Towards a Framework for the Integration of Information Security into Undergraduate Computing Curricula

by

Lindokuhle Gcina Gomana

2017

Towards a Framework for the Integration of Information Security into Undergraduate Computing Curricula

by

Lindokuhle Gcina Gomana

Dissertation

Submitted in fulfilment of the requirements for the degree

Masters

in

Information Technology

in the

Faculty of Engineering, the Built Environment and Information Technology

of the

Nelson Mandela Metropolitan University

Supervisor: **Prof Lynn Ann Futcher**

Co-Supervisor: **Prof Kerry-Lynn Thomson**

October 2017

Declaration of Originality

I, **Lindokuhle Gcina Gomana**, **210031492**, hereby declare that the dissertation for **Masters in Information Technology** is my own work and that it has not previously been submitted for assessment or completion of any postgraduate qualification to another University or for another qualification.

____

Lindokuhle Gcina Gomana

Abstract

Information is an important and valuable asset, in both our everyday lives and in various organisations. Information is subject to numerous threats, these can originate internally or externally to the organisation and could be accidental, intentional or caused by natural disasters. As an important organisational asset, information should be appropriately protected from threats and threat agents regardless of their origin. Organisational employees are, however, often cited as the “weakest link” in the attempt to protect organisational information systems and related information assets. Additionally to this, employees are one of the biggest and closest threat-agents to an organisation’s information systems and its security.

Upon graduating, computing (Computer Science, Information Systems and Information Technology) graduates typically become organisational employees. Within organisations, computing graduates often take on roles and responsibilities that involve designing, developing, implementing, upgrading and maintaining the information systems that store, process and transmit organisational information assets. It is, therefore, important that these computing graduates possess the necessary information security skills, knowledge and understanding that could enable them to perform their roles and responsibilities in a secure manner. These information security skills, knowledge and understanding can be acquired through information security education obtained through a qualification that is offered at a higher education institution.

At many higher education institutions where information security is taught, it is taught as a single, isolated module at the fourth year level of study. The problem with this is that some computing students do not advance to this level and many of those that do, do not elect information security as a module. This means that these students may graduate and be employed by organisations lacking the necessary information security skills, knowledge and understanding to perform their roles and responsibilities securely. Consequently, this could increase the number of employees who are the “weakest link” in securing organisational information systems and related information assets.

The ACM, as a key role player that provides educational guidelines for the development of computing curricula, recommends that information security should be pervasively integrated into computing curricula. However, these guidelines and recommendations do not provide sufficient guidance on ***“how”*** computing educators can pervasively integrate information security into their modules. Therefore, the problem identified by this research is that **“*currently, no generally used framework exists to aid the pervasive integration of information security into undergraduate computing curricula*”**.

The primary research objective of this study, therefore, is **to develop a framework to aid the pervasive integration of information security into undergraduate computing curricula**. In order to meet this objective, secondary objectives were met, namely: *To develop an understanding of the importance of information security*; *to determine the importance of information security education as it relates to undergraduate computing curricula*; and *to determine computing educators’ perspectives on information security education in a South African context*.

Various research methods were used to achieve this study’s research objectives. These research methods included a *literature review* which was used to define and provide an in-depth discussion relating to the domain in which this study is contained, namely: *information security* and *information security education*. Furthermore, a *survey* which took the form of semi-structured interviews supported by a questionnaire, was used to elicit computing educators’ perspectives on information security education in a South African context. *Argumentation* was used to argue towards the proposed framework to aid the pervasive integration of information security into undergraduate computing curricula. In addition, *modelling* techniques were used to model the proposed framework and *scenarios* were used to demonstrate how a computing department could implement the proposed framework. Finally, *elite interviews* supported by a questionnaire were conducted to validate the proposed framework.

It is envisaged that the proposed framework could assist computing departments and undergraduate computing educators in the integration of information security into their curricula. Furthermore, the pervasive integration of information security into undergraduate computing curricula could ensure that computing graduates exit higher education institutions possessing the necessary information security skills, knowledge and understanding to enable them to perform their roles and responsibilities securely.

It is hoped that this could enable computing graduates to become a stronger link in securing organisational information systems and related assets.

Acknowledgements

I would like to thank the **Lord** for the strength, knowledge and understanding he has given me throughout the course of completing this dissertation. Moreover, he has blessed me with all the people who have supported me, as listed below:

- My supervisors, **Prof Lynn Ann Futcher** and **Prof Kerry-Lynn Thomson**, whose knowledge, guidance, support and patience have played a major role in the completion of this dissertation. You have shaped this study with your guidance and diligence.
- My parents, **Nomawonga** and **Tembani Gomana**; my dearest friend **Timothy Speckman** and the rest of my family and friends. I appreciate your encouragement, love and support.
- **Lynn Nontokozo Sibanda**, for proofreading this dissertation.
- The financial assistance of the **National Research Foundation (NRF)** and **NMMU Research Capacity Development (RCD)** towards this research is hereby acknowledged. Opinions expressed and conclusions arrived at, are those of the authors, and are not necessarily to be attributed to the NRF or RCD.

Table of Contents

List of Tables

List of Figures

Chapter 1 – Introduction

This chapter introduces this research project by providing a high-level overview of the study undertaken. It introduces information security as the main field of study, with information security within higher education in computing being the key area upon which this research project is based.

1.1. Background Information

Information is the lifeblood of modern-day organisations, as it is an important organisational asset that is core to their well-being. Landoll (2006, p. 30) specifically defines an information asset as information that has value to an organisation. The important objective for most organisations is, therefore, to protect and to increase the value of their information as well as the information systems that process the information (Hinson, 2005; Landoll, 2006, p. 30; Safa, Von Solms, & Futcher, 2016; Von Solms & Von Solms, 2009, p. 113).

Organisations reap numerous benefits from information assets, these could include providing a competitive edge over their competitors, allowing financial prosperity and real-time reporting (Posthumus, Von Solms, & King, 2010). However, threats which could include but are not limited to viruses, worms, Trojan horses, Denial of Service (DoS) attacks and malware, could potentially cause severe damage to an organisation's information assets, financial prosperity, reputation and its well-being. These threats to information could originate internally or externally and could be accidental, intentional or caused by natural disasters. As an important organisational asset, information should, therefore, be appropriately protected from threats and threat agents regardless of their origin (ISO/IEC 27002, 2013; ISO/IEC 27005, 2011; Safa et al., 2015). Additionally, according to Landoll (2006, p. 194), the increase of threats to an organisation's information assets has led to a greater appreciation for a strong information security capability within organisations.

Whitman and Mattord (2014, p. 4) define information security as, "…the protection of information and its critical characteristics (confidentiality, integrity and availability), including the systems and hardware that store, transmit that information, through the application of policy, training and awareness programmes, and technology".

As seen in the information security definition provided above, a number of security measures play an integral role in the effective protection of information assets from potential threats. These security measures include technical measures (technology), organisational measures (policies and practices) and human factors (education, training and awareness) (McCumber, 2005; Safa et al., 2016).

Technical measures are focused on technological solutions, which are applied by humans in order to securely design, deploy, configure and maintain information systems. However, with technical measures, humans are often the key failure point in achieving the required security level of information systems and related information assets (Furnell & Clarke, 2012). Agreeably, Deloitte (2009) and Kabay (2002) specifically cited humans as the "weakest link" in the attempt to protect information systems.

