argued that every business has a large number of IT risks to

[6] Not-for-profit organisations include most HEIs.

control but prioritising which risks to control is probably more acute for small businesses because of their limited resources and small IT staff. The study used the Delphi technique (discussed in Section 3.3) to survey IT experts from around the world to determine the top IT controls in a small business. The experts were asked to rank the top ten IT controls from an initial list of thirty based on COBIT. After three Delphi rounds, eleven key controls for small businesses were revealed. The three most important controls were: updated firewalls and secure wireless connections, up-to-date virus and spyware protection, and regular and tested back-up procedures. Other important controls that made it to the top eleven list include file access privilege controls, IT as part of a long- and short-range plan, an IT continuity and recovery plan, identification and authentication procedures, employee IT security training programme, and data input controls. An interesting finding of the study was that experts in small businesses rated software scaling (ensuring that software is capable of meeting future needs for increased data processing and so on) as a top control whereas those who did not were from medium to large enterprises. This highlights the fact that relevance of IT controls depends on the characteristics of the entity that enforces them. The study concluded by stating that executing these controls in a small business can greatly improve the security, reliability, strategic use and accuracy of its IT resources.

2.8 Summary

From the research studies discussed above, it is evident that the implementation of IT controls at HEIs is important. Many studies have focussed on IT governance frameworks to guide the implementation of IT controls and/or provide a means for assessing the IT function by way of an IT audit. Most studies have found that the controls specified in COBIT are suitable for a higher education context but require some adaptation. The literature, therefore, provides a solid foundation for the purpose of this research.

Chapter 3 Research Methodology

3.1 Introduction

Sound research is always based on a sound research methodology, which includes defining the research goals, adopting or adapting an appropriate research method, stating how this is a good measure for the research, and defining the limitations of the study. Consequently, this chapter first reflects on the aims of this research that were presented in Section 1.3. A theoretical discussion of the research technique to be used will then ensue, followed by the specific research steps, which are also presented visually. The challenges of the study are discussed, along with how the research study addresses issues of validity and reliability to ensure a sound research study.

3.2 Research Aim

As stated in Section 1.3, the primary aim of this research is to develop a set of IT control criteria that are relevant to an IT audit in a South African HEI. Sub-objectives in realising this aim are assessing whether it is fitting to use generic IT control criteria to audit an HEI, whether there are differences between corporate organisations and HEIs in terms of IT, and to develop a set of IT control criteria, including the associated ranking of these criteria, that are relevant to an IT audit in an HEI.

3.3 Research Methodology Overview

The method used in this research is called the Delphi technique. What follows is a discussion of the characteristics of the Delphi technique along with an explanation as to why it was appropriate for this research. An outline of the research steps for using the Delphi technique in this research follows thereafter.

Broadly, the Delphi technique is defined by Cuhls (2003) in a quote from Hader and Hader as a "relatively strongly structured group communication process, in which matters, on which naturally unsure and incomplete knowledge is available, are judged upon by experts". Building on that, Amos and Pearse (2008, p. 95) quote Gibson and Miller saying "the method brings a broad range of perspectives and ideas to bear on problem solving from a comprehensive panel of experts responding to feedback". Amos and Pearse (2008) present the Delphi technique with five main characteristics, namely, a focus on researching the future or where there is incomplete knowledge, the use of expert opinion, reliance on remote group processes, an iterative research process, and creating a consensus of opinion. These characteristics make the Delphi technique well-suited to this research as discussed in greater detail below.

Although there has been a fair amount of research with regard to audit controls, and bodies such as ISACA are dedicated to furthering research around IT auditing, not much research has been done with regard to IT auditing in HEIs. The Delphi technique therefore is ideal for this research because, as stated by Amos and Pearse (2008, p. 96), the Delphi is useful when there is a "lack of agreement or incomplete state of knowledge concerning either the nature of the problem or the components which must be included in a successful solution". Currently HEIs are audited according to corporate IT auditing standards and control criteria (Viljoen, 2005). The aim of this research is to challenge whether this is appropriate by creating a separate model of audit control criteria for higher education IT auditing. Being a futures technique, Delphi is aligned with the aims of this research in that it focuses on expert opinion of future requirements as opposed to current practice (Amos and Pearse, 2008).

The Delphi technique makes use of a panel of experts who are presented with a data capturing instrument and are required to participate based on their knowledge, insight and experience. Hsu and Sandford (2007, p. 3) state that "individuals are considered eligible to be invited to participate in a Delphi study if they have somewhat related backgrounds and experiences concerning the target issue, are capable of contributing helpful inputs, and are willing to revise their initial or previous judgments for the purpose of reaching or attaining consensus". The question of who is or is not an expert is a controversial one and will be discussed in more detail in Section 3.5. The use of expert opinion as the data source for this research is well-suited in that knowledge in this area is incomplete and collating expert opinion on the matter will allow for depth and solid creation of knowledge. Additionally, by

including researchers such as members of ISACA as part of the expert panel, this research can also trigger further research around IT auditing in higher education amongst the ISACA community once they realise that the area requires more attention.

A further characteristic of the Delphi technique is reliance on remote group processes. Snyder-Halpern, Thompson and Schaffer (2000, p. 809) state that "the Delphi technique provides a means of assessing the judgements of a group of experts without the necessity of having these experts meet together". Okoli and Pawlowski (2004) argue that a key advantage of controlled and remote opinion feedback is that it avoids direct confrontation with the experts. This is important to allow for independent thought and "gradual formulation of considered opinion" as opposed to "hasty formulation of preconceived notions". Remote processes also allow for anonymity and confidentiality which minimises social challenges such as coercion or reluctance to participate (Hsu and Sandford, 2007). Reliance on a remote research process is suited to the proposed research in that experts will be spread around the country at various audit houses and HEIs so it is more viable to adopt a research design that allows for remote communication, which would be via email and online surveys.

The Delphi technique is also characterised by an iterative process that should culminate in consensus. The researcher performs the role of moderator and surveys the experts in a number of rounds, providing feedback of voiced opinion allowing experts to gather new information as the rounds progress (Cuhls, 2003). The same experts are able to assess the same matters iteratively, but influenced by the opinions of the other experts. The objective is for the group to reach consensus (Amos and Pearse, 2008). These two characteristics of iteration and consensus fit in with the aim of this research to develop a reliable and considered set of criteria. The model of IT audit criteria specific to HEIs would stem from an iterative and collaborative process in which consensus has been reached.

3.4 Research Steps

Following from the nature of the Delphi technique, the method undertaken in this research to reach the final result is obtained by analysing the results of each round. It is therefore imperative to include the results of initial rounds in a write-up of the methodology as these

play a significant role in deciding the way forward with regard to the method. Therefore the methodology outlined in this chapter includes the results from initial rounds leading up to the final results. However, the final results are excluded from this chapter and dealt with in Chapter 4.

The research steps were divided into three phases: Preparation, Data Capture and Data Analysis. What follows is an in-depth discussion of these phases. A visual representation of the research steps undertaken in this study is outlined in Figure 3.1.

Firstly, in the Preparation phase, IT and auditor experts within South Africa were identified. According to Hsu and Sandford (2007, p. 3), choosing appropriate subjects is "the most important step in the entire process because it directly relates to the quality of the results generated". The pool of experts consisted of two groups of professionals, namely, (a) IT officials at South African HEIs who are directly involved in administering the institution's IT as well as participate in the IT audit process, and (b) auditor professionals from various audit houses in the country, who audit the IT of South African HEIs as well as corporate organisations. It was originally intended to have a third category of research participants: IT professionals from corporate organisations around the country. This was envisaged so as to obtain a good mix of opinion based on the auditing of controls in HEIs as opposed to corporate organisations. In practice, however, the third category was omitted as IT professionals in corporate organisations did not believe they could contribute effectively to the research project as they have no dealings with HEIs and would not be able to legitimately compare the two contexts. They also had no interest in participating in research that was aimed at HEIs and would not be beneficial to their work. Naturally, this leads to the question: how can the category of IT professionals in HEIs compare the two contexts? IT audits in South African HEIs are based on corporate IT audits so it is believed that IT professionals in HEIs have an adequate understanding of controls needed in corporate organisations.

The participant group in this research was therefore restricted to the two aforementioned categories: IT professionals in South African HEIs who are directly involved in administering the institutions' IT as well as participate in the IT audit process, be it internal or external audits, and audit professionals from various audit firms around the country. Note that the IT auditor category is made up of those who audit HEIs as well as corporate organisations, so

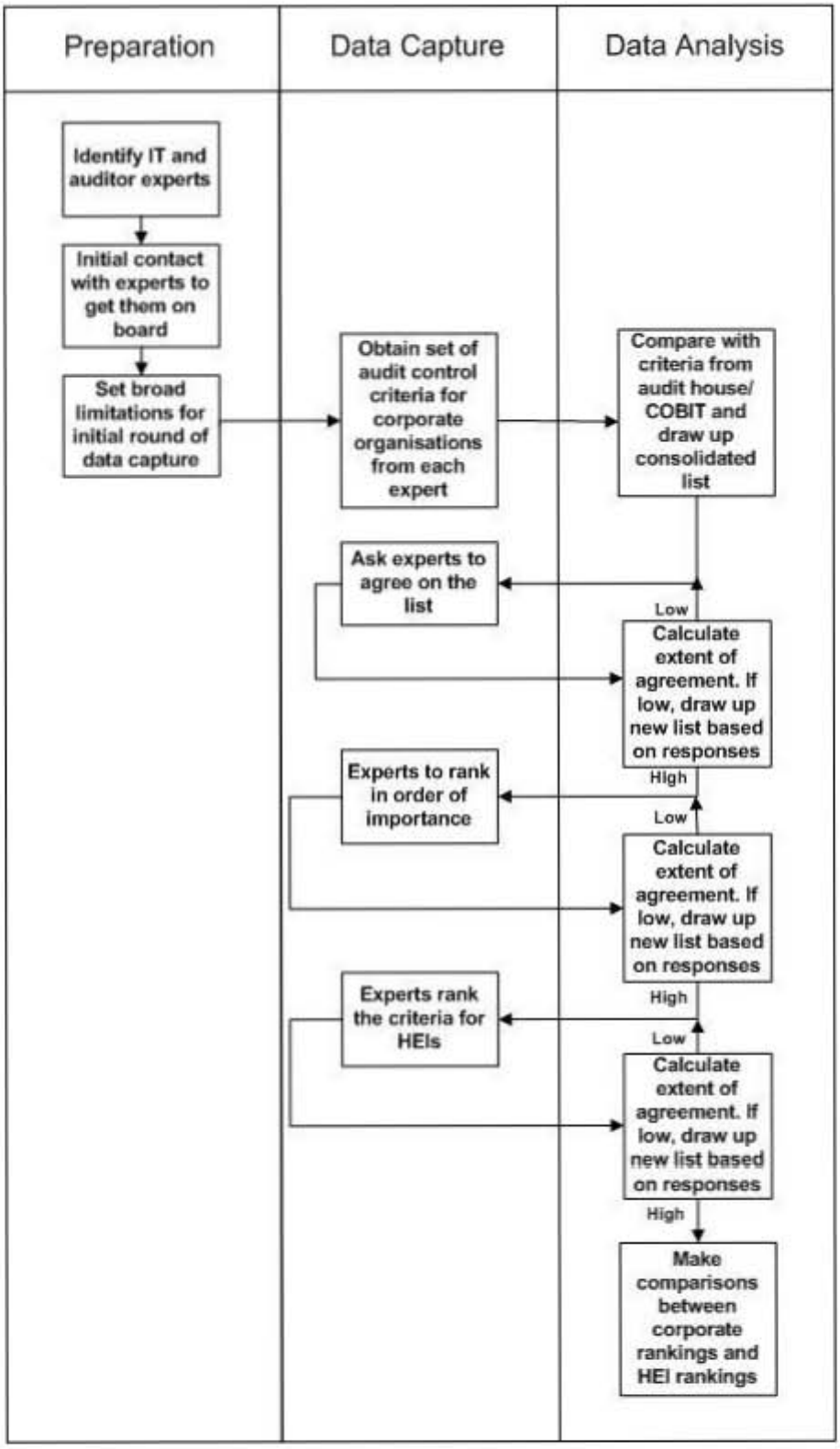


Figure 3.1: Research steps

this allows for solid comparison between the two contexts which could potentially have been lost by omitting the third category.

The second step in the Preparation phase was to make contact with the two categories of professionals, and outline the aim of the research as well as the structure, in order to get them on board. Issues of encouraging participation and high attrition rates remain a challenge of the Delphi technique and are discussed in greater detail in Section 3.5. Participants were obtained through various channels. An email was sent out to the ASAUDIT[7] mailing list which included IT directors from HEIs in South Africa, see Appendix A for a copy of the email. Participants were also obtained via connections of the researcher's colleagues to various IT professionals and auditors. These professionals were contacted directly by the researcher and/or her colleagues to ask for their participation. Following from the various modes of contact made, twelve professionals agreed to participate in the research. The group consisted of four auditors from various audit houses, and eight IT professionals from HEIs around the country. The size of the group was considered appropriate in that it was small enough to be manageable, but also large enough, in terms of using the Delphi technique, to ensure validity.

Another challenge of the Delphi technique is deciding on the definition of an expert who would be able to contribute meaningfully towards the research study. The job title and level of each participant was used as the decider in this case. All participants held high level positions ranging from senior managers at auditing firms to IT directors at HEIs. All twelve participants were therefore accepted as experts in their field.

The third step of the Preparation phase was to set broad limitations for the initial Data Capture phase so as to avoid responses that were too open-ended. The study was based on and limited to various framework control criteria but the participants were not told this initially so as to encourage freedom of thought.

The iterative nature of the Delphi technique lent itself to a back and forth scenario between the next two phases, namely, the Data Capture and Data Analysis phases. Data collected in

[7] ASAUDIT is an acronym for the Association of South African University Directors of Information Technology. Its purpose is to "promote and advance the use and support of computing and information technology at South African universities, and to further develop relationships with key members in the Higher Education sector both locally and internationally" (ASAUDIT, 2012).

the Data Capture phase was analysed during the Data Analysis phase, which provided feedback and was used as a base on which to progress in the following Data Capture phase; these iterations are referred to as "rounds" in the literature. The research study consisted of a number of these rounds of data collection, where participants were approached and their opinions sought on matters involving the research question. The communication medium was email and where appropriate, online surveys were used. These surveys allowed participants to click on a link in an invitation email that directed them to a site where they could complete the survey. Links sent to participants were unique and each response was recorded against the participant's name for administrative purposes. The participants were not made aware of whom their fellow participants were and all opinions were treated anonymously. This was done for a number of reasons. Firstly, it allowed them to be completely honest without concern over what others thought of their opinion. Secondly, particularly in the case of audit firms, there are strict rules regarding confidentiality and whether opinions would be seen as originating from the firm or from the individual. The researcher was in fact approached regarding this matter and the participant concerned was assured that all responses were completely anonymous and no employers would be exposed.

3.4.1 Round One

The first round of the Data Capture phase was to obtain a set of IT audit control criteria from each expert; in other words, a set of controls that the participants thought are relevant to auditing IT at any organisation. The aim of this step was to obtain pure opinion based on experience without priming the experts with what was expected beforehand, much like a brainstorming exercise. The participants were contacted directly by the researcher via email, see Appendix B for a copy of the email, and were told to expect an invitation email with a link to a survey for round one of the research study. Being professionals in the information security field, this provided reassurance that the link would be legitimate, and they were asked to contact the researcher should they doubt the integrity of the link. This seemed to have helped the process as all twelve participants completed the survey online within the timeframe given. See Appendix C for a copy of the survey for round one. The survey was aimed at obtaining information about the participants and their involvement in higher education IT audits, as well as their opinions on the IT controls that form the basis of IT audits in any environment. These opinions were used quantitatively by the researcher in the Data Analysis phase to draw up a list of top IT controls to be tested in any environment.