According to Hinson (2005), the human factor is an immediate, close and dangerous threat agent that could cause vulnerabilities to exploit information systems and related information assets. Amankwa, Loock and Kritzinger (2014) and Whitman (2003) specifically refer to the human factor as the most overlooked aspect of an organisation's attempt to secure their information assets. McCumber (2005), however, refers to the human factor as the most important security measure and it is by ensuring that employees understand the threats and vulnerabilities associated with the use of information systems that they can effectively attempt to deal with the other security measures. Agreeing with this, Amankwa et al. (2014) argue that as, "… employees are part of the information security problem, they must, be part of the information security solution by means of information security education, training and awareness". The human factors' security measure incorporates education, training and awareness.

Since the success of an organisation's information security depends on the human factor to effectively deal with the technological and organisational security measures, organisations should ensure that the human factor is appropriately addressed. Appropriate information security education, training and awareness could enable employees to effectively protect organisational information systems and related information (Amankwa et al., 2014; Hinson, 2005; McCumber, 2005).

According to Amankwa et al. (2014), organisational employees should be information security conscious, in order to be able to make well-informed information security decisions while performing their roles and responsibilities. These authors further state that this can be achieved through educating employees with regards to the information security threats within their area of work. Agreeably, Schneider (2013) indicates that, organisational employees who are educated are essential to the building of information systems that are secure.

Computing graduates, who in the context of this research are defined as graduates in the Computer Science (CS), Information Systems (IS) and Information Technology (IT) disciplines, upon graduating from higher education institutions, become organisational employees.

It can be argued, therefore, that, computing graduates are also required to possess adequate information security knowledge to perform their organisational roles and responsibilities in a secure manner. It is important that computing students are taught information security to enable them to build secure information systems (Conti, Hill, Lathrop, Alford, & Ragsdale, 2003).

The following section presents the problem area that this research aims to solve.

1.2. Problem Area

According to Futcher, Schroder and Von Solms (2010) and Talib, Khelifi and Ugurlu (2012), higher education institutions are responsible for producing computing graduates who possess the adequate information security understanding that could enable them to handle organisational information assets securely. Furthermore, the information security education of computing students should result in graduates who are prepared for the challenges they will encounter in their organisational roles and responsibilities (Irvine, Chin & Frincke, 1998).

For decades, the Association for Computing Machinery (ACM), the Association for Information Systems (AIS), the Association of Information Technology Professionals (AITP) and the Computer Society of the Institute for Electrical and Electronic Engineers (IEEE-CS), have been providing higher education institutions with computing curricular recommendations and guidelines for the development of educational material. Most South African higher education institutions offering CS, IS and IT qualifications rely on these guidelines for their curriculum development.

During the deliberations of the Special Interest Group for Information Technology Education (SIGITE) Curriculum Committee, several themes emerged that were considered essential. Furthermore, these essential themes did not seem to belong to a single specific knowledge area or unit and they were referred to as pervasive themes. One of these essential themes is Information Assurance and Security (IAS). IAS is unique in the collection of knowledge areas as it is defined as both a pervasive theme and knowledge area (ACM/IEEE - CS, 2008b, 2013; SIGITE Curriculum

Committee, 2005). Similarly, the ACM/IEEE - CS (2008b, 2013) provides recommendations and guidelines that indicate that, information security should be integrated into computing curricula as a pervasive theme. According to ACM/IEEE - CS (2008b, 2013) and SIGITE Curriculum Committee (2005), a pervasive theme should be addressed multiple times, in multiple modules and from a different perspective in each module.

Although IAS is defined as both a pervasive theme and knowledge area, Futcher and Van Niekerk (2011) and Perrone, Aburdene and Meng (2005) argue that at some higher education institutions, IAS may be overlooked until the fourth year of study. This is a concern, as the fourth year of study is not compulsory at all higher education institutions, meaning that students who do not proceed to this year of study may exit higher education institutions without being exposed to IAS. Although ACM/AIS/IEEE-CS have been providing curriculum guidelines for the development of educational materials and programmes for decades, Futcher and Van Niekerk (2011) argued that, even though these guidelines assist in the development of educational material and programmes, they do not provide enough guidance to computing educators on ***"how"*** they can pervasively integrate information security into their modules.

The problem, therefore, identified for this research is:

Currently, no generally used framework exists to aid the pervasive integration of information security into undergraduate computing curricula.

The research objectives identified to address this problem are provided in Section 1.3, while in Section 1.4, the research methods used are briefly introduced together with the manner in which they relate to the research objectives. In addition, this chapter discusses the ethical considerations in Section 1.5 and the delineation and limitations of this study are indicated in Section 1.6. The chapter layout is presented in Section 1.7, while Section 1.8 provides a list of publications related to this research study. Finally, the chapter is concluded in Section 1.9.

1.3. Research Objectives

The research objectives to address the identified problem stated in this research are outlined in this section.

In order to address the problem stated in Section 1.2, the **primary objective** of this research study is:

To develop a framework to aid the pervasive integration of information security into undergraduate computing curricula.

The **secondary objectives** identified to collectively achieve this primary objective include:

1. To develop an understanding of the importance of information security;
2. To determine the importance of information security education as it relates to undergraduate computing curricula; and
3. To determine computing educators' perspectives on information security education in a South African context.

Table 1.1, depicts the relation between the research objectives and the methods used to achieve each of the research objectives.

Research Objectives	Method(s) to be used
Primary Objective: To develop a framework to aid the pervasive integration of information security into undergraduate computing curricula	Argumentation Modelling Scenarios Elite Interviews (Questionnaire)
Secondary Objective 1: To develop an understanding of the importance of information security	Literature Review
Secondary Objective 2: To determine the importance of information security education as it relates to undergraduate computing graduates	Literature Review
Secondary Objective 3: To determine computing educators' perspectives on information security education in a South African context	Survey (Semi-structured Interviews)

Table 1.1: Research Objectives and Research Methods

The three secondary objectives depicted in Table 1.1 were used to meet the primary objective. The primary objective of this research study was met through a number of research methods, namely: Argumentation, modelling, scenarios and elite interviews supported by a questionnaire. Secondary objectives 1 and 2 were met using the literature reviews, while secondary objective 3 was met through the use of a survey that took the form of semi-structured interviews supported by a questionnaire. The following section discusses how these research methods relate to this research study.

1.4. Research Methods

This section discusses the research methods that were used to achieve this study’s’ research objectives.

1.4.1. Literature Review

A literature review is an evaluation of literature reports related to the selected research area. It is conducted through selecting literature that is in the same topic area. The literature should be described, summarised, evaluated and clarified according to the relationship it has with the particular area of research (Boote & Beile, 2005).

This research study consists of two literature review chapters. The first literature review chapter (*Chapter 3: Information Security*) aims to provide an understanding of information security. The second literature review chapter (*Chapter 4: Information Security within Higher Education*) provides the importance of information security education as it relates to undergraduate computing students.

1.4.2. Survey

Surveys are used when one seeks to elicit opinions, desires and attitudes from a number of people and these are related to a particular subject or topic that they are seeking information on. These people should be willing and able to communicate and relate these to the research (Bhattacherjee, 2012; Hofstee, 2006, p. 122). Hofstee (2006, p. 122) and Olivier (2009, p. 10), state that a survey can be conducted in the form of a questionnaire or an interview.

According to Saunders et al. (2012), interviews can be categorised as either structured, semi-structured, unstructured or in-depth interviews. When conducting a semi-structured interview, a researcher usually has a list of themes and possibly some key questions to be covered. The use of these questions can differ from interview to interview. This means that the researcher can omit some questions in certain interviews and the order in which the questions are asked can vary in accordance with the flow of the conversation. Using semi-structured interviews also provides the researcher with the opportunity to probe answers where the researcher wants the participant to explain or build on their previous response (Saunders et al., 2012, p. 374, p. 375).

This research made use of the survey method and was conducted in the form of semi-structured interviews, supported by a questionnaire to elicit the South African educators' opinions, desires and attitudes relating to information security.

The survey is specifically linked to Secondary Objective 3 of this research, which is ***to determine computing educators' perspectives on information security education in a South African context.***

In order to meet this secondary objective, four survey objectives were identified as outlined in Table 1.2.

Survey Objectives	
Survey Objective 1	To determine computing educators' perspectives on the integration of information security into undergraduate computing curricula
Survey Objective 2	To determine computing educators' perspectives on the current integration of information security into their curricula
Survey Objective 3	To determine which fundamental information security concepts should be integrated into undergraduate computing curricula as a pervasive theme
Survey Objective 4	To identify possible ideas and challenges for integrating information security concepts into computing curricula

Table 1.2: Survey Objectives

Each of the four survey objectives was supported by questions to ensure that they were met. The design of the questionnaire that was used in supporting the semi-structured interviews is discussed in Chapter 2, Section 2.5.

1.4.3. Argumentation

An argument is a set of assumptions from which conclusions can be drawn that can be obtained by one or more reasoning steps (Besnard & Hunter, 2008). It is formed by combining existing facts to derive new facts. The fact from which any conclusion is made is known as the premise of the argument. The conclusion often forms a premise for the argument to follow. Premises are acquired from facts reported elsewhere. These can be facts obtained from definitions, own observation, or from conclusions of previous arguments (Olivier, 2009, p. 105, p. 106).

This research argues that by pervasively integrating information security education into undergraduate computing curricula, computing students could become a stronger link in securing organisational information systems and their related information assets from potential threats. Furthermore, it argues towards a framework to aid the pervasive integration of information security into the undergraduate computing curricula.

1.4.4. Modelling

According to Tomhave (2005), a model is defined as an abstract or conceptual construct that represents processes, variables and relationships that do not provide specific guidance on how to be implemented.

Modelling techniques were used to develop a framework for integrating information security into undergraduate computing curricula.

1.4.5. Scenarios

A scenario can be defined as taking representative examples of the use of a system, as a basis for establishing requirements for a new design. Scenarios are often used as a means of assessing the consequences and possibilities of a design. The purpose of using scenarios is to demonstrate how a proposed design may be used (Pocock, Harrison, Wright, & Johnson, 2001).

A scenario was used to demonstrate how a computing department could implement the proposed information security education framework by contextualising the proposed framework.

1.4.6. Elite Interviews

The term “elite” is applied to a person or group of people that are generally considered important. Furthermore, the idea of elite involves the formation of identities in relation to concepts of professionals and professionalism and points at the power they have and that is associated with them. The “elite” can typically be seen to have knowledge, influence, control and power in a given setting or situation (Moore & Stokes, 2012). An elite interview, therefore, is interviewing an expert or elite person.

Elite interviews were conducted to validate the proposed framework. These elite interviews were conducted with a Director of School, Head of Department and Senior Lecturers. The elite interviews were supported by a questionnaire.

1.5. Ethical Considerations

Ethical clearance was not sought from the higher education institutions involved in the survey as the participants were not of a vulnerable group. Although some basic demographic information was collected, this information will not be published, thus ensuring that the participants remain anonymous in the reporting of the results and findings. Furthermore, the results of the research will not be damaging to the reputation of any parties that participated, and participation in the survey was entirely voluntary.

1.6. Delineation and Limitations of Study

According to Hofstee (2006, p. 87), it is important to set delineation and limitation boundaries of what the research study will investigate. This protects the researcher from criticism as to why they did not consider other relevant work in the research area.

The key focus of this research is within the South African context. This research focuses on the CS, IS and IT disciplines since these three computing qualifications are being offered at most South African higher education institutions. Cost and time constraints limited the researcher from reaching all South African higher education institutions offering CS, IS and IT as participants in the semi-structured interviews. However, seven higher education institutions were included in this study, all being universities.

1.7. Chapter Outline

This dissertation consists of eight chapters. The contents of these chapters are briefly discussed below.

Chapter 1 - Introduction

This chapter introduces this research study by providing the background literature of this research. It introduces the problem area and explicitly states the problem that this research aims to solve. It presents the research objectives of this research study that were used to meet the identified problem. In addition, it briefly introduces the research methods used in this research and how they relate to the research objectives. Furthermore, it discusses the ethical considerations, the delineation of this study, the chapter layout, the publications that are related to this research study and the conclusion of this chapter.

Chapter 2 – Research Design

This chapter provides a brief discussion of the research approach as well as the research techniques and procedures that were used in this study. It introduces the research methods that were used when conducting this research, as well as how each of the research methods relates to the objectives of this research study. This chapter also provides the design of the questionnaire that was used when conducting the survey.

Chapter 3 – Information Security

This chapter introduces, defines and provides an in-depth discussion relating to the domain in which this study is contained namely: *Information Security*. It provides the importance of protecting organisational information systems and related information assets. Furthermore, the multi-dimensions of information security which include the critical characteristics of information, the various information states and security measures are discussed. This chapter concludes by discussing information security within organisations.

Chapter 4 – Information Security within Higher Education

This chapter discusses the role that information security education within higher education can have on ensuring the protection of organisational information systems and related information assets from potential threats. This is achieved through an introduction and discussion of the role players that provide computing curricula guidelines and recommendations and through the discussion of computing graduate requirements. Furthermore, this chapter discusses the manner in which information security can be integrated into computing curricula and the related challenges in doing so. This chapter concludes with a discussion of the significant impact that the pervasive integration of information security could provide.

Chapter 5 – The Integration of Information Security into Computing Curricula: A South African Perspective

This chapter provides the results and findings pertaining to the survey undertaken to determine computing educators' perspectives on information security education in a South African context. Furthermore, it provides results and findings relating to the fundamental information security concepts that should be integrated into undergraduate computing curricula as a pervasive theme and the possible ideas and challenges for integrating information security concepts into computing curricula. Additionally, it provides a discussion of the key findings from the undertaken survey.

Chapter 6 – Information Security Education Framework

This chapter provides the proposed solution to the research problem stated in Chapter 1, Section 1.2. This solution is presented as a framework that can be implemented by higher education institution's computing departments and computing educators to pervasively integrate information security into their undergraduate computing curricula.

Chapter 7 – Validation of Information Security Education Framework

This chapter provides the validation of the framework proposed in Chapter 6. The framework is validated using elite interviews and is supported by a questionnaire.