The survey then moved onto more qualitative questioning in that participants were asked whether they felt that any audit controls tested are irrelevant in the higher education context, and, following from this, whether HEIs face any different information security risks than corporate organisations. They were asked whether they believed that HEI IT audits should take this uniqueness into account when performing an audit, and would they go so far as to say that different IT controls should be measured at an HEI, in addition or in place of the IT controls that they had mentioned previously. They were also asked about the maturity level of IT governance in HEIs. Results of these qualitative questions are discussed in Chapter 4.

Whilst obtaining the responses for round one, the researcher was granted access to a list of IT controls tested by an audit house specifically for a particular South African HEI. This assisted in understanding the general controls officially tested for an HEI.

Once the preliminary set of control criteria had been obtained from the experts in the first round, the results were compared in the Data Analysis phase, with what was actually used by the audit houses to audit IT in general, as well as with the fundamentals of COBIT and other frameworks discussed in Section 2.3. It was decided not to base control selection on any particular framework, for example the 11 domains of ISO 27001, but rather to use a "green-fields" approach and rely on the expertise of the participants. This was so as not to bias the control selection as the applicability of standards such as ISO 27001 to HEIs could be questionable (see Section 2.3.3). From the responses in round one, a list of the top fifteen IT controls was drawn up in no particular order, see Table 3.1. Each control made it onto the list by its popularity amongst participants, within reason and in comparison with accepted standards. The list comprised general IT controls that should be audited in any environment, not particularly in a higher education context.

3.4.2 Round Two

The consolidated list based on the experts' sets of criteria, the audit house criteria, and various aforementioned frameworks, was then presented back to the expert panel via email for round two of the Data Capture phase. See Appendix D for a copy of the email. The experts were asked if they agreed with the list. If not, the list in Table 3.1 would be modified based on the responses of the participants in round two, and a further round of Data Capture

Table 3.1: Output from round 1 – preliminary list of top 15 IT controls in any environment (not ordered)

Sound access control practices in granting, reviewing, amending and revoking user access rights
Segregation of duties, i.e. one person not responsible for initiating, actioning, approving, and reviewing
Policies governing security
Change control, i.e. control over the authorisation, testing and approval of application programme changes
Back-ups performed regularly
Firewalls implemented and maintained
Secure configuration of hardware and software
Qualified security-aware staff
Effective password controls and password ageing
Anti-virus software
Audit logging and review of logs
Disaster recovery planning, and regular updating and testing thereof
Data input validation in application programmes
Physical security
Restriction of administrator and privileged access rights, i.e. based on principle of least privilege

would ensue to gain agreement on the new list. If the experts did agree with the list, i.e. consensus had been reached, the experts would be asked to rank the list in order of importance. It was decided beforehand that 75% agreement would allow progression to the next level. This figure would be calculated simply by dividing the number of participants in agreement by the total number of participants.

In the Data Analysis phase of round two, it was found that only half the participants agreed with the list. This required that the list be revised based on the responses in round two and another iteration undertaken to agree on the revised list.

3.4.3 Round Three

The research progressed to a round three Data Capture phase with the slightly modified unordered list revised in the Data Analysis phase of round two in order to obtain agreement on that list. See Appendix E for a copy of the email for round three. The responses were analysed in the Data Analysis phase of round three and the required level of agreement for round three was obtained. The consolidated list of controls presented to participants in round three, see Table 3.2, was therefore taken through to round four, which involved ranking the list.

3.4.4 Round Four

The Data Capture phase of round four consisted of an online survey (see Appendix F), which allowed the participants to rank the agreed-upon list shown in Table 3.2. The rankings would then be statistically compared against each other in the Data Analysis phase in order to assess whether participants had reached consensus of opinion over the rankings. Also, the responses to specific questions in round one were built upon in round four to gain more information on opinions of difference of IT and IT governance in higher education as opposed to corporate organisations. These qualitative responses are discussed in Chapter 4.

As mentioned, the Data Analysis phase of round four involved calculating a statistical level of agreement on the ranked list obtained from the Data Capture phase of round four using Kendall's coefficient of concordance. This followed a similar study conducted by Pare, Sicotte, Joana and Girouard (2007) where experts ranked a list in order of priority and the

Table 3.2: Output from round 3 – top 18 IT controls in any environment (not ordered)

Sound access control practices in granting, reviewing, amending and revoking user access rights
Segregation of duties, i.e. one person not responsible for initiating, actioning, approving, and reviewing
Policies governing security, acceptable use and confidentiality
Change management, i.e. control over the authorisation, testing and approval of system changes
Back-ups performed regularly
Secure configuration of hardware and software, e.g. firewalls implemented and maintained
Qualified and experienced security-aware staff
Sound password policies and controls, including password ageing
Anti-malware software
Audit logging and review of logs
Business continuity planning, i.e. cooperative collection of disaster recovery plans, and regular updating and testing thereof
Data input validation in application programmes
Physical security
Restriction of administrator and privileged access rights, i.e. based on principle of least privilege
IT steering committee, i.e. IT alignment to strategic goals
A complete inventory of authorised assets maintained
Wireless device control
Penetration testing

degree of consensus amongst the panellists was measured using the Kendall rank correlation coefficient. “The rounds of ranking stopped when the correlation coefficient indicated a strong consensus” (Pare et al., 2007). This study followed a similar procedure to measure attainment of consensus on ranked lists. If the Data Analysis phase of round four found that a statistical level of agreement was not obtained in its Data Capture phase, then participants would be asked to agree on a new ranked list generated by the average rankings of the responses in round four. If statistical agreement was obtained, then the study would progress to the final level, which involved obtaining a ranked list of controls in a higher education context.

There are various statistical measures to assess the degree of similarity between ranked lists. Spearman’s rank correlation coefficient, Kendall’s rank correlation coefficient and Pearson’s correlation coefficient all evaluate the similarity between two ranked lists (Mazurek, 2011). Kendall’s coefficient of concordance however measures the degree of similarity amongst more than two ranked lists, which is necessary for the purposes of this study as there are twelve ranked lists to compare (i.e. twelve participants). Mazurek (2011) states that Kendall’s coefficient of concordance, hereafter referred to as Kendall’s W, ranges from 0 (no agreement among rankings) to 1 (complete agreement). It is defined by Equation (1), where X_i is the sum of the ranks for object i (in the case of this study, object i is a control criterion), k is the number of rankings (i.e. the number of participants), and n is the number of objects (i.e. the number of control criteria being ranked). A more comprehensive account of its use with real values is presented when evaluating its value for round four.

$$W = \frac{\sum_{i=1}^{n} X_i^2 - \frac{\left(\sum_{i=1}^{n} X_i\right)^2}{n}}{\frac{1}{12} \cdot k^2 \cdot \left(n^3 - n\right)}, \qquad (1)$$

Once Kendall’s W has been calculated, statistical significance of this value must be determined by testing the null hypothesis H_0, that is, the computed Kendall’s W does not evidence agreement among rankings ($W = 0$), against the alternative hypothesis H_A, that is, the computed Kendall’s W evidences agreement among rankings ($W = 1$) (Mazurek, 2011). There are various ways to test statistical significance of Kendall’s W. Mazurek (2011) uses

the Chi-squared (X^2) test with $n - 1$ degrees of freedom. Legendre (2010) however, states that the X^2 test is only valid when $k \leq 20$ and $n \leq 7$. In this study, the number of rankings k is 12 (i.e. number of participants), and the number of objects n is 18 (i.e. the number of control criterion being ranked), so the X^2 test is deemed inappropriate for use. Legendre (2010) presents the F statistic to be used in evaluating statistical significance of Kendall's W. The F statistic is defined in Equation (2) with $v_1 = n - 1 - (2 / k)$ and $v_2 = v_1 (k - 1)$ degrees of freedom.

$$F = (k - 1) W / (1 - W) \qquad (2)$$

Using a specific p-value, e.g. 0.05, the critical value for the F statistic is obtained from the F distribution table. If the observed value of F is greater than the critical value, the null hypothesis must be rejected and it should be stated that there is statistically significant agreement among rankings.

For the purposes of this study, it was decided upfront that the value for Kendall's W must exceed 0.5 in order to progress to the next level. Kendall's W for round four was calculated to be 0.460, see Appendix G. Being below 0.5, there was insufficient agreement on the rankings of respondents in round four. Consequently, another iteration was required to obtain higher agreement. The average ranked list, given in Table 3.3, was constructed from the responses in this round. This list was then presented back to participants in round five for further agreement.

3.4.5 Round Five

The Data Capture phase of round five asked participants to rank the new list using a further online survey, see Appendix H for a copy of the email explaining this and Appendix I for a copy of the survey. If the Data Analysis phase of round five found that a statistically significant level of agreement was not obtained in its Data Capture phase, then participants would be asked to agree on a new ranked list generated by the average rankings of the responses in round five. If statistical agreement was obtained, then the study would progress to the final level, which involved obtaining a ranked list of controls in a higher education context.

Table 3.3: Output from round 4 – preliminary ranked list of top IT controls in any environment

1	Policies governing security, acceptable use and confidentiality
2	Segregation of duties, i.e. one person not responsible for initiating, actioning, approving, and reviewing
3	Sound access control practices in granting, reviewing, amending and revoking user access rights
4	Sound password policies and controls, including password ageing
5	Change management, i.e. control over the authorisation, testing and approval of system changes
6	IT steering committee, i.e. IT alignment to strategic goals
7	Restriction of administrator and privileged access rights, i.e. based on principle of least privilege
8	Secure configuration of hardware and software, e.g. firewalls implemented and maintained
9	Qualified and experienced security-aware staff
10	Business continuity planning, i.e. cooperative collection of disaster recovery plans, and regular updating and testing thereof
11	Audit logging and review of logs
12	Physical security
13	Data input validation in application programmes
14	Back-ups performed regularly
15	Anti-malware software
16	Penetration testing
17	A complete inventory of authorised assets maintained
18	Wireless device control

In the Data Analysis phase of round five, Kendall's W was computed as 0.737, see Appendix J. The F statistic was calculated to be 30.77 and the critical value for F(17, 185) with a 0.05 p-value is 1.68. Thus, the F statistic was greater than the critical value. So based on the F statistic, the null hypothesis that stated there was no significant agreement among the rankings was rejected. Therefore, statistically significant agreement on the ranked list given in Table 3.3 had been obtained. This agreement meant that we now had consensus on a complete ranked list of top IT controls to be tested in any environment.

To provide for further confirmation that consensus had been reached at round five, the Cronbach alpha coefficient was also determined. The Cronbach alpha is a measure of internal consistency, which describes "the extent to which all the items in a test measure the same concept or construct and hence it is connected to the inter-relatedness of the items within the test" (Tavakol and Dennick, 2011). In other words, if the value for Cronbach increased between rounds four and five, and the value is within an acceptable level, then consensus had been reached at round five. Values for Cronbach's alpha can range between 0 and 1, where 1 shows the highest internal consistency. Tavakol and Dennick (2011) state that acceptable values of Cronbach's alpha range between 0.7 and 0.95. The Cronbach alpha coefficient was thus calculated for the ranked control lists of rounds four and five using the statistical programming language R[8]. A value of 0.88 was obtained for round four and a value of 0.97 was obtained for round five. This shows a definite improvement in consensus and is within the acceptable range of values. The calculation of Cronbach's alpha coefficient thus confirms that the results of Kendall's W are reliable, and progression could be made to round six.

The output obtained for round five, i.e. the ranked control list for corporate organisations, is presented in Chapter 4. What remained for this research methodology was to obtain a ranked list of top IT controls in a higher education context.

3.4.6 Round Six

In the Data Capture phase of round six, experts were asked to rank the same criteria decided upon in round five for its importance in a higher education environment. The ranked list of top IT controls in any environment was used as a base to obtain the ranked list of top IT

[8] Available at http://www.r-project.org/

controls in a higher education context. This was done in order to be able to compare apples with apples statistically. Any new controls identified for the higher education context were collected separately. Appendix K shows the email sent to participants explaining the details of this final step and asking them to expect an invitation email containing a link to another survey. See appendix L for the round six survey.

Kendall's W was calculated in the Data Analysis phase of round six, see Appendix M, as the value 0.524. The F statistic was calculated as 12.127 and the critical value for F(17, 185) with a 0.05 p-value is 1.68. Thus, the F statistic was greater than the critical value. So based on the F statistic, the null hypothesis stating that there was no significant agreement among the rankings was rejected. Statistically significant agreement among the rankings of IT control criteria in a higher education context had therefore been reached. The research was concluded at this point with the final results presented in Chapter 4 where the general ranked list obtained in round five and the higher education ranked list obtained in round six are compared. These comparisons should allow some conclusions to be drawn with regard to the aims of the research. Besides identifying the criteria most relevant to auditing IT within a higher education environment, these conclusions should show whether differences exist between what is audited in corporate organisations as opposed to that in HEIs.

Appendix N shows the email of thanks to participants for their efforts throughout the research process, which required constant back and forth communication between researcher and participant, as is typical in the use of the Delphi technique.

3.5 Challenges of the Study

As mentioned earlier, the use of the Delphi technique brings with it some challenges. The first challenge involved defining what an expert in the field actually is. The expert needed to have IT experience as well as experience in IT auditing, either as an auditor or someone who has been part of an audit. The next challenge was identifying specifically who the experts would be. This was done by referral or, where referral was not possible, by contacting specific audit houses and institutions. The third challenge was ensuring participation from the experts. It was necessary to be fully transparent with potential participants and indicate

exactly what was expected from them in order to encourage participation. A characteristic of the Delphi technique is the high attrition rate, which would have had a negative impact on the study, especially with a small pool of participants. It was therefore imperative that participants signed off on their participation and declared their participation throughout the study. Another challenge was defining the limitations for the responses required. In the initial round, it was important not to supply the control criteria outright but to encourage freedom of thought. A balance needed to be achieved between what to prime the participants with and what not to, as it was necessary to have a good idea of what kind of response was expected but not be dictated to with regard to the criteria they should respond with.

3.6 Validity and Reliability

Whitelaw (2001) states that validity and reliability are the criteria used to assess whether the research provides a good measure. Hence, validity and reliability are imperative in determining the quality of the research. It is therefore necessary to discuss how well this study meets the requirements for validity and reliability.

Broadly, validity tests how well the research method measures what it is supposed to measure, while reliability tests how consistently it measures what it is supposed to measure (Whitelaw, 2001). The very nature of the Delphi technique lends itself both to validity and reliability in that there are continuous iterations of interaction between participants, reviewing previous opinions and obtaining consensus of opinion. This allows for validation of the findings of each round against the sources of information (i.e. the participants) and increases the reliability of the information collected.

The fact that the Delphi technique sources opinions of experts with extensive knowledge and experience in the field also increases validity and reliability. The controversial question is who really is an expert, but as previously mentioned, the level and job description of participants were assessed and participants were considered senior enough to be experts in their field.

The combination of qualitative and quantitative methods used in this research also increases the validity. Holey, Feeley, Dixon, and Whittaker (2007) argue that a combination of quantitative statistics be used to "reduce subjectivity and ensure maximum validity of results in Delphi methodology for improved evidence of consensual decision-making". The Delphi technique is usually used as a qualitative measure, but the introduction of quantitative methods in the form of statistical significance can contribute to validity in a positive way.

The size of the sample can in some ways be deemed to be small in terms of validity, but for the purposes of this research and the subjective nature of the Delphi technique as well as it being a normal sample size for the Delphi, the sample size was deemed appropriate.