Chapter 8 – Conclusion

This chapter draws conclusions based on the research presented in the preceding chapters. It specifically states how and where in the dissertation each of the primary and secondary research objectives were met.

1.8. Related Publications

This subsection presents the publications related to this research study.

Gomana, L., Futcher, L., & Thomson, K.-L. (2015). Integrating Information Security into the IT Undergraduate Curriculum : A Case Study. In E. Coleman (Ed.), 44 The Annual Southern African Computer Lecturers Association 2015 (SACLA 2015) (pp. 19–26). Johannesburg, South Africa (See Appendix A1).

Gomana, L., Futcher, L., & Thomson, K.-L. (2016). An Educators Perspective of Integrating Information Security into Undergraduate Computing Curricula. In N. Clarke & S. Furnell (Eds.), Proceedings of the Tenth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2016) (pp. 179–188). Frankfurt, Germany (See Appendix A2).

1.9. Conclusion

This chapter provided the literature background that this research study is based upon. Relating to the problem that was identified it is, therefore, important to further investigate the field in which this research study is contained in order to solve the identified problem.

To solve the identified problem, a systematic process should be followed. The systematic process followed when conducting this research study is presented in the following chapter.

Chapter 2 – Research Design

This chapter provides a brief discussion of the research approach as well as the research techniques and procedures used in this study. It introduces the research process that was used when conducting this research. Furthermore, it provides the design of the questionnaire that was used when conducting the survey discussed in Chapter 1, Subsection 1.4.2.

2.1. Introduction

To achieve the research objectives outlined in Chapter 1, Section 1.3, it is important to follow a systematic research process. According to Rajasekar, Philominathan and Chinnathambi (2006), following an appropriate systematic research process allows the researcher to correctly achieve the specified research objectives. Section 2.2 of this chapter discusses the deductive and inductive logical reasoning research approach. The inductive logical reasoning approach is discussed in relation to its applicability to this research study. Section 2.3 presents the research process that was followed when conducting this research, while the sampling and data collection techniques that were used are discussed in Subsection 2.4.1 and 2.4.2, respectively. Subsection 2.4.3 describes the participants of this survey. The manner in which this survey was conducted is discussed in the interview process in Subsection 2.4.4. The design of the questionnaire that was used when conducting the survey that took the form of semi-structured interviews is discussed in Section 2.5.

2.2. Research Approach

Table 2.1 depicts the comparison of the deductive and inductive logical reasoning research approaches according to Saunders, Lewis, & Thornhill (2012).

	Deductive Approach	Inductive Approach
Logic	In a deductive inference, when the premises are true, the conclusion must also be true	In an inductive inference, known premises are used to generate untested conclusions
Generalisability	Generalising from the general to the specific	Generalising from the specific to the general
Use of data	Data collected is used to evaluate propositions or hypotheses related to an existing theory	Data collected is used to explore a phenomenon, identify themes and patterns and locate these

		in a conceptual framework and test this through subsequent data collection and so forth
Theory	Theory falsification or verification	Theory generation and building

Table 2.1: A Comparison of the Deductive and Inductive Logical Reasoning Research Approaches (Saunders et al., 2012, p. 144)

A further comparison between the two research approaches presented in Table 2.1 is discussed in Subsections 2.2.1 and 2.2.2 below.

2.2.1. Deductive Reasoning

According to Saunders et al. (2012, p. 144), the deductive reasoning approach adopts the 'top-down' approach. This reasoning approach works from the general to the specific in the sense that it begins with a theory, which is often developed through conducting a literature review. A research strategy is then designed to test the accepted or rejected theory.

2.2.2. Inductive Reasoning

The inductive reasoning approach, on the other hand, adopts the 'bottom-up' approach. This approach starts by exploring a phenomenon from collected data to generate or build a theory, often in the form of a conceptual framework. Researchers using this reasoning approach often work with qualitative data and use a variety of methods to collect data in order to develop various phenomena (Saunders et al., 2012, p. 144, p. 145, p. 146, p. 147).

This research study uses the inductive reasoning approach. This was done by conducting a literature review to identify a problem in the information security field. From there, a primary objective and secondary research objectives were derived to address the identified problem. These primary and secondary research objectives are stated in Chapter 1, Section 1.3. Various methods were used to collect both primary and secondary data. Secondary data was obtained through literature reviews, while primary data was gathered by conducting a survey, which took the form of semi-structured interviews and these were supported by a questionnaire. Both qualitative and quantitative data was collected through the survey. From the literature reviewed and the data collected from the survey, a framework was built. The framework was validated using elite interviews, which were supported by a questionnaire.

2.3. Research Process

This section introduces and discusses the research process that this study followed in order to address the identified problem.

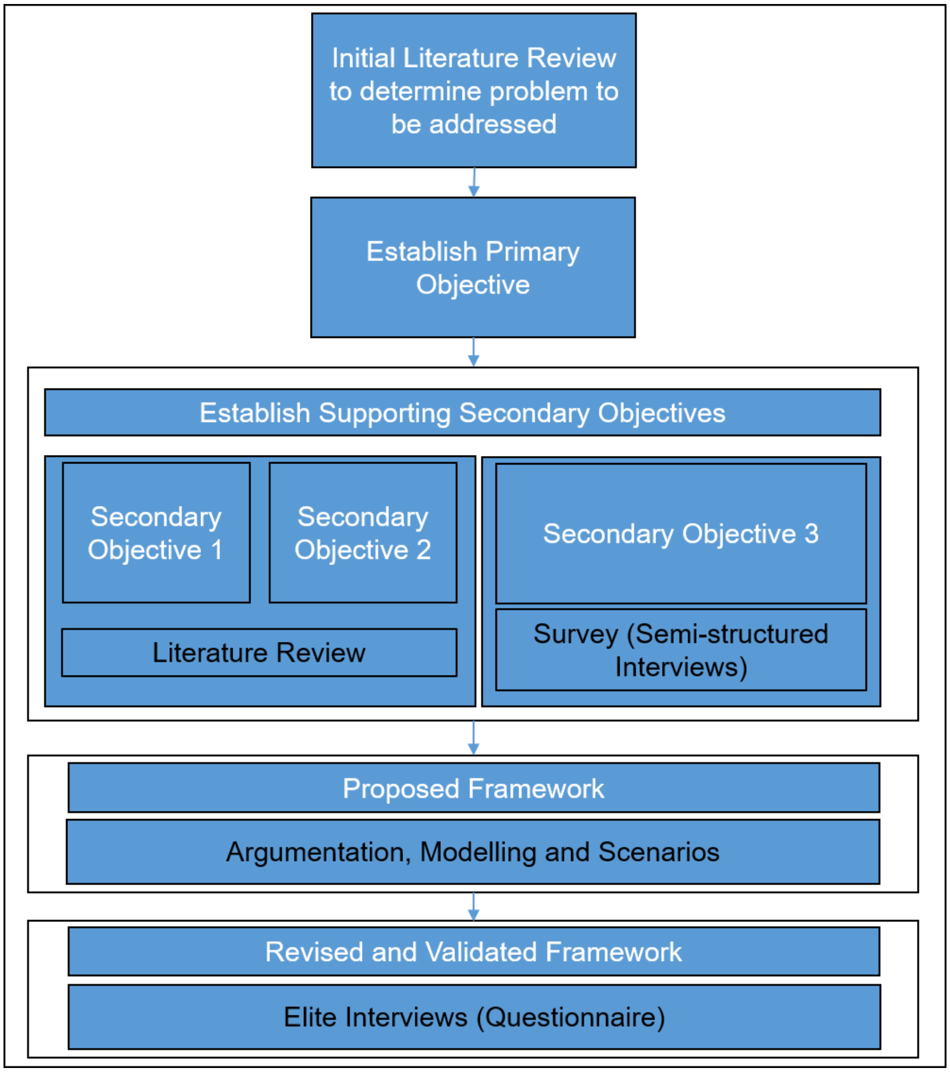
Initial Literature Review to determine problem to be addressed
Establish Primary Objective
Establish Supporting Secondary Objectives
Secondary Objective 1
Secondary Objective 2
Literature Review
Secondary Objective 3
Survey (Semi-structured Interviews)
Proposed Framework
Argumentation, Modelling and Scenarios
Revised and Validated Framework
Elite Interviews (Questionnaire)