Another area contributing to the validity and reliability of this research is anonymity of the participants. This prevented coercion and worries over confidentiality; in other words, participants felt less restricted in voicing their opinions as fear of putting employers at risk given the industry in which the research is based was reduced, owing to anonymity.

3.7 Summary

The use of the Delphi technique was deemed appropriate for the research aims of this study for the reasons highlighted in this chapter. Applying the technique resulted in a fairly intensive series of rounds involving back and forth iteration between the Data Capture and Data Analysis phases to obtain consensus of opinion. Not only was this method subjective and qualitative, but it also involved quantitative statistical tests that aided in deciding whether consensus had been reached and how to progress between rounds. This mixed method fared well against the criteria of validity and reliability and therefore, was a good measure for the purposes of this research.

Chapter 4 Results and Discussion

4.1 Introduction

This chapter focuses on the results that were obtained during the research process and aligns them to the aims and objectives of this research. The study relied on qualitative and quantitative analysis of results in achieving the research objectives. What follows is a discussion of the qualitative results obtained in rounds one and four. Following that, quantitative results for rounds five and six are presented showing a statistical comparison of the control list obtained for corporate organisations and that for HEIs, respectively.

4.2 Qualitative Results for Round One

Round one of the research process not only sought preliminary top IT controls from participants for corporate organisations, it also asked a number of questions regarding their opinion on IT auditing in a higher education context; refer to Appendix C for details of the survey. Their responses to these questions are discussed below.

Participants were asked whether they felt that any of the audit controls tested are irrelevant in higher education (see Figure 4.1). Two participants (16.67%) said that they felt some IT controls are irrelevant in the higher education context. This was substantiated by one stating that auditors have little or no understanding of academic freedom. Another participant said that the word “irrelevant” is a strong term and perhaps the term should be “over-applied” or “over-emphasised”. Audit items should perhaps, therefore, carry different risk weightings. However, the majority agreed that the audit controls tested in a higher education context are relevant.

A further question asked participants whether they believed that HEIs face different information security risks than corporate organisations. Eight participants (66.67%) said that HEIs do face some information security risks that corporate organisations do not (see Figure 4.2).

8. From your experience in IT audits, have you ever felt that any of the audit controls tested are irrelevant in the Higher Education context?

Answer	Count	Percentage
Yes (Y)	2	16.67%
No (N)	10	83.33%
No answer	0	0.00%
Not completed or Not displayed	0	0.00%

Figure 4.1: Question 8 of round 1 survey

9. Following from this perspective, do you believe that Higher Education Institutions face any different information security risks than corporate organisations?

Answer	Count	Percentage
Yes (Y)	8	66.67%
No (N)	4	33.33%
No answer	0	0.00%
Not completed or Not displayed	0	0.00%

Figure 4.2: Question 9 of round 1 survey

In substantiating their responses, one participant said that the risk profile differs for HEIs – hackers are less likely to hack for financial benefit, but rather for fraud with respect to qualifications. Many participants supported the claim that academic information is the greater focus for information security risk in HEIs. One said that "integrity of the student record and degrees is the main concern – the incentives for financial fraud are lower". Others also concentrated on risks that sensitive academic information, for example course marks, official degree transcripts, and intellectual property, could be compromised by unauthorised personnel.

A participant went on to say that the student population inside the network is also a risk. Another participant supported this claim stating that there is a greater proportion of internal attacks in the higher education context as there is less ability to control and restrict what users do. He stated that there is more Internet bandwidth for use by researchers and students, with correspondingly less restriction on its use, as well as unauthorised services facilitating research. One participant stated that the segmentation of the network between areas accessible to students versus that of academics and administrative staff is critical as HEIs

"provide network access to thousands of potential hackers" (students). There is also licensing and illegal use of software by students on the higher education IT infrastructure.

The need to "maintain historical data beyond the seven year South African Revenue Services (SARS) requirements, specifically on student records" was another information security risk that participants felt faced an HEI as opposed to a corporate organisation. One participant said "student records need to be protected from an integrity and confidentiality perspective for a significant timeframe". Many of the items brought up by participants in this particular question were unsurprisingly covered in the discussion in Chapter 2 on the HEI being a different entity to a corporate organisation.

Following from the preceding question, another question in the round one survey asked participants whether they believed that IT audits should take the context of the organisation into account when performing an IT audit. According to the results depicted in Figure 4.3, 75% said that they believed IT audits should take higher education uniqueness into account when performing an audit.

10. Do you believe that Higher Education IT audits should take this uniqueness into account when performing an audit?

Answer	Count	Percentage
Yes (Y)	9	75.00%
No (N)	3	25.00%
No answer	0	0.00%
Not completed or Not displayed	0	0.00%

Figure 4.3: Question 10 of round 1 survey

In a following question, four participants went so far as to say that different IT controls should be measured at an HEI (see Figure 4.4). The main focus of participants in this question was on IT controls specific to systems that support the academic function. External IT audits in HEIs focus on systems that support financial administration, rather than the academic function, so it was their opinion that external audits should move away from this. Therefore, in this question, participants focussed not necessarily on measuring different IT controls, but measuring the same IT controls for academic-focussed systems. For example,

segregation of duties for maintaining academic records must be tested and not just segregation of duties for financial transactions.

11. Would you go so far as to say that different IT controls should be measured at an Higher Education Institution, in addition or in place of items you named in question 7?

Answer	Count	Percentage
Yes (Y)	4	33.33%
No (N)	8	66.67%
No answer	0	0.00%
Not completed or Not displayed	0	0.00%

Figure 4.4: Question 11 of round 1 survey

The last question in round one involved obtaining the participants' opinion on the level of maturity of IT governance in higher education. Establishing the maturity level of IT governance in higher education is important for the purposes of this research as a low maturity level suggests that there is work to be done when deciding on the way IT must be managed, controlled and audited in HEIs. A low maturity level therefore supports the significance of this research. From the responses to this question, all participants were of the opinion that IT governance in higher education is indeed low.

In substantiating their responses, one participant said that "IT departments in higher education have only now started to consider governance of IT as an important issue. HEIs still do not have the CIO[9] role embedded into the corporate culture and one of the duties of a CIO would be to enforce IT governance". Another stated that a low maturity level is because "IT generally reports too low in the hierarchy and prior to King III has not been viewed as a strategic and enabling asset. In general, IT governance does not appear to cover information governance in HEIs. Higher education CIOs do not really exist and the IT director is also generally not the CIO, even though they may carry that title". Another participant stated that "the progress of technology at an HEI is much slower than at a corporate organisation. There are too many decision-makers in the institution therefore when a simple policy needs to be approved it could take months or longer. The process should be simpler and not as complex as it is". Another stated that the reason for low maturity levels of IT governance is primarily due to "a lack of understanding of the importance or reliance on IT by the institutions

[9] CIO is an acronym for Chief Information Officer.

themselves. This leads to lack of appropriate resources in terms of funding and staffing, etc. IT is not the core business of HEIs, and so it doesn't factor highly on their agenda. However it underpins the core business of higher education, and it could not effectively function or compete without it". This was supported by another participant who stated that "IT decision making is often reactive" due to a lack of understanding of its importance. Another stated that controls are less formalised and therefore so are governance structures. He stated that IT has historically not been considered as an enabler and key player to meeting the HEIs' strategic objectives. The participant concluded that inadequate budget and insufficient focus on the importance of IT in achieving the institution's strategic objectives are key reasons as to why there is a low level of IT governance maturity.

Another participant expanded further on the concept of tight budgets in HEIs, stating that "financial implications of having mature levels of IT governance mean that usual business practice may not always be possible and so ad-hoc 'best we can do' solutions are found. I believe that the audit and the resultant report should be rigorous but that where controls are in place, the type of reporting should cater for acknowledgement of the errors but not highlight risk necessarily. In our case the report is often all about finding one error out of a large base and then reporting this as risk. All that does is invoke a tick-box mentality and does not heighten the maturity of the governance in any way whatsoever". This view supports the claim that risk weightings should differ for IT audits in higher education.

In his comment on IT governance in higher education, another participant described attraction and retention of students and staff in higher education as "a war on talent". He stated that it is important that HEIs focus on using technology to attract and retain academics and students, for example through innovation. He argued that "maturity of IT governance in higher education is therefore becoming a key area of focus". This participant also stated that the PPI Bill, referred to in Section 1.1, will have a significant impact on HEIs and their IT maturity as they now have to dedicate themselves to securing information, as required by law. Another participant supported this claim and stated that processes that increase IT governance maturity are "only starting to be in place. IT governance needs to be enforced, probably through legislation in the same manner as which financial governance is enforced".

Another participant said that the low level of maturity is due to historical reasons – there is a lower level of business drive and a different organisational culture. However, he went on to

say that “the governance levels at HEIs have been improving significantly over the past five years, and governance standards such as King III have upped the minimum levels and pressure on management”. Another stated that HEIs have varying levels of IT governance. Nevertheless, the notion throughout responses to this question was that the maturity level of IT governance in higher education is relatively low compared to that in corporate organisations.

4.3 Qualitative Results for Round Four

As is usual for the Delphi technique, the opinions voiced in round one of the subjective questioning were analysed, revised and built upon for further questioning in round four, refer to Appendix F for details of the round four survey. A summary of these answers is discussed below. It must be noted that one participant did not complete the survey for round four, but this had little bearing on the research process as responses were presented back to the participants in round five at which stage the participant who missed round four was able to provide his opinion.

In round one, participants were of the opinion that none of the controls tested in a higher education context are irrelevant, but that they should perhaps have different risk weightings. Based on this response, participants were asked to agree on whether the usual IT controls should be tested in HEIs for the purpose of an overall security assessment, but should receive different risk weightings. According to Figure 4.5, 83% of participants agreed with this statement.

Participants were asked to pass comment on the reason for their answers. The overall opinion was summed up by one as “sound IT general controls across the IT domains are key, irrespective of the entity, corporate culture and operating environment”. The participant expanded further with an example: “administrator and privileged access restrictions are still required, as a breakdown in this control could result in academic record manipulation, which could put the HEI's reputation at risk”. Another participant stated that IT controls “are still relevant, just not necessarily as relevant, thus it is not whether or not they should be tested, but the emphasis placed on them when reporting the findings”. Another complemented this

point by stating that all controls must be retained but weighted and prioritised according to risks within the higher education environment and its restricted resources.

2. It has been mentioned by participants that Higher Education Institutions (HEIs) carry differing risks to corporate organisations e.g. HEI IT systems have less restrictions on what users can do in order to allow for academic freedom and to keep research channels open; students roam within the network; academic records are as important as financials; academic records are required to be kept for longer than the usual SARS requirements for financial information so historical academic data needs to be protected; in addition, there is illegal use of software by students. Differing risks as well as the HEI being an entity whose focus is not strictly for financial gain has lead to some research participants in previous rounds saying that control criteria tested by IT auditors are often over-emphasised. It has been said that control criteria should not carry as much risk-weighting as they do in corporate organisations. For example, restriction of administrator and privileged access rights is difficult in small HEIs where tasks are shared because teams are small and organisational structure is not as formalised. However these controls should still be tested for purposes of an overall security assessment. Do you agree with this view? Do you have any comments on this?

Answer	Count	Percentage
Yes (A1)	10	83.33%
No (A2)	1	8.33%
Comments	7	58.33%
No answer	0	0.00%
Not completed or Not displayed	1	8.33%

Figure 4.5: Question 2 of round 4 survey

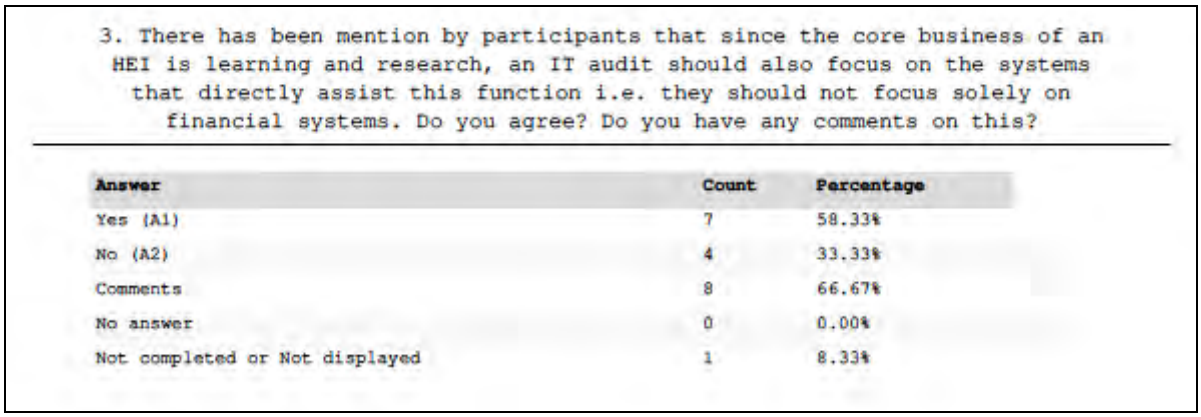
One participant argued that if the teams are small and the structure more informal then other mitigating controls are required to limit the risk. Another participant supported this by stating that "our ITGC[10] audit places an emphasis on border security. We assume that the border is porous and that the internal risk is as great, or greater, than the external risk. Thus we fail on their requirements for intrusion detection, etc. However, if they were to look at individual systems and internal network design, they'd find that their concerns were largely mitigated by other means". So even though a system could fail an audit test for standard compliance, if other mitigating controls specific to its context were tested then it would fare better.

There were two conflicting opinions regarding the testing of IT controls and academic freedom. One participant said that the overall university culture has the effect that senior users of the system such as lecturers want to have a large degree of freedom, for example during the procure-to-pay process with minimal authorisation required before a purchase is

[10] ITGC is an acronym for Information Technology Governance Committee.

made. The other participant argued that academic freedom does not have anything to do with the need for controls as controls are required in any environment. The overall opinion however, is not whether the controls are necessary, but whether the risk weighting should be as high, given the context.

The next question built upon the notion in round one responses that the IT audit should focus on systems that directly assist the core business of the HEI, i.e. learning and research, and not focus solely on financial systems. Seven participants (58%) agreed with this statement (see Figure 4.6).



3. There has been mention by participants that since the core business of an HEI is learning and research, an IT audit should also focus on the systems that directly assist this function i.e. they should not focus solely on financial systems. Do you agree? Do you have any comments on this?

Answer	Count	Percentage
Yes (A1)	7	58.33%
No (A2)	4	33.33%
Comments	8	66.67%
No answer	0	0.00%
Not completed or Not displayed	1	8.33%

Figure 4.6: Question 3 of round 4 survey

This question attracted a fair amount of comment indicating its controversial nature. The overall opinion of participants was that the core function of the HEI must be governed by the same class of controls. However, many participants stated that it depends on the type of audit being carried out and that one should distinguish between the external and internal audit. One participant stated that the external audit "tends to focus on risks that affect financial performance" whereas the internal audit "looks at general operational risks". An internal audit would therefore be more inclined to assess systems that deal with academic information and could link to an academic quality assurance assessment. External auditors do not necessarily have the required expertise to perform an adequate IT audit. One participant was adamant that the adequacy of an IT system in terms of its performance for its core mission should be measured through the quality assurance assessment and not via an external IT audit. Another stated that "if the external auditors perform the IT audit they will do so with the intention of placing reliance on the financial systems to limit their substantive audit procedures, and thus will naturally be required to focus on financial systems". He concluded

that "if internal auditors perform the IT audit, it is probably more likely that they should focus on those systems that have strategic importance within the entity". Another participant stated that "there is both a direct and an indirect financial link between the students system and the core financial system. It is therefore important to include core components of the students systems in the IT controls review process". Lastly, one participant referred to the USA's Sarbanes-Oxley principle (referred to in Section 2.3.4) in that an IT system audit should "pre-qualify" a financial audit.