Figure 2.1: Research Process

As depicted in Figure 2.1, an initial literature review was conducted to determine a relevant problem in the chosen field of study, namely information security education. The problem identified by this literature review is that ***"currently, no generally used framework exists to aid the pervasive integration of information security into undergraduate computing curricula"***. A primary objective was established together with the secondary objectives necessary to meet the primary objective.

The appropriate research methods to meet each of the secondary objectives were identified. In order to meet Secondary Objectives 1 and 2, literature reviews were conducted. Furthermore, a survey that took the form of semi-structured interviews supported by a questionnaire was conducted to meet Secondary Objective 3 as shown in Figure 2.1.

The framework was designed in three phases, namely: the initial framework design, the validation of the initial design of the framework and the design of the revised and validated framework.

Findings from the literature review and survey conducted were used to argue towards the initial design of the framework. This phase of the framework design was constructed using modelling techniques. Scenarios were used to show ***"how"*** the framework can be implemented by higher education institution's computing departments and computing educators. The second phase was to validate the initially proposed framework. This was done through conducting elite interviews, which were supported by a questionnaire. The third phase was to revise the validated framework based on the feedback provided. Findings from the elite interviews conducted were used to revise and validate the design of the initial framework.

2.4. Research Techniques and Procedures

This section discusses the sampling and data collection techniques and procedures used to conduct the survey discussed in Chapter 1, Subsection 1.4.2.

2.4.1. Sampling Techniques

Regardless of one's research questions or objectives, a researcher still needs to consider whether they will collect and analyse data from an entire population or from a select sample of the population. Collecting and analysing data from an entire population can occasionally be possible, but restrictions such as time, funding and access to the population, often make it impossible to do so. Sampling techniques allow the researcher to reduce the amount of data they need to collect by considering only the data from a subgroup rather than from an entire population. This is referred to as the case or elements (Marshall, 1996; Saunders et al., 2012, pg 258).

Figure 2.2, illustrates the differences between population, sample and case or elements. Saunders et al. (2012, p. 260) state that it is unnecessary to collect data from the entire population when a sample can be selected which represents the entire population.

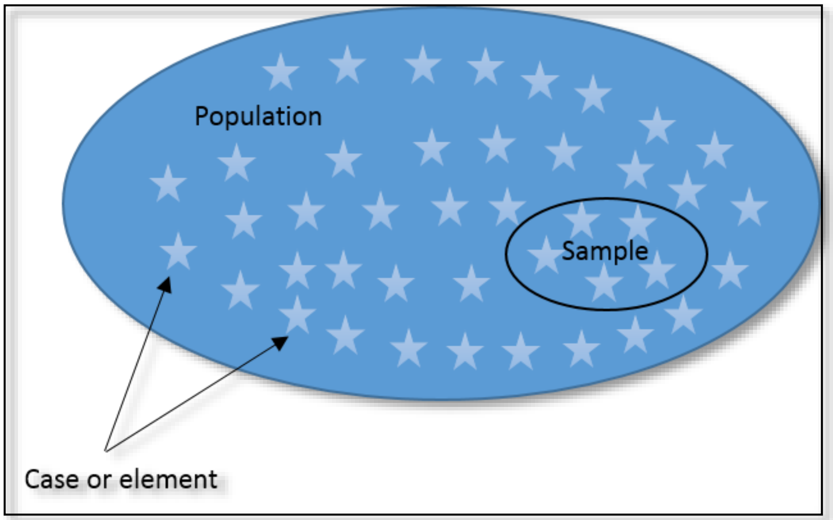

Figure 2.2: Population, Sample and Individual Cases (Saunders et al., 2012, p. 259)

Relating to the survey conducted for this research, selecting a sample proved a reasonable alternative to the entire set of cases or population for the following reasons:

- It was impractical to survey all computing educators at all South African higher education institutions;
- The availability of the entire population could not be guaranteed;
- Research funds were limited for travel; and
- Time constraints made surveying of the entire population unfeasible.

According to Saunders et al. (2012, p. 261), the sampling process consists of two types of sampling techniques, namely: Probability and non-probability sampling. Probability sampling is when the researcher selects a large number of participants that meet specific criteria from an existing and accurate sample. Non-probability sampling occurs when not all members of the population have a chance to participate in the study. The non-probability sampling process selects a few cases in various forms, such as people, places or objects, or when the researcher requires answers to questions that elicit the ‘how’ and ‘why’ questions (Bhattacherjee, 2012; Saunders et al., 2012, p. 262, p. 265, p. 266, p. 281, p. 283).

For the purpose of this research study, non-probability sampling was used as it was impractical to survey the entire population of all CS, IS and IT educators from higher education institutions in South Africa. This was influenced by both the lack of time and financial limitations.

Non-probability sampling includes but is not limited to several specific types of techniques, such as convenience sampling. Convenience sampling is involved with the selection of a sample in a haphazard manner relating to how easily available the sample is to obtain. Although convenience sampling is widely used, it is prone to influences and bias that are beyond the control of the researcher (Bhattacherjee, 2012; Marshall, 1996; Saunders et al., 2012, pg 291). However, according to Skowronek and Duerr (2009), if steps are taken to control uncertainty and bias, useful data can be generated by convenience sampling. This can be done by controlling and assessing the sample's representativeness**.** This can be achieved by attempting to obtain a miniature version of the entire population.

Relating to convenience sampling, this research controlled and assessed the sample's representativeness by inviting participation from all CS, IS and IT educators regardless of the modules they offer to their students and the year in which they offer the module.

2.4.2. Data Collection

According to Driscoll (2011), data collection techniques can either gather primary or secondary data. Primary data is gathered by the researcher first-hand by communicating with the subject that the data is being collected from, through observing the subject or by examining a phenomenon. The ultimate goal in conducting primary research is to learn something new that can be supported by other researchers and to eliminate the researchers own bias. Secondary data is derived through reviewing existing literature or other existing data sources (Driscoll, 2011).