Following from the participant's views in round one that maturity levels of IT governance in HEIs are low, participants were asked in round four whether this low level of maturity contributes to HEIs not seeing the need to audit systems directly supporting its core mission. Only 25% of participants agreed with this statement (see Figure 4.7). Participants felt that failure to audit systems that directly support the academic function is a combination of lack of financial resources, staff, and institutional process maturity. It is not just a matter of IT governance – "it goes beyond IT, there is no awareness at top management level". Another participant stated that the "external audit is driven by CFOs[11] and traditional audit firms. The whole focus of external audits needs to change to what the 'business' of an HEI is. Its performance is not solely measured in financial terms". One participant argued that this way of thinking is "changing due to growing IT governance maturity, as well as the DHET HEMIS[12] audits and the Auditor-General's growing involvement with HEIs". Another supported this by stating that the auditors themselves view the academic systems and financial systems independently. She stated that the academic systems and data therein are already audited via the HEMIS data audit whereas the financial systems are audited by financial audit firms. The HEMIS data audit however, does not include an IT systems audit.

In closing, round four asked participants whether undergoing an IT audit heightens the maturity of IT governance in an organisation. Participants had divided views on this (see Figure 4.8).

[11] CFO is an acronym for Chief Financial Officer.
[12] HEMIS is an acronym for the Higher Education Management Information System managed by the Department of Higher Education and Training (DHET) in South Africa. HEIs are required to submit student and staff data to the DHET for input into HEMIS and government subsidy is calculated for the HEI based on that data.

4. Most participants agree that the maturity level of IT governance in HEIs is low. Do you think that this low IT governance means that HEIs do not see the value in auditing systems that facilitate the academic function and so only financial risks are assessed? If you do not agree then please comment on why it is that HEIs only perform an audit of the IT underpinning the financial processing of the institution.

Answer	Count	Percentage
Yes (A1)	3	25.00%
No (A2)	8	66.67%
Comments	8	66.67%
No answer	0	0.00%
Not completed or Not displayed	1	8.33%

Figure 4.7: Question 4 of round 4 survey

8. IT audits are used as a means of achieving some level of IT governance. Some participants however view IT auditing with merely a tick-box mentality and no real understanding of the "business" of the organisation being audited and so undergoing an audit does not heighten the maturity of the IT governance in any way. Do you agree with this statement? Do you have any comments on this?

Answer	Count	Percentage
Yes (A1)	6	50.00%
No (A2)	5	41.67%
Comments	8	66.67%
No answer	0	0.00%
Not completed or Not displayed	1	8.33%

Figure 4.8: Question 8 of round 4 survey

One participant had an interesting perspective on this. He stated that his understanding of IT audits has over time "evolved from something-stupid-we're-forced-to-go-through to something-we-can-use-strategically-to-drive-change-in-the-organisation". This supports the claim that IT audits heighten the maturity of IT governance. Another participant stated that it depends on the IT organisation and the audit company – if there is a good partnership then the level of IT governance will improve. Another stated that "auditors will often not budge on whether something should be reported, even if there is no solution within the parameters of the institution. This causes frustration within IT teams who are reducing and eliminating risk via mechanisms that are perhaps not industry standard but never the less perform the function". This participant was therefore of the opinion that IT audits are not aligned with the maturity of IT governance. Another participant complemented this view by stating that "IT governance should not only focus on risks and audit. It is more importantly related to alignment of IT with the strategy of the HEI, on how decisions are made, resources allocated,

etc. in order to ensure alignment. In short, IT governance should revolve around the strategic nature of IT in an HEI achieving its goals".

4.4 Summary of Qualitative Results for Rounds One and Four

As a summary of the responses to the subjective questioning in rounds one and four, we can conclude that participants do not believe that audit controls are irrelevant in the higher education context, but should perhaps carry different risk weightings since HEIs do face different information security risks than corporate organisations and so uniqueness must be taken into account. From the results of round four it is evident that sound IT general controls are relevant regardless of the context, but just not necessarily as relevant depending on the context.

All participants agreed that there is a low level of maturity of IT governance in higher education. This low level of IT governance maturity increases the significance of this research in that it suggests that there is a need to establish a sense of IT importance in HEIs and a need for appropriate IT control and auditing.

Participants were of the opinion that external IT audits should not just have a financial focus and that the systems that support the core function of the HEI must be governed and audited by the same class of controls. It was affirmed that the lack of auditing of academic systems is due to lack of financial resources, staffing, and institutional process maturity, not just a low level of IT governance maturity. It was also concluded that IT audits can improve IT governance maturity if appropriately aligned.

This summarised conclusion of the subjective questioning of participants is supported by the statistical comparison of the two lists of top IT controls in corporate organisations and HEIs, established in rounds five and six, as discussed in the sections that follow.

4.5 Results for Round Five

The final list obtained in round five consisted of the top eighteen IT controls (listed in Table 4.1) that participants thought should be tested by auditors in any environment. As explained in Chapter 3, a number of rounds were required to achieve consensus on this list, as is the nature of the research technique used. The initial list proposed by participants was standardised by referring to various frameworks and an official audit list of controls tested by an audit house for a particular South African higher education institution. This aimed to keep the list in line with industry standards and bring it closer to reality should the participants stray off course. What follows is a critical discussion of the particular IT controls identified, as well as examples of how these controls can be tested in an audit process.

Policies play an integral role in IT governance, which comprises "the body of issues addressed in considering how IT is applied within the enterprise" (ISACA, 2010). Policies officially set out the processes that should be in place when applying IT. ISACA in their Guidelines on IT Audit and Assurance (2010), state that how IT is applied has a large effect on whether the organisation will achieve its strategic goals. To this end, it is fitting that the existence of IT policies was identified as the most important IT control in any environment. Policies fit into the Plan and Organise domain of COBIT 4.1 and the Plan domain of the PDCA process in ISO 27001. These domains deal with defining a strategic IT plan and the processes that go with it. The auditor must review the IT governance document and ensure that adequate policies for IT are in place and maintained.

The second most important control in any IT environment was found to be *segregation of duties*. Segregation of duties refers to the implementation of a division of roles and responsibilities such that a single individual does not have the potential to compromise a critical process (IT Governance Institute, 2007). The auditor must ensure that roles are divided and employees are performing only authorised duties that are relevant to their respective job (IT Governance Institute, 2007). COBIT describes a way to test this by investigating the number of conflicting responsibilities between employees, in other words, that roles overlap and employees do not have the ability to perform critical processes from beginning to end on their own. This is another control that not only falls into the Plan and

Table 4.1: Output from round 5 – ranked list of top IT controls in any environment

1	Policies governing security, acceptable use and confidentiality
2	Segregation of duties, i.e. one person not responsible for initiating, actioning, approving, and reviewing
3	Sound access control practices in granting, reviewing, amending and revoking user access rights
4	Sound password policies and controls, including password ageing
5	Change management, i.e. control over the authorisation, testing and approval of system changes
6	IT steering committee, i.e. IT alignment to strategic goals
7	Restriction of administrator and privileged access rights, i.e. based on principle of least privilege
8	Secure configuration of hardware and software, e.g. firewalls implemented and maintained
9	Qualified and experienced security-aware staff
10	Business continuity planning, i.e. cooperative collection of disaster recovery plans, and regular updating and testing thereof
11	Audit logging and review of logs
12	Physical security
13	Data input validation in application programmes
14	Back-ups performed regularly
15	Anti-malware software
16	Penetration testing
17	A complete inventory of authorised assets maintained
18	Wireless device control

Organise domain of COBIT and the Plan phase of the PDCA cycle in ISO 27001, but also into the Deliver and Support domain of COBIT and the Do phase in ISO 27001 when assuring that system security is maintained by removing the potential of a single individual to undermine the security of the system by being permitted to carry out critical tasks and make changes in full without interference from another individual as a control measure. It is fitting that this control came in at number two.

Thirdly, *access control* is a fairly broad concept and is covered in all the COBIT domains. There should be, not only role-based access, i.e. a level of access defined for each group of employees according to their job level, linking with the segregation of duties control, but also appropriate rules in place for the granting and revoking of that access to users. For example, in the granting of access, the auditor must ensure that there is evidence of access for an individual being authorised by a relevant party; in the revoking of access, the auditor must ensure that there is an adequate process in place for removing access if an employee were to resign. Since access controls are what allow users access to a system, it is fitting that they would be perceived as being high on the list of controls to be tested. Inadequate access controls could contribute to compromise of confidentiality and integrity, although accountability would be maintained.

Passwords are the first line of defence for almost all current corporate IT systems. Bad password practice allows anyone to gain authorised access to the system. It is therefore fitting that the existence of sound password policies is the next most important control to be tested. Auditors must ensure that the system enforces good password practices such as password ageing. Password ageing forces users to change their passwords at regular intervals, thus reducing the potential for passwords that have been in use for a long period to be found by others and used to compromise the system.

Change management refers to the processes in place when making changes to the system. Good change management ensures that adequate authorisation is obtained before implementing the change, that changes are adequately tested before release, and that there is adequate approval to release a change to the live environment. An example of good change management that an audit process could assess is the use of a version control platform in which versions of application code can be recorded for roll-back purposes. Change management is covered in the Acquire and Implement domain of COBIT and in

the Plan and Do phases of the PDCA process in ISO 27001, and is necessary to "reduce solution and service delivery defects and rework" (IT Governance Institute, 2007). Change management is important for reducing the impact of change on a functioning system.

A pertinent control objective in COBIT is the establishment of an *IT steering committee*. An IT steering committee reviews IT alignment to strategic goals in terms of everything from resource allocation to monitoring of service levels (IT Governance Institute, 2007). An IT steering committee is necessary in any medium to large organisation that relies heavily on IT. It is believed that the IT steering committee plays an integral role in IT governance of an organisation so it is fitting that it appears in the top half of the list of IT controls to be reviewed.

The control rated the seventh most important is *restriction of administrator and privileged access rights*, which implies that access must be based on the principle of least privilege. This principle states that users must be given enough access according to their roles, but nothing more. Although this control is broadly covered in the aforementioned access and segregation of duties controls, it receives special definition in that it deals with administrator access, or "root" access. Administration of the IT system is carried out using administrator access, but unrestricted access to the root allows easy and devastating compromise of the system.

The eighth control, *secure configuration of hardware and software*, refers to the implementation and maintenance of firewalls, network segmentation, security certificates and various other measures to prevent unauthorised access. This is a broad concept and is covered mostly in the Delivery and Support domain of COBIT (and the Do phase in ISO 27001) in ensuring system security. The number of unauthorised IP addresses denied would be an example of how an auditor would test this control (IT Governance Institute, 2007). This control is critical in ensuring system security and thus is rightfully in the top half of the list.

COBIT defines four IT resources that are leveraged to deliver against organisation goals: applications, information, infrastructure and people. An IT infrastructure uses "people skills and technology infrastructure to run automated business applications while leveraging business information" (IT Governance Institute, 2007). People are therefore an

integral part of the IT organisation which is why *qualified and experienced security-aware staff* comes in at number nine on the list. This can be tested in the audit process by investigating whether adequate reference checks are carried out when staff are employed, or checking whether adequate computer skills testing is performed when selecting an appropriate candidate for employment in a computer-based environment.

Business continuity planning is another important control to have in place in order to recover from unplanned incidents that compromise the system and/or the information that it holds. To test this control, the auditor must review the plans in place as well as any incident reports and follow-up activities for incidents that may have occurred and which required disaster recovery procedures. The auditor must also ensure that offsite back-up storage is utilised. Business continuity planning is covered in the Deliver and Support domain of COBIT under Ensure Continuous Service.

The eleventh top control identified is *audit logging and review of logs*. It is critical to record log-in attempts and changes to the database, as this provides for accountability within the system. Whether these logs are reviewed remains a challenge for many organisations. This item, therefore, rates fairly low on the list.

The IT Governance Institute (2007, p. 145) stated that "effective management of the physical environment reduces business interruptions from damage to computer equipment and personnel". This can be measured in an audit process by the number of incidents occurring due to physical security breaches as well as reviewing the measures taken to secure the physical assets, for example physical access to the building, or reviewing measures taken to control the environment, for example fire detectors in server rooms. Ensuring *physical security* was seen as number twelve in the list of eighteen top IT controls in any environment.

In order to manage the quality of data input as well as prevent the entering of malicious input into the system, *data input validation* is required on the application layer. There are many unfortunate examples where attacks such as *SQL injection* have occurred because of inadequate data input validation. Structured Query Language (SQL) is a fourth generation language used to process and interrogate data in a relational database. A SQL injection attack can take advantage of inadequate data input validation by entering SQL statements

that affect the execution of legitimate predefined SQL commands on the database allowing attackers to effectively read, modify, add and delete sensitive data from the database, or execute administrative operations on the database, amongst other unauthorised actions (Agarwwal et al., 2008). As most databases contain consumer or user information; these attacks can lead to identity theft, loss of confidential information, or fraud (Halfond, Viegas, and Orso, 2006). Variations of SQL injection attacks allow attackers to gain full control of the host server (Halfond et.al., 2006). Obviously this can have devastating consequences for the organisation so adequate data input validation in applications is critical. Data input validation is covered in the Plan and Organise domain of COBIT.

The fourteenth control is *back-ups performed regularly*. Back-ups are related to business continuity planning, but receive special mention here because they are integral to the functioning of an organisation even if there is no official business continuity plan. Back-ups could be as simple as making copies of data on an external hard drive, or could be more large-scale in terms of utilising off-site back-up storage with remote changing of back-up tapes by a robot. As it is a corrective control, back-ups fall lower on the list than some of the first-line preventative controls appearing higher on the list.

With the ever increasing number of Internet users, comes an increasing amount of malicious software being released. The use of *anti-malware software* to prevent damage caused by viruses, worms, spyware, and so on, is specified as a control objective in the Deliver and Support domain of COBIT and the Do phase of the PDCA process in ISO 27001 to ensure system security. This control rates low on the list of top controls because it should not be key if all the aforementioned controls have been implemented adequately.

Penetration testing is used as a measure of how well a system would fare against attack, in other words, its responsiveness to threats. Penetration testing is most often only used by large corporate organisations that rely heavily on IT. The output of a penetration test is a report on vulnerabilities identified in the IT infrastructure and should be used to rectify them. Penetration testing is not high on the list as a control. In fact, it was not on the original list identified earlier in the research process (see Table 3.1).

Another control that was included at the end is a *complete inventory of authorised assets to be maintained*. This allows the system to know which IP addresses are valid and should have access and to deny access to those that are not. This did not rate as highly as the other controls and, like penetration testing, was not on the original list identified earlier in the research process (see Table 3.1).

Owing to the increased use of wireless devices, participants felt that mention of a *wireless device control* was necessary as a top IT control, and as such, was included last on the list. This control also did not feature on the original list identified earlier in the research process (see Table 3.1).

In conclusion, the final list of top IT controls required to be tested in any environment, obtained via consensus-based research from experts in the field, seems rational and fair when compared to industry standards, for example, COBIT or ISO 27001. The next list to be discussed is that obtained from the same experts in round six for the top IT controls required to be tested in an HEI.

4.6 Results for Round Six

The list of top IT controls for South African HEIs identified by participants in round six is presented in Table 4.2. This list is compared with the list obtained in round five in two ways: first, through a statistical test using Spearman's rank correlation coefficient, and then, by means of a qualitative comparison between the two lists where relative positioning of the controls in each list is assessed.

Table 4.2: Output from round 6 – ranked list of top IT controls in higher education

1	Sound password policies and controls, including password ageing
2	Policies governing security, acceptable use and confidentiality
3	Sound access control practices in granting, reviewing, amending and revoking user access rights
4	IT steering committee, i.e. IT alignment to strategic goals
5	Change management, i.e. control over the authorisation, testing and approval of system changes
6	Segregation of duties, i.e. one person not responsible for initiating, actioning, approving, and reviewing
7	Restriction of administrator and privileged access rights, i.e. based on principle of least privilege
8	Qualified and experienced security-aware staff
9	Business continuity planning, i.e. cooperative collection of disaster recovery plans, and regular updating and testing thereof
10	Secure configuration of hardware and software, e.g. firewalls implemented and maintained
11	Back-ups performed regularly
12	Physical security
13	Data input validation in application programmes
14	Audit logging and review of logs
15	Anti-malware software
16	A complete inventory of authorised assets maintained
17	Penetration testing
18	Wireless device control

4.7 Quantitative Comparison of the Two Control Lists

To assess statistical comparability between the two lists, Spearman's rank correlation coefficient was used. As mentioned before, Kendall's W is only used when there are more than two lists to compare so although Kendall's W was used to compare the lists for agreement between participants, it was considered inappropriate for this particular comparison where only two lists were compared.

Spearman's rank correlation coefficient is defined by Equation (3) where d_i is the difference in rankings for each object i:

$$r_s = 1 - \frac{6\sum_{i=1}^{n} d_i^2}{n(n^2-1)} \qquad (3)$$

Mazurek (2011) states that Spearman's rank correlation coefficient is normalised to the interval <-1,1> where maximum similarity is given by $r_s = 1$ and maximum dissimilarity is given by $r_s = -1$.

In this study, the number of objects n is 18, i.e. the number of control criterion being ranked. To calculate d_i, the ranking of one criterion is subtracted from the ranking of the same criterion in the second list. For example, for the segregation of duties control, the ranking of 2 in the first list, is subtracted from the ranking of 6 in the HEI list giving $d_i = -4$ and $d_i^2 = 16$. The calculation for the complete list is given in Appendix O.

Spearman's rank correlation coefficient was thus calculated to be 0.942, which means that there is very high similarity between the two lists. In conclusion, the two lists are statistically very similar and so it is fitting to use generic IT audit control criteria to audit a South African HEI, but it is worth noting that there are slight differences in rankings as explained in the qualitative analysis that follows. This supports the claim made in earlier rounds that the same IT controls must be tested in HEIs, albeit with different risk weightings.

4.8 Qualitative Comparison of the Two Control Lists

The discussion in Chapter 2, as well as the responses to the subjective questioning in rounds one and four, proposed the notion of an HEI as a different entity and presented differences between HEIs and corporate organisations. Characteristics particular to an HEI were found to be, for example, the concept of academic freedom, small IT budgets, and emphasis on issues of academia rather than IT. For these reasons, IT in higher education is somewhat lax and under-emphasised. This culture is a possible contributor to the following controls found to be more, or less, significant in a higher education environment in round six.

The three controls that moved up significantly on the HEI list of top IT controls are: sound password policies and controls, IT steering committee, and back-ups performed regularly. This suggests that these controls are considered more important in a South African higher education context than in general. Possible reasons for this are discussed below.

As mentioned previously, passwords are the first-line of defence for most IT systems. If there is less emphasis placed on IT security in a higher education environment then sound password practices are one of the most important aspects to get right. It is therefore fitting that this is given top importance in the higher education context as an IT control to be tested.

Similarly, ensuring that there is an adequate IT steering committee and one that meets regularly, is another way of increasing the maturity of IT in higher education. The level of maturity of IT governance in South African HEIs was argued by the participants as being relatively low. It is therefore fitting that the IT steering committee should be perceived as a more important function in a higher education context.

Following from the perceived relaxed IT environment in South African HEIs, a possible lack of official business continuity plans in HEIs means that, at the minimum, back-ups should be performed if no other corrective controls are in place. Alternatively, if IT security is low then back-ups are important to restore the HEI to original functioning after data loss. For these reasons, back-ups obtained greater importance on the higher education list of controls.

Three controls that moved down significantly on the HEI list of top IT controls are: segregation of duties, audit logging and review of logs, and secure configuration of hardware and software. This suggests that these controls are considered less important in a higher education context than in general. Possible reasons for this are discussed below.

COBIT states that segregation of duties is "commonly used in large organisations so that no single person is in a position to introduce fraudulent or malicious code without detection" (IT Governance Institute, 2007, p. 193). In the higher education IT context where budgets are tight and IT teams are small, segregation of duties is mostly not possible. Limited resources mean that one person may need to perform a task on his/her own without segregation. It is therefore fitting that this control rated lower on the list for South African HEIs and it should ideally receive less weighting in a South African higher education context as it is often not possible to implement thoroughly.

It is also fitting that audit logging and review of logs rated lower on the list. The reasoning behind this is also due to small IT teams in HEIs. Time pressures and lack of people resources mean that review of logs is impossible. Spending time on other security matters is often deemed more appropriate use of time than performing a detective role of reviewing logs.

Secure configuration of hardware and software such as implementing firewalls and ensuring network segmentation is very difficult in HEIs. Since academic material must be available to a wide variety of stakeholders in the HEI, allowing for this while maintaining security is a challenge. This context must be taken into account when reviewing this control and so it is fitting that it rates lower on the list for HEIs.

This qualitative comparison of relative positioning of items on each list suggests that, even though the same IT controls must be tested, that they should possibly carry different risk weightings according to the context in which they operate.

4. 9 Additional Controls Identified

It remains to be noted that some additional controls were identified for testing in a South African HEI. However, these were very similar controls to those that had already been identified. What made them additional was that they related to academic information systems, not financial systems. These controls were explored in the round four survey (see Figure 4.9) and were based on previous responses.

a. Network segmentation controls (to separate student domain from staff and admin systems)

Answer	Count	Percentage
Yes (Y)	9	75.00%
No (N)	2	16.67%
No answer	0	0.00%
Not completed or Not displayed	1	8.33%

b. Segregation of duties for non-financial transactions such as student results

Answer	Count	Percentage
Yes (Y)	11	91.67%
No (N)	0	0.00%
No answer	0	0.00%
Not completed or Not displayed	1	8.33%

c. Access security for non-financial transactions such as student results

Answer	Count	Percentage
Yes (Y)	11	91.67%
No (N)	0	0.00%
No answer	0	0.00%
Not completed or Not displayed	1	8.33%

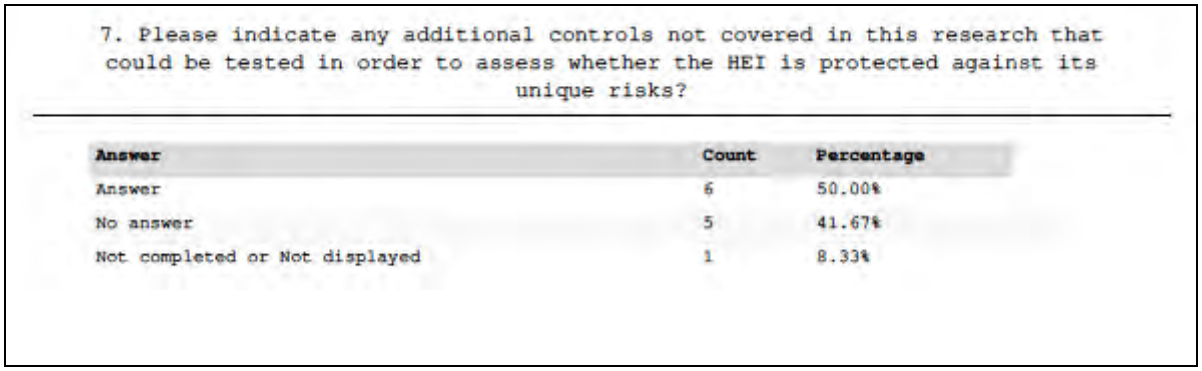
d. Controls with respect to intellectual property

Answer	Count	Percentage
Yes (Y)	9	75.00%
No (N)	2	16.67%
No answer	0	0.00%
Not completed or Not displayed	1	8.33%

Figure 4.9: Additional controls identified in round 4

The additional controls identified are: network segmentation controls (covered in the aforementioned lists under secure configuration of hardware and software), segregation of duties and access security for non-financial transactions, such as student results, and controls relating to intellectual property.

Figure 4.10 shows that participants were further prompted for controls in a free-format structure. These controls were not mentioned by participants in earlier rounds and so were not integrated into the main results. They are also perceived as not being the main controls to be tested and would possibly fall under broader items already discussed. One participant mentioned a control related to (a) in Figure 4.9 by stating that postgraduate students are often also staff members, so segregation of duties relating to roles should be tested. A few participants mentioned physical security and access security controls in terms of attendance at examinations. Another participant mentioned the creation and reviewing of information policies for how academic information such as research data, outputs, and knowledge resources are stored and protected. Another proposed the auditing of government grants based on the enrolment and results of students. These controls are worthy of mention, but were not deemed appropriate for integration into the main list.



7. Please indicate any additional controls not covered in this research that could be tested in order to assess whether the HEI is protected against its unique risks?

Answer	Count	Percentage
Answer	6	50.00%
No answer	5	41.67%
Not completed or Not displayed	1	8.33%

Figure 4.10: Question 7 of round 4 survey

4.10 Comparison with the Literature

As discussed in Chapter 2, general frameworks such as COBIT have relevance in a higher education context (Council, 2006; Viljoen, 2005; Sayana, 2002). In addition, this study has shown that it is appropriate to use the same set of IT audit control criteria that is used to audit IT in a corporate organisation, for a South African HEI. Thus, as IT control frameworks are

used as a source of audit control criteria, it is applicable to use these frameworks on which to base an IT audit in an HEI. This study is therefore in line with what is presented in the literature.

In addition, comparisons can be drawn between this study and the study of top IT controls in small businesses (Busta et al., 2006) discussed in Section 2.7. Busta et al. (2006) found the top three IT controls for small businesses to be: updated firewalls and secure wireless connections, up-to-date virus and spyware protection, and regular and tested back-up procedures. These three controls did not feature as highly on the HEI list. In fact, they featured quite low. The HEI list seemed to focus more on strategy and policies as having the highest importance. This can either be attributed to the strategic focus of an HEI, or it could be due to the job level of the experts who participated in the study as they are at the level where strategy is more focal to their work. Alternatively it could be attributed to the geographic location of the study administered by Busta et al. (2006) in the US, as opposed to this study being based in South Africa. Nonetheless, IT as part of the organisation's long- and short-term plans featured number five on the top IT controls in a small business. This shows that strategy is still fairly prominent in small businesses in the US.

Interestingly, the topmost control in small businesses, i.e. updated firewalls and secure wireless connections, appeared notably lower on the HEI list when compared with the corporate list and that of small businesses. This supports the notion proposed in Section 4.8 where implementation of firewalls and ensuring network segmentation is very difficult in HEIs. This is because academic material must be available to a wide variety of stakeholders in the HEI. Nevertheless, allowing for this while maintaining security is a challenge. Therefore, whereas small businesses and larger corporate organisations rate the importance of this control quite highly, it is fitting that the HEI list rates it lower.

File access privilege controls achieved a similar rating in both studies, that is, number four on the small business list, and number seven on the HEI list. It must be noted that the HEI list contained eighteen controls and the small business list contained eleven, so proportion must be taken into account when comparing the two lists. We can therefore say that ranking four on the small business list is similar to ranking seven on the HEI list.

Segregation of duties was rated low or not at all on both lists, whereas it rated higher on the corporate list. This supports the fact that small businesses and HEIs have small IT teams that are less structured, and thus segregation of duties is often not possible, as discussed in Section 4.8. The same can be said for the reviewing of audit logs control.

Identification and authentication procedures scored fairly highly on all lists, showing that this is an important control in any environment. Employee awareness and data input validation were two controls that were present on all lists and were ranked similarly; in fact, employee awareness was ranked slightly higher than data input validation on all lists, i.e. for small businesses, corporate organisations, and HEIs. This supports the fact that having employees that are security aware reduces the need for data input validation, but obviously does not negate it.

Based on the discussion in this section, it is evident that the literature supports, to a large extent, what has been found in this study.

4.11 Summary

This chapter presented the final results of this study, as well as discussions thereof. It provided statistical validation, as well as validation against the literature. Based on the responses in each round of this research process, as well as the qualitative and quantitative analysis thereof, what remains is to conclude with a discussion of whether the objectives of this research as presented in Chapter 3 have been reached. This is done in Chapter 5.

Chapter 5 Conclusion and Future Work

"A compliance-based approach adds little value to the governance of a company as it merely assesses compliance with existing procedures and processes without an evaluation of whether or not the procedure or process is an adequate control". This quote by the Institute of Directors in Southern Africa and the King Committee on governance in the King III report (2009, p. 14) sums up the essence of this research. Higher education institutions undergo IT audits that require a level of compliance. But are the controls relevant in this context? This research attempted to answer that question.

5.1 Summary of the Research Process

This research made use of the Delphi technique to obtain consensus of opinion from experts in the IT and auditing fields, in order to achieve its research objectives. The participants were drawn from HEIs as well as audit firms around the country, on a voluntary basis. Communication was via email and data was collected by means of online surveys.

As is typical of the Delphi technique, the study underwent a number of rounds of questioning and surveys to obtain subjective opinion on IT auditing in a higher education context as well as to identify two IT control lists. Kendall's coefficient of concordance was used to assess whether agreement had been reached on the lists for each round. This statistic determined progression onto the next round of surveys. The first list that was identified depicted the participants' consensus of the top IT controls that should be tested in an IT audit for a corporate organisation. The second list consisted of the top IT controls that should be tested in an IT audit for South African HEIs.

The two lists were compared in two ways to check whether there are differences between IT auditing in HEIs and that in corporate organisations. First, a statistical test using Spearman's rank correlation coefficient was performed. Second, a qualitative comparison of the relative positioning of IT controls in each list was carried out. Responses to subjective questioning apart from the list of controls were also analysed.

Spearman's rank correlation coefficient was found to indicate a high similarity between the two lists. This means that participants felt that the same IT controls should be audited in an HEI as in a corporate organisation. However, qualitative analysis of the two lists shows slight differences in rankings and suggests that further research may find that there is a statistically significant difference in risk weightings that should be assigned to IT controls tested in an IT audit of a South African HEI.

An additional finding was that other systems should be audited in both internal and external IT audits of an HEI, not just the financial system. This supports the finding that the two lists are similar and the study suggests that the same controls must be used to audit other systems that directly support the core function of the institution, in other words, academic-related systems.

5.2 Achievement of Research Objectives

This study had the following research objectives:

- To determine whether there are differences between corporate organisations and HEIs in terms of IT.
- To assess whether it is fitting to use generic IT control criteria to audit an HEI.
- To identify control criteria (including the associated ranking of these criteria) relevant to IT audits in HEIs.

The first objective was achieved by finding that there are indeed differences between corporate organisations and HEIs in terms of IT. These differences include academic freedom, lack of financial resources, and an academic focus rather than focus on financial profit. It was also found that the maturity level of IT governance in higher education is relatively low compared to corporate organisations. This low maturity level indicates that research such as this to identify effective ways of managing and auditing IT is indeed important.

Regarding the second research objective, it was found that, to an extent, it is fitting to use generic IT control criteria to audit an HEI. All IT infrastructures require sound IT general controls to perform their function. It was found that, although all controls are deemed relevant, some are not as relevant or even possible in a higher education context, for example segregation of duties. These controls should possibly receive different risk weightings in HEIs as opposed to corporate organisations. Further research using more specific controls is necessary to prove this statistically.

In achieving the third objective, a ranked list of IT controls required to be tested in an HEI was formulated via consensus of expert opinion. It was also found that similar controls in academic systems directly supporting the core function of the HEI must also be tested during the external audit process.