Relating to this research, both primary and secondary data were used. Primary data was gathered through conducting a survey in the form of semi-structured interviews supported by a questionnaire. The survey aimed to determine the current integration of information security in higher education institutions in South Africa, with a specific focus on undergraduate computing qualifications and to determine computing educators' perspectives on information security education in a South African context. Secondary data was gathered through reviewing existing literature in the information security field, which this research is based. The aim of the literature review was to develop an understanding of the importance of information security and how it relates to undergraduate computing graduates in higher education institutions.

The data collection methods below are presented in relation to their applicability to this research.

2.4.3. Participants

The survey included 21 participants who were all educators in either the Computer Science (CS), Information Systems (IS) or Information Technology (IT) computing discipline. These participants were from seven higher education institutions in three provinces of South Africa, namely: The Eastern Cape, Gauteng and Western Cape. Four of the participants were Professors, two participants were Heads of Departments, 14 were Senior Lecturers and one participant was a Junior Lecturer. Participation in the study was voluntary.

2.4.4. Interview Process

A semi-structured face-to-face interview was conducted with each of the 21 participants. Interviews were only conducted with the participants who were available to be interviewed at the time of the visit to the higher education institution. The semi-structured interviews conducted were supported by a questionnaire (see Appendix B1). The researcher designed a questionnaire with standard questions to ask each of the participants in an interview. All questions were asked and the researcher sometimes probed for additional answers, based on the response provided by the participant. The flow of each interview was not the same and questions were asked depending on the direction the interview took. The questionnaire was structured according to the four survey objectives as shown in Chapter 1, Table 1.2 and the results and findings of the survey conducted are reported on in Chapter 5.

2.5. Questionnaire design

The following subsections present the questions that were used to meet each of the four survey objectives as shown in Chapter 1, Table 1.2.

Survey Objective 1

As depicted in Chapter 1, Table 1.2, survey objective 1 aimed ***to determine computing educators' perspectives on the integration of information security into undergraduate computing curricula****.* This survey objective was achieved through the questions depicted in Table 2.2.

Question 1	What is your perspective on the importance of information security education to undergraduate computing students?
Question 2	What is your perspective on the pervasive integration of information security into undergraduate computing curricula?

Question 3	What is the department/colleagues perspective on the pervasive integration of information security into undergraduate computing curricula?
Question 4	Has your department ever had a formal discussion regarding information security?

Table 2.2: Survey Objective 1 Questions

Questions 1, 2, 3 and 4: The aim of the questions in this section was to determine the participant's standing concerning information security in order to determine whether that would influence their willingness to integrate information security education pervasively into their module. The integration of information security into undergraduate computing curricula could ensure that institution can produce computing graduates with information security skills, knowledge and understanding to perform their roles and responsibilities securely within organisations.

Survey Objective 2

This survey objective aimed ***to determine computing educators' perspectives on the current integration of information security into their curricula***. This survey objective was achieved through the questions depicted in Table 2.3.

Question 5	Does the department have a security-related module that is taught to all undergraduate computing students?
Question 6a	Do you integrate information security into your module?
Question 6b	If Yes, do you assess information security within your module?

Table 2.3: Survey Objective 2 Questions

Questions 5, 6a and 6b: The questions within this subsection aimed to determine whether the department had a security-related module that is taught to all undergraduate computing students and whether the participants were currently integrating information security into their modules. These questions aimed to determine whether the department was producing any computing graduates who possess information security skills, knowledge and understanding.

For the computing educators who currently integrate information security into their modules, it is important to determine whether they assess information security within their module to see whether the students have acquired the information security knowledge that they have been taught.

Survey Objective 3

This survey objective aimed ***to determine which fundamental information security concepts should be integrated into undergraduate computing curricula as a pervasive theme***. Table 2.4 below, depicts the question that was asked to achieve this survey objective.

Question 7	What fundamental information security concepts do you think should be pervasively integrated into undergraduate computing curricula?

Table 2.4: Survey Objective 3 Question

This survey objective comprises of only one question. However, it was supported by a checklist of 23 information security concepts (see Appendix B2). When completing the checklist, the participants were encouraged to provide a brief comment as to why they thought the specific concept should or should not be regarded as a fundamental information security concept.

Question 7: The list of information security concepts that could be pervasively integrated into undergraduate computing curricula was derived from the following literature sources:

- '*Information Technology 2008, Curriculum Guidelines for Undergraduate Degree Programmes in Information Technology*' document (ACM/IEEE - CS, 2008b);
- '*Computer Science Curriculum 2013*' document (ACM/IEEE - CS, 2013);
- ISO Standards (ISO/IEC 7498-2, 1989); and
- Management of Information Security authored by (Whitman & Mattord, 2014).

The manner in which the 23 information security concepts were derived is discussed in Subsection 4.4.3. The aim of this survey objective was to determine which of the information security concepts should be regarded as fundamental in order to use them in a scenario to show computing educators ***"how"*** they can pervasively integrate the fundamental information security concepts into their modules.

Survey Objective 4

The aim of survey objective 4 was ***to identify possible ideas and challenges for integrating information security concepts into computing curricula***. This survey objective was met through the questions depicted in Table 2.5 below.

Question 8	Do you have any ideas on how to pervasively integrate information security concepts into various undergraduate computing modules?
Question 9	What challenges do you foresee in the pervasive integration of information security concepts into undergraduate computing curricula?
Question 10	Do you think computing educators would be able to pervasively integrate these fundamental information security concepts into their various modules?

Table 2.5: Survey Objective 4 Questions

Question 8: This question aimed to determine the ideas that the participants had that could be used to pervasively integrate information security into various undergraduate computing curriculum modules. These were to identify a few ideas that could ultimately be used by computing educators to pervasively integrate information security into their modules.

Question 9: Numerous authors including, Davis and Dark (2003); Futcher et al., (2010); Hentea, Dhillon and Dhillon (2006); Taylor and Azadegan (2008); Yang, (2001) have mentioned the challenges related to integrating information security into computing curricula. It is, therefore, important to identify the challenges that computing educators are faced with in their various higher education institutions and respective departments that could prevent them from pervasively integrating information security into their modules.

Question 10: It was also necessary to determine whether the participants think that other computing educators would be able to integrate the fundamental information security concepts into their modules. This was to determine their perspectives regarding other computing educators.

2.6. Conclusion

This chapter presented the research approach that was used when conducting this study. The research process was presented, the research techniques and procedures that were used were defined and a design of the questionnaire was presented.

The following chapter provides the findings from the literature review which aimed to introduce information security as the domain in which this research is contained.

Chapter 3 – Information Security

The aim of this chapter is to provide an overview of information security. It specifically highlights its significance in relation to computing graduates and their potential roles and responsibilities within organisations. It defines and discusses information security and its multi-dimensions and concludes by discussing information security within organisations.

3.1. Introduction

Information is an important and valuable asset in organisations and in our everyday lives. Information has, in fact, become the lifeblood of various organisations and it is core to the well-being of any modern-day organisation. Organisations of all types and sizes collect, store, transmit and process information. An information asset can be defined, therefore, as knowledge or information, that has value to an organisation, regardless of its form. These assets can include but are not limited to personal information, financial information, employee information and customer contact details (ISO/IEC 27000, 2012; ISO/IEC 27001, 2013; Landoll, 2006, p. 30; Safa, Von Solms & Futcher, 2016; Von Solms & Thomson, 2002; Von Solms & Von Solms, 2006).

Owing to their value, information assets are subject to various threats, whether accidental, intentional, internal, external, or natural. Regardless of the means by which the information is transmitted, it should always be appropriately protected. It is essential for information assets to be protected by effectively defining, achieving, maintaining and improving information security (ISO/IEC 27000, 2012; ISO/IEC 27002, 2013; ISO/IEC 27005, 2011).

Section 3.2 defines and discusses various threats and the related threat agents that could cause such threats to occur, while Section 3.3 provides a definition of information security and the critical characteristics of information. Section 3.4 provides the multi-dimensions of information security and discusses the security measures that can be used or put in place to protect information systems and the related information assets. Section 3.5 presents information security within organisations and Section 3.6 concludes this chapter.

3.2. Threats to Information Assets

According to Von Solms and Von Solms (2009), one of the biggest challenges is ensuring that an organisation’s information assets are protected from threats which can result in huge risks (Von

Solms & Von Solms, 2009, p. vii). In most, if not all organisations, information is captured, stored, processed, and transmitted using information systems. These information systems are continuously exposed to a wide variety of threats which can compromise the critical characteristics of the information. Threats are defined as undesirable events that can inflict damage to an organisation's IT systems and related information assets, resulting in significant loss, damage to an organisation's reputation and undue interruption of business activities. The related processes, systems, networks and people that use and access this information have inherent weaknesses, which could be exploited by these threats. These weaknesses are often referred to as vulnerabilities (ISO/IEC 27000, 2012; ISO/IEC 27002, 2013; NIST SP 800-30, 2002; Von Solms & Von Solms, 2009, p. vii).

Table 3.1 provides a list of typical threats that exist, categorised according to their threat type. Within each threat type, threats are grouped alphabetically and not according to priority. For each threat, its origin is indicated. 'D' indicates all threats where deliberate actions are aimed at information assets, 'A' is used for all human actions that can accidentally cause damage to information assets and 'E' depicts all the threats which are based on environmental (natural) origins (ISO/IEC 27005, 2011).

Threats Type	Threats	Origin of threat
Compromise of Information	Disclosure	A, D
	Remote spying	D
	Tampering of hardware	D
	Tampering of software	A, D
	Theft of equipment	D
	Theft of media or documents	D
Compromise of Functions	Abuse of rights	A, D
	Breach of personnel availability	A, D, E
	Denial of actions	D
	Error in use	A
	Forging of rights	D
Natural events	Climatic phenomenon	E
	Seismic phenomenon	E
	Volcanic phenomenon	E
	Meteorological phenomenon	E
	Flood phenomenon	E
Technical Failures	Breach of information security maintenance	A, D
	Equipment failure	A

	Equipment malfunction	A
	Software malfunction	A
	Saturation of information system	A, D
Unauthorised Actions	Corruption of data	D
	Illegal processing of data	D

Table 3.1: Examples of Typical Threats (adapted from (ISO/IEC 27005, 2011))

A threat is linked to a threat agent that causes it to occur. Numerous threat agents exist. These threat agents include but are not limited to nature, malicious hackers and organisational employees (Landoll, 2006, p. 31, p. 32).

All organisations entrust their employees to perform their roles and responsibilities accurately, consistently and honestly within the organisational policies. Furthermore, employees are the key to providing an appropriate and adequate level of information security. However, this is not always the case as employees may make errors in data entry, programming errors, release proprietary information, or decide to defraud the organisation (Landoll, 2006, p. 32). This has resulted in employees being cited by numerous authors such as Amankwa et al. (2014); Deloitte (2009); Kabay (2002) and Thomason (2013) as the “weakest link” in the attempt to protect organisational information systems and the related information assets. Similarly, NIST SP800-12 (1995) stated that, employees are the “weakest link” because they are capable of making mistakes and being wrong. In essence, employees are one of the biggest threats to an organisation’s information security, and they are the closest threat agent to information systems (Deloitte, 2009; ISO/IEC 27005, 2011; Kabay, 2002).

Whitman and Mattord (2014) argue that employees will remain the “weakest link” unless security measures (education, training and awareness; policy; and technology) are used properly to prevent employees from intentionally and accidentally causing harm to organisational information assets (Whitman & Mattord, 2014). In addition, NIST SP800-12 (1995) argues that information security education, training and awareness will enhance employees’ information security skills and the in-depth knowledge that is needed to protect information systems. Furthermore, it will also enable them to perform their jobs in a secure manner, including designing, implementing or operating organisational information systems in a secure manner. These security measures will be discussed further in Subsection 3.4.3.

Particular attention should, therefore, be given to human threats. These human threats include outsider and insider threat agents. Outsider threat agents could include hackers and crackers, terrorists, computer criminals, amongst many others. Insider threat agents include poorly trained, disgruntled, malicious, negligent, dishonest, or terminated employees. These human threat agents are driven by various motivations (ISO/IEC 27005, 2011).

Human threat agent	Motivation	Possible consequences
Hacker, cracker	Challenge, ego, rebellion, status, money	Hacking, social engineering, system intrusion, break-ins, unauthorised system access
Computer criminal	Destruction of information, illegal information disclosure, monetary gain, unauthorised data alteration	Computer crime (e.g. cyber stalking), fraudulent act (e.g. replay, impersonation, interception), information bribery, spoofing, system intrusion
Insiders	Curiosity, ego, intelligence, monetary gain, revenge, unintentional errors and omissions (e.g. data entry error, programming error)	Computer abuse, fraud and theft, information bribery, input of falsified, corrupted data, interception, malicious code (e.g. virus, logic bomb, Trojan horse), sale of personal information, system bugs, system intrusion, system sabotage, unauthorised system access

Table 3.2: Human Threat Agent Motivation and Possible Consequences (ISO/IEC 27005, 2011)

Table 3.2 illustrates human threat agents, the motivation that drives them, as well as the possible consequences of their actions towards the organisation. All of these threats and threat agents impact the organisation negatively and cause critical harm to the organisation's information systems and related information assets (ISO/IEC 27005, 2011; Landoll, 2006, p. 31, p. 32).

The following section introduces information security as the discipline used to ensure the protection of information assets from potential threats.

3.3. What is Information Security?

In order to fully understand the term *'information security,'* one needs to be able to understand the individual terms, namely '*information'* and '*security'*.

There is a distinct difference between information and data. This has resulted in many people having difficulty in understanding the difference between these two terms. Some people even go as far as using these terms interchangeably (O'Brien, 2002, p. 13). However, data can simply be defined as raw information, it has no significance beyond its existence, it simply exists. Information, on the other hand, is data that has been collected and processed, thus giving the data meaning, usefulness, relevance and purpose (Ackoff, 1989; Bellinger, Castro, & Mills, 2004; Drucker, 1988). These attributes are given to data by humans to transform the data into useful information (Davenport & Prusak, 1997, p. 9).

Organisations reap numerous benefits from information including providing them with a competitive edge over their competitors, allowing for financial prosperity and real-time reporting (Posthumus et al., 2010). However, the increase of threats to an organisation's information assets has led to a greater appreciation for a strong information security capability within an organisation (Landoll, 2006, p. 194).