Based on the results presented in Chapter 4, the objectives of this research have thus been achieved. In conclusion, it was found that HEIs should continue to audit their IT in the same way that corporate organisations do, but should acknowledge that the institution faces different risks. The need for future research in this area has been highlighted by this study and is discussed in Section 5.4.

5.3 Assessment of the Findings

In order to critically assess the findings of this research, it is necessary to investigate the consequences of the limitations stated in Section 1.7.1. Limitations can lead to the collection of obscured data which could have consequently invalidated the results.

The limitation introduced by the static nature of email communication and online surveys which provides less opportunity for discussion by participants, was offset by the advantage of an outstanding mix of participants from around the country made possible through the use of email.

Issues involved in the administering of questionnaires, such as leading questions, and ambiguity, was compensated for in the iterative nature of the research process. If a question was misinterpreted, there was opportunity to revise it in a following round.

A limitation introduced through the use of the Delphi technique is a high attrition rate. This was offset by ascertaining the experts' participation upfront and maintaining it by having a manageable sample of participants who could receive special attention if interest waned. This also counteracted another limitation, that is, the lack of incentive to participate apart from interest in the research question. The iterative nature of the Delphi technique and its use of experts in the field provides for a reliable method for this research.

Another limitation introduced through the use of participants with different work experience is that of IT control lists not being too specific. If control lists were more specific it is possible that the study could have obtained different results. This remains an area for future work.

5.4 Recommendations and Future Research

Although no statistically significant difference was found between the corporate IT control list and that of HEIs, this research provides a solid base for further research as qualitative comparison of the lists suggests that differences in risk weightings exist.

However, the IT controls in each list were somewhat broad. If the controls were drilled down and refined, it may lead to a different solution. Controls could be broken down into four categories: management controls (e.g. security policies), business processes (e,g, business continuity planning), operational controls (e.g. back-ups) and technical controls (e,g, anti-virus software) (Wright, 2006). An alternative would be to base control selection on the eleven domains of ISO 27001. This could be used to explore the applicability of a specific standard to HEIs.

If further research were to prove that that there is a statistical difference between the controls used to audit corporate organisations and HEIs, it could prompt the IT auditing community to rethink their current audit practice in the higher education context.

References

Abrahams, L, 2003. *Thinking Without the Box: Perspectives on Education and Convergence.* Convergence, vol. 3, no. 4, pp. 60-61.

Amos, T and Pearse, N, 2008. *Pragmatic Research Design: An Illustration of the Use of the Delphi Technique*. The Electronic Journal of Business Research Methods, vol. 6, no. 2, pp. 95-102.

ASAUDIT, 2012. *ASAUDIT home page*. [Online]. Available at: http://www.asaudit.ac.za [Accessed 1 December 2012].

Agarwwal, A, Bellucci, D, Coronel, A, DiPaola, S, Fedon, G, Goodman, A, Heinrich, C, Horvath, K, Ingrosso, G, Liverani, RS, Kuza, A, Luptak, P, Mavituna, F, Mella, M, Meucci, M, Morana, M, Parata, A, Su, C, Sureddy, HS, Roxberry, M, and Stock, A, 2008. *OWASP Testing Guide v3.0*. [Online]. Available at: https://www.owasp.org/ [Accessed 4 June 2011].

Barlette, Y and Fomin, V, 2008. *Exploring the suitability of IS Security Management Standards for SMEs*. In Proceedings of 41st Hawaii International Conference on System Sciences (HICSS), Los Alamitos, pp. 308- 317.

Busta, B, Portz, K, Strong, J, and Lewis, R, 2006. *Expert Consensus on the Top IT Controls for a Small Business*. ISACA Information System Controls Journal, vol. 6, pp. 22-24.

Council, CL, 2006. *An Investigation of a COBIT Systems Security IT Governance Initiative in Higher Education*, PhD dissertation, AAT 3206177, Nova South Eastern University.

Cuhls, K, 2003. *Delphi Method*. [Online]. Available at: http://www.unido.org/fileadmin/import/16959_DelphiMethod.pdf [Accessed 22 November 2011].

Disterer, G, 2013. *ISO/IEC 27000, 27001 and 27002 for Information Security Management*. Journal of Information Security, vol. 4, pp. 92-100.

EDUCAUSE, 2002. *Higher Education Contribution to National Strategy to Secure Cyberspace*. A report submitted by EDUCAUSE on behalf of the higher education community. Also available at: http://net.educause.edu/ir/library/pdf/NET0027.pdf [Accessed 27 November 2011].

Gallegos, F, Manson, DP, and Allen-Senft, S, 1999. *Information Technology Control and Audit*. CRC Press LLC, Boca Raton.

Glenn, M, 2008. *The Future of Higher Education: How Technology Will Shape Learning*. An Economist Intelligence Unit Publication.

Halfond, WGJ, Viegas, J, and Orso, A, 2006. *A Classification of SQL Injection Attacks and Countermeasures*. In Proceedings of the International Symposium on Secure Software Engineering (ISSSE 2006).

Hewlett-Packard Development Company, 2006. *ITIL Foundation for IT Service Management*. Student Guide Publication.

Holey, EA, Feeley, JL, Dixon, J, and Whittaker, VJ, 2007. *An Exploration of the Use of Simple Statistics to Measure Consensus and Stability in Delphi Studies*. BMC Medical Research Methodology, vol. 7, no. 52.

Hsu, CC and Sandford, BA, 2007. *The Delphi Technique: Making Sense of Consensus*. Practical Assessment, Research & Evaluation, vol. 12, no. 10, pp. 1-8.

ISACA, 2010. *IT Standards, Guidelines, and Tools and Techniques for Audit and Assurance and Control Professionals*. ISACA publication.

ISACA, n.d. (a). *Glossary*. [Online]. Available at: http://www.isaca.org/Pages/Glossary.aspx?tid=4292&char=I [Accessed 26 November 2011].

ISACA, n.d. (b). *COBIT FAQs*. [Online]. Available at: http://www.isaca.org/Knowledge-Center/cobit/Pages/FAQ.aspx [Accessed 3 November 2012].

ISACA, n.d. (c). *COBIT 5: A Business Framework for the Governance and Management of Enterprise IT*. [Online]. Available at: http://www.isaca.org/COBIT/Pages/default.aspx [Accessed 20 October 2012].

IT Governance Institute, 2000. *COBIT 3rd Edition Audit Guidelines*. IT Governance Institute Publication. ISBN: 1-893209-18-0.

IT Governance Institute, 2007. *COBIT 4.1*. IT Governance Institute Publication. ISBN: 1-933284-72-2.

ITIL, 2012. *What is ITIL?* [Online]. Available at: http://www.itil-officialsite.com/AboutITIL/WhatisITIL.aspx [Accessed 20 October 2012].

Institute of Directors in Southern Africa and the King Committee on Governance, 2009. *King Report on Governance for South Africa*. King III code for corporate governance. IOD Report.

Laurillard, D, 2006. *E-Learning in Higher Education*. In P Ashwin (ed). Changing Higher Education: The Development of Learning and Teaching. London, RoutledgeFalmer.

Legendre, P, 2010. *Coefficient of concordance*. In NJ Salkind (ed). Encyclopedia of Research Design. SAGE Publications Inc., Los Angeles, pp. 164-169.

Maria, E and Haryani, E, 2011. *Audit Model Development of Academic Information System: Case Study on Academic Information System of Satya Wacana*. Researchers World – Journal of Art, Science & Commerce, vol. 11, no. 2, pp. 12-24.

Mazurek, J, 2011. *Evaluation of Ranking Similarity in Ordinal Ranking Problems*. Acta academica karviniensia, pp. 119-128.

Naudé, P, 2011. *Lets Protect Our Universities*. [Online]. Available at: http://www.ru.ac.za/media/rhodesuniversity/content/documents/institutionalplanning/Let's%20protect%20our%20universities%20-%20Piet%20Naude%2023May2011.pdf [Accessed 30 November 2011].

Okoli, C and Pawlowski, SD, 2004. *The Delphi method as a Research Tool: An Example, Design Considerations and Applications*. Information and Management, vol. 42, no. 1, pp. 15–29.

Pare, G, Sicotte, C, Joana, M, and Girouard, D, 2007. *Prioritizing the Risk Factors Influencing the Success of Clinical Information System Projects: A Delphi Study in Canada*. Methods Inf Med, vol. 47, no. 3, pp. 251-259.

Price, P and Officer, E, 2005. *Can Professionals from the Corporate World Succeed as Managers in Higher Education?* In Proceedings from the Conference on Trends in the Management of Human Resources in Higher Education. Paris, France.

Republic of South Africa, 2012. *Protection of Personal Information Bill*. Government Gazette No. 32495. Also available at: http://www.justice.gov.za/legislation/bills/B9-2009_ ProtectionOfPersonalInformation.pdf [Accessed 5 December 2012].

Sarbanes, P and Oxley, M, 2002. *The Sarbanes-Oxley Act of 2002*. Public Law 107–204, 107th Congress. Also available at: http://www.sec.gov/about/laws/soa2002.pdf [Accessed at 5 December 2012].

Sayana, SA, 2002. *The IS Audit Process*. ISACA Journal, vol. 1. [Online] Available at: http://www.isaca.org/Journal/Past-Issues/2002/Volume-1/Pages/The-IS-Audit-Process.aspx [Accessed at 7 December 2012].

Schutte, JG, 2002. *Virtual Teaching in Higher Education: The New Intellectual Superhighway or Just Another Traffic Jam?* [Online]. Available at: http://www.csun.edu/sociology/virexp.htm [Accessed at 3 November 2012].

Sharma, NK, and Dash, PK, 2012. *Effectiveness of ISO 27001, as an Information Security Management System: An Analytical Study of Financial Aspects*. Far East Journal of Psychology and Business, vol. 9, no. 3, pp. 42-55.

Snyder-Halpern, R, Thompson, CB, and Schaffer, J, 2000. *Comparison of Mailed vs. Internet Applications of the Delphi Technique in Clinical Informatics Research*. In Proceedings of the AMIA Symposium, American Medical Informatics Association, p. 809-813.

Stewart, N, 2010. *An Audience with the GRI's King*. Inside Investor Relations. [Online]. Available at: http://www.insideinvestorrelations.com/articles/case-studies/16371/audience-mervyn-king/ [Accessed 1 December 2012].

Susanto, H, Almunawar, MN, and Tuan, YC, 2011. *Information Security Management System Standards: A Comparative Study of the Big Five*. International Journal of Electrical & Computer Sciences, vol. 11, no. 5, pp. 23-29.

Tavakol, M and Dennick, R, 2011. *Making sense of Cronbach's alpha*. International Journal of Medical Education, vol. 2, pp. 53-55. ISSN: 2042-6372.

Viljoen, S, 2005. *Applying a Framework for IT Governance in South African Higher Education Institutions*. Masters dissertation, Nelson Mandela Metropolitan University.

Weber, R, 1999. *Information Systems Control and Audit*. Prentice Hall, Upper Saddle River, NJ.

Whitelaw, PA, 2001. *Reliability and Validity: The Terrible Twins of Good Research*. Multifactor Leadership Questionnaire Network, pp. 108-110.

Wilson, JM, 2001. *The Technological Revolution: Reflections on the Proper Role of Technology in Higher Education*. In Altbach, PG, Gumpart, PJ, Johnstone, DB (eds). In Defence of American Higher Education, pp. 202-26, Johns Hopkins University Press, London.

Wright, S, 2006. *Measuring the effectiveness of security using ISO 27001*. White paper – Siemens Communications.

Appendices

Appendix A – Initial contact with potential participants, via email

My name is Lynne Angus, a Masters student at Rhodes University wishing to obtain participants for my research. The focus of my thesis is IT audits in higher education. The purpose of the research is to ascertain whether IT audits in higher education should differ from IT audits in the corporate world. It has been argued that an higher education institution is a very different entity to organisations in the corporate world so perhaps their IT should be audited differently.

My research will be based on the ratings and opinions of professionals in the IT field who have been involved at some stage in an IT auditing process. This could be IT professionals in higher education institutions who are at the receiving end of IT audits or IT auditors themselves. The study will be email-based and consist of a few rounds to achieve consensus in the rating of IT controls and their relevance in a higher education context. It is proposed to take place over a period of three to four months this year very much at the leisure of the participant, and each round will not be time-intensive. A more detailed methodology will be forwarded to interested parties. It is hoped that the experience brought to the table from the various parties will lead to rich research around the relevance of IT audits conducted in higher education.

At this stage of the research, a pool of IT professionals who are specifically able to contribute to this research needs to be generated. As such your assistance is required. Please could you provide the name and contact details of those individuals you feel are best able to contribute to this research. There is no limit to the number of people as long as you feel they are able to contribute.

Thank you

Lynne Angus

Appendix B – Email contact to elicit the participants' response for round 1 survey

Dear `Research Participant`,

Thank you very much for agreeing to participate in this research. Your input is greatly appreciated and is invaluable to the completion of this research.

The aim of the research is to ascertain whether differences exist between the governance and auditing of IT in Higher Education Institutions as opposed to corporate organisations. It will consist of a few rounds of online questionnaires in order to gain consensus on the matter. The first round is somewhat open-ended in order not to lead answers. Further rounds will be multiple choice format.

The first round of data collection is ready for your participation. You will receive an email within two days from "LimeService" containing a link to complete the survey online at infosec.limeask.com. This is the researcher's personal domain name hosted by LimeSurvey.com. Please do not hesitate to contact me if you doubt the integrity of the link.

The deadline for completion of this survey is Monday 21 May 2012. Please contact me if you are unable to complete it by that time. You will be sent a reminder email a few days before the deadline.

Once the deadline has passed, the responses will be collated and further rounds will be communicated to you.

Once again, thank you for your participation and I look forward to your response.

Kind regards

Lynne Angus

Appendix C – Round 1 survey

IT Governance in Higher Education

This questionnaire is the first of several rounds of a research study aimed at IT professionals in Higher Education Institutions and IT auditors that audit these institutions. The aim of the research is to ascertain whether differences exist between the governance and auditing of IT in Higher Education Institutions as opposed to corporate organisations.

Please note that this round is somewhat free-format in an attempt not to lead answers. Any future rounds will be multiple choice format. Please take a moment to complete this questionnaire. Your input is very much appreciated.

There are 17 questions in this survey

Preliminary Questions

1 [Q0001]1. What is your current job designation? *

Please write your answer here:

2 [Q0002]2. Are you employed by a higher education institution or an audit firm? *

Please choose only one of the following:

- ◯ Higher education insitution
- ◯ Audit firm
- ◯ Other

3 [Q0003]3. Please indicate the extent to which you are involved in the IT audit process? *

Please choose only one of the following:

- ◯ Not involved
- ◯ Slightly involved
- ◯ IT audits form 50% of my work
- ◯ Very much involved
- ◯ IT audits form 100% of my work

Appendix C (continued)

4 [Q0004]4. Please indicate the extent to which you are involved in the IT audit process at Higher Education Institutions? *

Please choose only one of the following:

- ○ Not involved
- ○ Slightly involved
- ○ IT audits in Higher Education form 50% of my work
- ○ Very much involved
- ○ IT audits in Higher Education form 100% of my work

5 [Q0005]5. How detailed is your IT audit or the IT audits you perform i.e. just auditing of the IT infrastructure that handles financials (general IT controls review) or a full audit of the whole IT infrastructure? *

Please choose only one of the following:

- ○ IT general controls review
- ○ Audit of entire IT infrastructure
- ○ Other [ ]

Appendix C (continued)

IT Risks and Audits

6 [Q0006]6. What do you believe are the top five information security risks in any environment? *

Please write your answer here:

7 [Q0007]7. What do you believe are the top ten most important IT controls in any environment? *

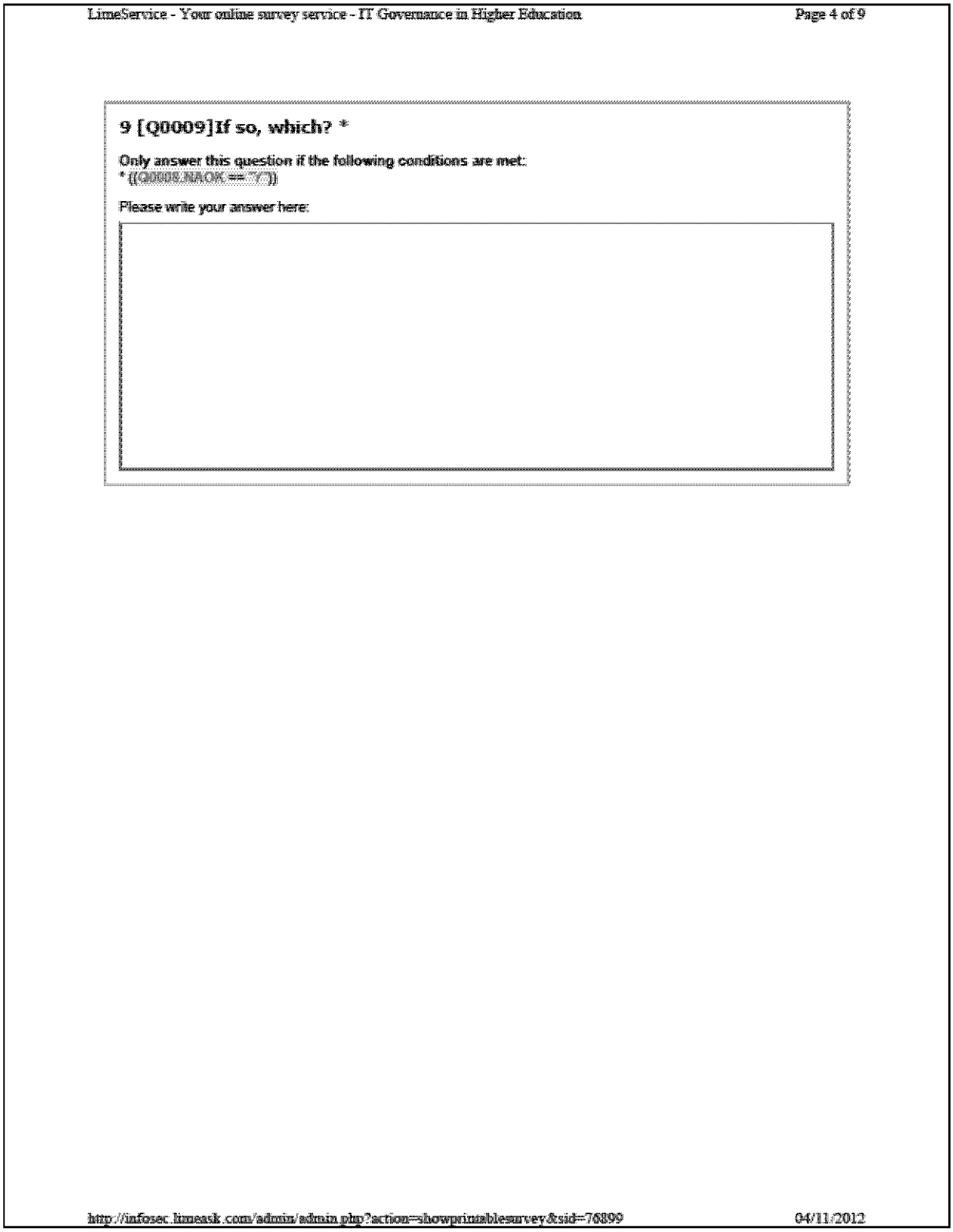
Please write your answer here:

8 [Q0008]8. From your experience in IT audits, have you ever felt that any of the audit controls tested are irrelevant in the Higher Education context? *

Please choose only one of the following:

- ○ Yes
- ○ No

Appendix C (continued)



9 [Q0009]If so, which? *

Only answer this question if the following conditions are met:
* ({Q0008.NAOK == "Y"})

Please write your answer here:

Appendix C (continued)

Higher Education IT Risks and Audits

The Higher Education environment can be unique in many ways e.g. decentralised decision-making, academic freedom, often small IT budget but high reliance on IT, specialised technologies e.g. e-learning requiring log session lengths, increased file-sharing, availability all year round.

10 [Q0010]9. Following from this perspective, do you believe that Higher Education Institutions face any different information security risks than corporate organisations? *

Please choose only one of the following:

- ◌ Yes
- ◌ No

11 [Q0011]If so, what are they? *

Only answer this question if the following conditions are met:
* ((Q0010.NAOK == "Y"))

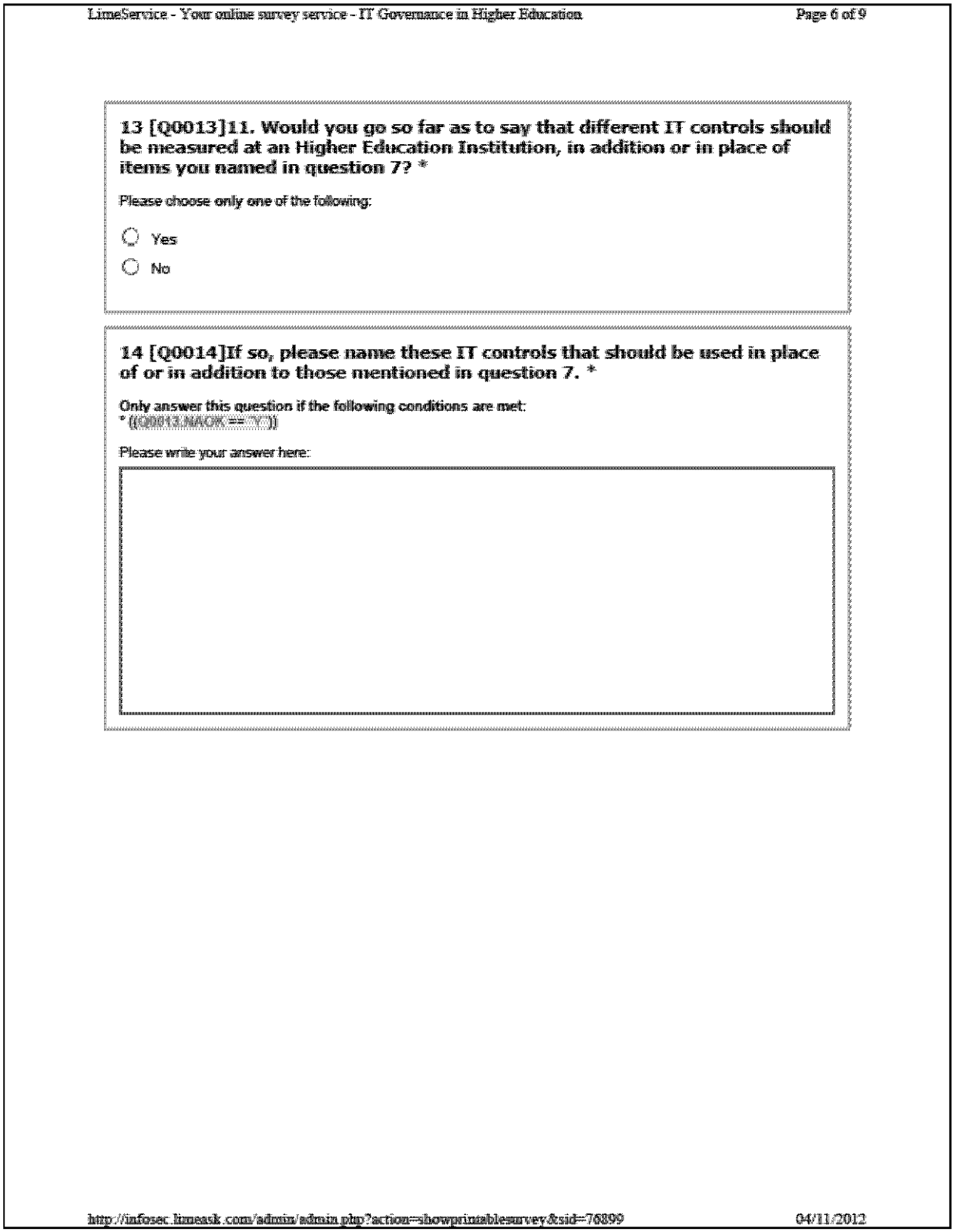
Please write your answer here:

12 [Q0012]10. Do you believe that Higher Education IT audits should take this uniqueness into account when performing an audit? *

Please choose only one of the following:

- ◌ Yes
- ◌ No

Appendix C (continued)



13 [Q0013]11. Would you go so far as to say that different IT controls should be measured at an Higher Education Institution, in addition or in place of items you named in question 7? *

Please choose only one of the following:

- ○ Yes
- ○ No

14 [Q0014]If so, please name these IT controls that should be used in place of or in addition to those mentioned in question 7. *

Only answer this question if the following conditions are met:
* ({Q0013.NAOK == 'Y'})

Please write your answer here:

Appendix C (continued)

IT Governance

Although IT is of high importance in Higher Education, it has been found by many that the level of maturity of IT governance at Higher Education Institutions is low and that it should receive urgent attention. Low IT governance maturity could be attributed to a culture of shared decision-making coupled with academic freedom and creativity, amongst other factors.

15 [Q0015]12. Please indicate the extent to which you agree that IT governance in Higher Education has a low maturity level. *

Please write your answer here:

16 [Q0016]13. If the maturity level is indeed low, why would you say so? *

Please write your answer here:

Appendix C (continued)

17 [Q0017]14. Please detail any further opinions that you may have on IT governance in Higher Education?

Please write your answer here:

Appendix C (continued)

01.01.1970 – 01:00

Submit your survey.
Thank you for completing this survey.

Appendix D – Round 2 email to elicit agreement on round 1 list

Dear `Research Participant`,

Thank you very much for completing my survey online. The quality of the responses received was astounding and I am very grateful for the effort invested by participants.

I have collated the responses and would like to proceed with the second round. The methodology being used is the Delphi technique which aims to achieve consensus of opinion. Attached is a visual representation of the methodology for this research, if you are interested. Note there will be couple more rounds.

From the responses, the top IT controls have been identified. This round simply requires you to answer whether you agree with the list. If not, please identify which items should be replaced, state why, and with what, or if you believe any item needs rephrasing. The controls are as follows, in no particular order:

a. Sound access control practices in granting, reviewing, amending and revoking user access rights
b. Segregation of duties, i.e. one person not responsible for initiating, actioning, approving, and reviewing
c. Policies governing security
d. Change control, i.e. control over the authorisation, testing and approval of application programme changes
e. Back-ups performed regularly
f. Firewalls implemented and maintained
g. Secure configuration of hardware and software
h. Qualified security-aware staff
i. Effective password controls and password ageing
j. Anti-virus software
k. Audit logging and review of logs
l. Disaster recovery planning, and regular updating and testing thereof
m. Data input validation in application programmes
n. Physical security
o. Restriction of administrator and privileged access rights, i.e. based on the principle of least privilege

Please respond directly to me via email by next Friday 8 June 2012. Your input is very much appreciated.

Kind regards,
Lynne

Appendix E – Round 3 email to elicit agreement on round 2 list

Dear `Research Participant`,

The list of top IT controls presented to you the other day has changed slightly due to feedback received. The research methodology requires a further iteration of responses to achieve agreement on the modified list. Note that these are controls in ANY environment. The higher education environment will be dealt with later.

Please state whether you agree with the following list of top IT controls:

a. Sound access control practices in granting, reviewing, amending and revoking user access rights
b. Segregation of duties, i.e. one person not responsible for initiating, actioning, approving, and reviewing
c. Policies governing security, acceptable use and confidentiality
d. Change management, i.e. control over the authorisation, testing and approval of system changes
e. Back-ups performed regularly
f. Secure configuration of hardware and software, e.g. firewalls implemented and maintained
g. Qualified and experienced security-aware staff
h. Sound password policies and controls, including password ageing
i. Anti-malware software
j. Audit logging and review of logs
k. Business continuity planning i.e. cooperative collection of disaster recovery plans, and regular updating and testing thereof
l. Data input validation in application programmes
m. Physical security
n. Restriction of administrator and privileged access rights, i.e. based on principle of least privilege
o. IT steering committee i.e. IT alignment to strategic goals
p. A complete inventory of authorised assets maintained
q. Wireless device control
r. Penetration testing

Please respond at your earliest convenience, no later than Wednesday 27 June.

Thanks once again.

Kind regards,
Lynne

Appendix F – Round 4 survey

IT Governance in Higher Education: Round 4

In the last couple of rounds of this research, we have identified a list of top IT control processes to be tested in an IT audit for any organisation. This round involves ranking these controls in terms of their importance in contributing to the IT security of an organisation whose main focus is for financial profit. Later we will rank the list for an organisation whose main focus is not for financial profit, namely a higher education institution.

There are 11 questions in this survey

IT Governance in Higher Education: Round 4

Appendix F (continued)

1 [Q1]1. Please rank the list below in order of importance in contributing to the security of an organisation's IT systems, considering that the organisation's main focus is financial profit.
*

Please number each box in order of preference from 1 to 18

- [ ] Sound access control practices in granting, reviewing, amending and revoking user access rights
- [ ] Segregation of duties, i.e. one person not responsible for initiating, actioning, approving, and reviewing
- [ ] Policies governing security, acceptable use and confidentiality
- [ ] Change management, i.e. control over the authorisation, testing and approval of system changes
- [ ] Back-ups performed regularly
- [ ] Secure configuration of hardware and software, e.g. firewalls implemented and maintained
- [ ] Qualified and experienced security-aware staff
- [ ] Sound password policies and controls, including password ageing
- [ ] Anti-malware software
- [ ] Audit logging and review of logs
- [ ] Business continuity planning i.e. cooperative collection of disaster recovery plans, and regular updating and testing
- [ ] Data input validation in application programmes
- [ ] Physical security
- [ ] Restriction of administrator and privileged access rights, i.e. based on principle of least privilege
- [ ] IT steering committee i.e. IT alignment to strategic goals
- [ ] A complete inventory of authorised assets maintained
- [ ] Wireless device control
- [ ] Penetration testing

Appendix F (continued)

2 [Q2]2. It has been mentioned by participants that Higher Education Institutions (HEIs) carry differing risks to corporate organisations e.g. HEI IT systems have less restrictions on what users can do in order to allow for academic freedom and to keep research channels open; students roam within the network; academic records are as important as financials; academic records are required to be kept for longer than the usual SARS requirements for financial information so historical academic data needs to be protected; in addition, there is illegal use of software by students. Differing risks as well as the HEI being an entity whose focus is not strictly for financial gain has lead to some research participants in previous rounds saying that control criteria tested by IT auditors are often over-emphasised. It has been said that control criteria should not carry as much risk-weighting as they do in corporate organisations. For example, restriction of administrator and privileged access rights is difficult in small HEIs where tasks are shared because teams are small and organisational structure is not as formalised. However these controls should still be tested for purposes of an overall security assessment. Do you agree with this view? Do you have any comments on this?
*

Please choose only one of the following:

- ○ Yes
- ○ No

Make a comment on your choice here:

Appendix F (continued)

3 [Q3]3. There has been mention by participants that since the core business of an HEI is learning and research, an IT audit should also focus on the systems that directly assist this function i.e. they should not focus solely on financial systems. Do you agree? Do you have any comments on this? *

Please choose only one of the following:

- ○ Yes
- ○ No

Make a comment on your choice here:

Appendix F (continued)

4 [Q4]4. Most participants agree that the maturity level of IT governance in HEIs is low. Do you think that this low IT governance means that HEIs do not see the value in auditing systems that facilitate the academic function and so only financial risks are assessed? If you do not agree then please comment on why it is that HEIs only perform an audit of the IT underpinning the financial processing of the institution. *

Please choose only one of the following:

- ○ Yes
- ○ No

Make a comment on your choice here:

Appendix F (continued)

5 [Q5]5. If HEIs are a unique entity and HE IT systems are associated with different risks then perhaps the controls tested do not carry as much weight as those that are not tested could. Do you agree with this statement? Do you have any comments on this?
*

Please choose only one of the following:

- ○ Yes
- ○ No

Make a comment on your choice here:

Appendix F (continued)

IT Governance in Higher Education: Round 4

The following are controls specific to HEIs that have been mentioned by participants as necessary to be tested in IT audits for HEIs, please indicate whether you agree that they should be tested.

6 [Q6a]a. Network segmentation controls (to separate student domain from staff and admin systems) *

Please choose only one of the following:

- ○ Yes
- ○ No

7 [Q6b]b. Segregation of duties for non-financial transactions such as student results *

Please choose only one of the following:

- ○ Yes
- ○ No

8 [Q6c]c. Access security for non-financial transactions such as student results *

Please choose only one of the following:

- ○ Yes
- ○ No

9 [Q6d]d. Controls with respect to intellectual property *

Please choose only one of the following:

- ○ Yes
- ○ No

Appendix F (continued)

10 [Q7]7. Please indicate any additional controls not covered in this research that could be tested in order to assess whether the HEI is protected against its unique risks?

Please write your answer here:

11 [Q8]8. IT audits are used as a means of achieving some level of IT governance. Some participants however view IT auditing with merely a tick-box mentality and no real understanding of the "business" of the organisation being audited and so undergoing an audit does not heighten the maturity of the IT governance in any way. Do you agree with this statement? Do you have any comments on this?
*

Please choose only one of the following:

- ○ Yes
- ○ No

Make a comment on your choice here:

Appendix F (continued)

01.01.1970 – 01:00

Submit your survey.
Thank you for completing this survey.

Appendix G – Kendall's coefficient of concordance calculation for round 4

Rankings of objects per respondent											
RM	NR	AB	RP	JK	KM	GH	JB	TC	CJ	HH	SUM
2	13	1	3	1	2	1	7	3	2	1	36
4	2	2	5	6	4	6	5	2	8	3	47
12	1	3	4	2	3	9	4	1	6	5	50
13	7	5	7	3	6	8	8	5	4	6	72
15	3	6	12	8	12	10	3	4	5	4	82
3	15	11	2	17	1	15	1	16	1	2	84
11	9	4	6	12	10	4	6	8	7	8	85
5	8	14	15	7	5	3	13	7	9	11	97
8	12	7	13	10	14	14	2	6	10	12	108
14	14	9	1	9	11	13	11	13	3	10	108
9	5	10	8	16	7	12	10	11	18	7	113
6	11	12	17	4	9	5	12	9	14	14	113
10	6	8	11	5	17	7	9	14	16	13	116
17	4	13	14	14	13	2	14	15	17	9	132
16	10	16	16	15	8	11	15	12	15	16	150
7	17	17	9	13	16	18	16	10	11	17	151
1	18	18	10	18	18	16	17	17	13	15	161
18	16	15	18	11	15	17	18	18	12	18	176

Chi	Chi-squared
36	1296
47	2209
50	2500
72	5184
82	6724
84	7056
85	7225
97	9409
108	11664
108	11664
113	12769
113	12769
116	13456
132	17424
150	22500
151	22801
161	25921
176	30976
1881	223547

k = 11
n = 18

$$W = \frac{\sum_{i=1}^{n} X_i^2 - \frac{\left(\sum_{i=1}^{n} X_i\right)^2}{n}}{\frac{1}{12} \cdot k^2 \cdot \left(n^3 - n\right)}$$

$$= \frac{223547 - \frac{1881^2}{18}}{\frac{1}{12} \cdot 11^2 \cdot (18^3 - 18)}$$

$$= 0.460$$

Appendix H – Email to elicit response for round 5 survey

Dear `Research Participant`,

Thank you for your participation in this research which is drawing to a close.

You will receive another invitation to participate in a survey tomorrow. It is a very short survey (only one question) and will not take more than two minutes to complete. Please complete it at your earliest convenience before next week Tuesday 11 September.

Kind regards

Lynne Angus

Appendix I – Round 5 survey

IT Governance in Higher Education: Round 5

This short round involves obtaining rank consensus on the list of IT controls that were ranked in the previous round according to order of importance to an organisation whose main focus is for financial gain.

There are 1 questions in this survey

IT Governance in Higher Education: Round 5

Appendix I (continued)

1 [Q1]

Below is a ranked list of IT controls based on the response from participants in round 4. Note that it is still based on IT in an organisation whose main focus is financial gain, not a higher education institution. In order to honour the research process, this list must be ranked again in order to achieve consensus on the ranking from the previous round. You may find that it is already ranked correctly, in which case you may preserve the ranking.

You will note that participants ranked, for example, anti-malware software quite low in importance. This is either intentional or not. Please give this list critical thought now that it is ranked based on previous response rankings.

*

Please number each box in order of preference from 1 to 18

Appendix I (continued)

- [ ] Policies governing security, acceptable use and confidentiality
- [ ] Segregation of duties, i.e. one person not responsible for initiating, actioning, approving, and reviewing
- [ ] Sound access control practices in granting, reviewing, amending and revoking user access rights
- [ ] Sound password policies and controls, including password ageing
- [ ] Change management, i.e. control over the authorisation, testing and approval of system changes
- [ ] IT steering committee i.e. IT alignment to strategic goals
- [ ] Restriction of administrator and privileged access rights, i.e. based on principle of least privilege
- [ ] Secure configuration of hardware and software, e.g. firewalls implemented and maintained
- [ ] Qualified and experienced security-aware staff
- [ ] Business continuity planning i.e. cooperative collection of disaster recovery plans, and regular updating and testing thereof
- [ ] Audit logging and review of logs
- [ ] Physical security
- [ ] Data input validation in application programmes
- [ ] Back-ups performed regularly
- [ ] Anti-malware software
- [ ] Penetration testing
- [ ] A complete inventory of authorised assets maintained
- [ ] Wireless device control

Appendix I (continued)

01.01.1970 – 01:00

Submit your survey.
Thank you for completing this survey.

Appendix J – Statistical analysis for round 5

Rankings of objects per respondent												
RM	NR	AB	RP	JK	KM	GH	JB	TC	CJ	HH	CF	SUM
1	1	1	2	1	1	1	3	1	1	1	9	23
4	2	2	3	2	4	3	7	2	2	2	6	39
5	5	3	4	3	2	2	6	3	4	3	5	45
6	4	6	5	4	3	4	10	4	5	4	3	58
7	6	5	6	5	14	5	4	6	6	5	4	73
2	10	9	1	6	13	6	1	7	3	6	14	78
8	3	4	7	7	11	7	5	5	8	7	10	82
13	7	7	8	8	5	8	11	11	9	8	11	106
12	11	8	9	9	6	12	2	12	10	9	7	107
10	12	10	10	10	12	11	9	13	7	10	1	115
9	9	11	12	13	7	14	18	9	11	11	16	140
11	8	12	18	11	8	13	16	8	12	12	12	141
14	13	13	11	12	15	9	15	14	13	13	8	150
15	14	14	13	14	16	10	8	10	14	14	2	144
16	15	15	14	16	18	15	13	15	15	15	13	180
17	16	16	15	17	9	16	14	17	16	16	17	186
3	17	17	16	18	17	17	17	16	17	17	18	190
18	18	18	17	15	10	18	12	18	18	18	15	195

Chi	Chi-squared
23	529
39	1521
45	2025
58	3364
73	5329
78	6084
82	6724
106	11236
107	11449
115	13225
140	19600
141	19881
150	22500
144	20736
180	32400
186	34596
190	36100
195	38025
2052	285324

k = 12
n = 18

$$W = \frac{\sum_{i=1}^{n} X_i^2 - \frac{\left(\sum_{i=1}^{n} X_i\right)^2}{n}}{\frac{1}{12} \cdot k^2 \cdot \left(n^3 - n\right)}$$

$$= \frac{285324 - \frac{2052^2}{18}}{\frac{1}{12} \cdot 12^2 \cdot (18^3 - 18)}$$

$$= 0.73667$$

Appendix J (continued)

$F = (k - 1)\, W / (1 - W)$

$= (12 - 1)(0.73667) / (1 - 0.73667)$

$= 30.77268$

$\nu_1 = n - 1 - (2 / k)$

$= 18 - 1 - (2 / 12)$

$= 16.8333$

$\nu_2 = \nu_1 (k - 1)$

$= 16.8333 (12 - 1)$

$= 185.1666$

P-value = 0.05

Critical value = 1.68

Appendix K – Email to elicit response for round 6 survey

Dear `Research Participant`,

We have reached the last step in the research process at last. You will be receiving an invitation shortly to participate in another online survey. It is just one question but remains the crux of the research as a whole. This is perceived to be the last round but if consensus is not achieved then there will be an additional round.

Once again, thank you for your valued participation in this research.

Kind regards
Lynne

Appendix L – Round 6 survey

IT Governance in Higher Education: Round 6

After obtaining consensus on a ranked list of IT controls for corporate organisations, the focus is now on higher education institutions.

There are 1 questions in this survey

IT Governance in Higher Education: Round 6

Appendix L (continued)

1 [1]

Participants have noted that control criteria in IT audits for HEIs should carry different risk weightings. Below is the ranked list of IT control criteria for corporate organisations decided upon in earlier rounds. Please rank it for an HEI, bearing in mind the different risks it faces. Also bear in mind this is not whether or not the controls should be tested, but how much emphasis should be placed on them when reporting the findings.

Below are some opinions expressed in this research about IT in HEIs which may assist in answering the question:
a. Segregation of duties is sometimes not completely possible within the small and informal organisational structure of an HEI.
b. Restriction of privileged access rights is sometimes not possible within the small and informal organisational structure of an HEI.
c. Policies are sometimes not as formalised.
d. Little emphasis is placed on having an IT steering committee.
e. Small budget for physical security.
f. Small budget for penetration testing.
g. Little capacity for regular review of audit logs.
h. The use of anti-malware software may be more important as private student computers have access to the internal network.

*

Please number each box in order of preference from 1 to 18

Appendix L (continued)

- [ ] Policies governing security, acceptable use and confidentiality
- [ ] Segregation of duties, i.e. one person not responsible for initiating, actioning, approving, and reviewing
- [ ] Sound access control practices in granting, reviewing, amending and revoking user access rights
- [ ] Sound password policies and controls, including password ageing
- [ ] Change management, i.e. control over the authorisation, testing and approval of system changes
- [ ] IT steering committee i.e. IT alignment to strategic goals
- [ ] Restriction of administrator and privileged access rights, i.e. based on principle of least privilege
- [ ] Secure configuration of hardware and software, e.g. firewalls implemented and maintained
- [ ] Qualified and experienced security-aware staff
- [ ] Business continuity planning i.e. cooperative collection of disaster recovery plans, and regular updating and testing thereof
- [ ] Audit logging and review of logs
- [ ] Physical security
- [ ] Data input validation in application programmes
- [ ] Back-ups performed regularly
- [ ] Anti-malware software
- [ ] Penetration testing
- [ ] A complete inventory of authorised assets maintained
- [ ] Wireless device control

Appendix L (continued)

01.01.1970 – 01:00

Submit your survey.
Thank you for completing this survey.

Appendix M – Statistical analysis for round 6

Rankings of objects per respondent														
RP	TC	JK	JB	HH	CF	RM	AB	CJ	KM	NR	GH	SUM	Chi	Chi-squared
3	2	3	5	4	1	5	7	3	6	1	3	43	43	1849
2	1	2	2	1	14	1	1	2	4	14	1	45	45	2025
4	8	5	4	5	5	8	3	6	7	9	2	66	66	4356
1	3	1	1	2	13	2	12	1	1	16	13	66	66	4356
5	6	9	3	3	3	14	5	5	13	5	4	75	75	5625
7	5	4	6	6	6	17	6	7	5	11	12	92	92	8464
6	9	7	7	8	11	9	4	8	8	10	9	96	96	9216
8	10	10	8	16	2	4	2	10	10	7	10	97	97	9409
10	4	11	10	9	8	11	11	4	2	15	14	109	109	11881
13	7	8	13	13	10	3	9	9	9	8	8	110	110	12100
11	11	14	12	11	4	10	14	14	15	3	6	125	125	15625
17	13	6	11	10	15	15	10	12	12	6	5	132	132	17424
14	15	13	14	12	7	6	13	13	14	2	11	134	134	17956
9	14	16	9	7	16	16	8	11	11	17	15	149	149	22201
12	17	12	16	14	17	7	15	15	16	4	7	152	152	23104
15	16	15	18	15	18	13	18	18	3	18	18	185	185	34225
18	12	18	17	17	9	18	16	16	17	12	16	186	186	34596
16	18	17	15	18	12	12	17	17	18	13	17	190	190	36100
													2052	270512

k=12
n=18

$$W = \frac{\sum_{i=1}^{n} X_i^2 - \frac{\left(\sum_{i=1}^{n} X_i\right)^2}{n}}{\frac{1}{12} \cdot k^2 \cdot \left(n^3 - n\right)}$$

$$= \frac{270512 - \frac{2052^2}{18}}{\frac{1}{12} \cdot 12^2 \cdot (18^3 - 18)}$$

$$= 0.524$$

Appendix M (continued)

$F = (k - 1)\, W / (1 - W)$

$= (12 - 1)(0.524) / (1 - 0.524)$

$= 12.127$

$\nu_1 = n - 1 - (2 / k)$

$= 18 - 1 - (2 / 12)$

$= 16.8333$

$\nu_2 = \nu_1 (k - 1)$

$= 16.8333 (12 - 1)$

$= 185.1666$

P-value = 0.05

Critical value = 1.68

Appendix N – Email of thanks for participation in research

Hi there,

Just a word of thanks for participating in my masters research on IT auditing in higher education. I am very grateful for the efforts afforded by participants throughout the research process. Please let me know if you wish to see the results when they are available.

Thanks again.

Kind regards,
Lynne

Appendix O – Spearman's rank correlation coefficient for comparison of the two final lists

	Corporate	HEI	d	d^2
Policies governing security, acceptable use and confidentiality	1	2	-1	1
Segregation of duties, i.e. one person not responsible for initiating, actioning, approving, and reviewing	2	6	-4	16
Sound access control practices in granting, reviewing, amending and revoking user access rights	3	3	0	0
Sound password policies and controls, including password ageing	4	1	3	9
Change management, i.e. control over the authorisation, testing and approval of system changes	5	5	0	0
IT steering committee, i.e. IT alignment to strategic goals	6	4	2	4
Restriction of administrator and privileged access rights, i.e. based on principle of least privilege	7	7	0	0
Secure configuration of hardware and software, e.g. firewalls implemented and maintained	8	10	-2	4
Qualified and experienced security-aware staff	9	8	1	1
Business continuity planning, i.e. cooperative collection of disaster recovery plans, and regular updating and testing thereof	10	9	1	1
Audit logging and review of logs	11	14	-3	9
Physical security	12	12	0	0
Data input validation in application programmes	13	13	0	0
Back-ups performed regularly	14	11	3	9
Anti-malware software	15	15	0	0
Penetration testing	16	17	-1	1
A complete inventory of authorised assets maintained	17	16	1	1
Wireless device control	18	18	0	0
				56

$$r_s = 1 - \frac{6\sum_{i=1}^{n} d_i^2}{n(n^2-1)}$$

$$= 1 - \frac{6 \times 56}{18(18^2-1)}$$

$$= 0.942$$