The general definition of security, as defined by Whitman and Mattord (2014, p. 3), is, "*the quality or state of being secure – to be free from danger*". Security is the protection from the risk of loss, damage, or unwanted modification or other hazards. Furthermore, it is the protection of assets from those that seek to misuse it (Andress, 2014, p. 3). This means protecting assets from potential threats.

Having established an understanding of the terms '*information'* and *'security'*, an understanding of the term *'information security'* follows. For instance, Michalson (2003) defines information security as the umbrella concept that includes information assets as well as information systems (Michalson, 2003). These information systems can be defined as the organisational combination of people, hardware, software, communication networks and data resources, that are used for the collection, storage, transmission and processing of organisational information (Clinch, 2009; ISO/IEC 27000, 2012; NIST SP800-100, 2006; O'Brien, 2002; Whitman & Mattord, 2014, p. 4). Volonino and Robinson (2004) further define information security as incorporating policies, practices and technology that must be in place for organisations to ensure the secure transaction of business over the networks. This security also includes the security of individuals and other organisations that might be at risk in the event that a security breach occurs (Volonino & Robinson, 2004).

Various other authors define information security as the active protection of information assets and information systems from threats, which can compromise their critical characteristics (Andress, 2014, p. 3; Clinch, 2009; ISO/IEC 27000, 2012; NIST SP800-100, 2006; Tipton & Krause, 2008,

p. 16; Whitman & Mattord, 2014, p. 4). These critical characteristics include confidentiality, integrity and availability as discussed in Subsection 3.4.1.

The following section presents the comprehensive nature of information security as being multi-dimensional, using McCumber's model (2005). The first and second dimensions of the model re-enforce that the critical characteristics of information should always be maintained whether in the transmission, storage, or processing state. The third dimension introduces the various security measures that must be employed in order to ensure the security of information systems and related information assets.

3.4. Multi-dimensions of Information Security

McCumber's model (2005) as presented in Figure 3.1 is a three-dimensional representation of information security. It includes the three critical characteristics of information (confidentiality, integrity, and availability) as the first dimension; information states (transmission, storage, and processing) as the second dimension; and security measures (human factors, policy and practices, and technology) as the third dimension.

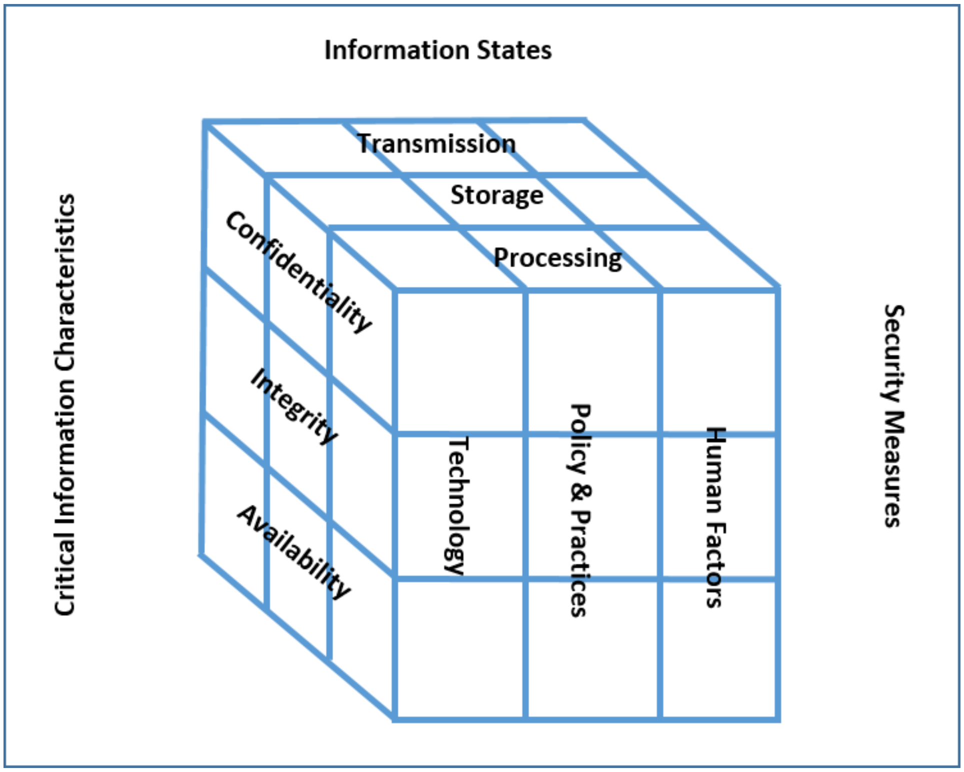

Figure 3.1: McCumber’s Model (McCumber, 2005)

From studying the literature on the McCumber model (2005), it is clear that the human factors dimension incorporates education, training and awareness.

The three dimensions of the model as illustrated in Figure 3.1, are namely: The critical information characteristics, information states and security measures, which are discussed in Subsections 3.4.1, 3.4.2 and 3.4.3, respectively.

3.4.1. Critical Characteristics of Information

In order to fully comprehend information security, one needs to understand the critical characteristics of information that should be maintained in order to ensure the protection of information systems and related information assets. These critical characteristics include confidentiality, integrity and availability and are described as follows:

- *Confidentiality* refers to protecting information from those who do not have sufficient privilege and a demonstrated need to gain access to the information;
- *Integrity* refers to the quality or the state of being untampered and complete. It ensures that information is not changed or modified in storage or transmission in an unauthorised or undesirable manner; and
- *Availability* refers to having access to information in a usable format, without interference or obstruction by an authorised entity (Andress, 2014, p. 6, p. 7; Clinch, 2009; Whitman & Mattord, 2014, p. 6, p. 7).

In the present day, there has been a need for more characteristics, as these three critical characteristics of information alone are inadequate. This is due to the fact that they are limited in scope and cannot encompass the constantly changing environment of the computing industry, which needs a more robust model. The critical characteristics have thus been expanded into a more comprehensive list of critical concepts and processes including privacy, identification, authentication, authorisation, accountability, non-repudiation and reliability (ISO/IEC 27000, 2012; Whitman & Mattord, 2014, p. 6). These are defined as follows:

- *Privacy* refers to the use of information solely for the purpose indicated by the owner of the information. Confidentiality and privacy are often regarded as similar. Although these concepts are closely related, they are not the same;
- *Identification* refers to an information system’s ability to recognise individual users. It is the

first step to gaining access to protected information. A user in this context refers to a person or computer. Identification serves as the foundation for authentication and authorisation;

- *Authentication* occurs when a user can prove that they possess the identity that they claim;
- *Authorisation* is a process whereby a user has been properly authorised to access, alter, or remove the contents of an information asset;
- *Accountability* refers to the assurance that any activity undertaken by a user can be attributed to that user;
- *Non-repudiation* refers to ensuring the occurrence of a claimed event or action and its originating entities can be proven; and
- *Reliability* refers to the property of consistent intended behaviour and results (ISO/IEC 27000, 2012; Whitman & Mattord, 2014, p. 6, p. 7).

It can, therefore, be concluded that a person or organisation will suffer harm if the critical characteristics of their information assets are compromised by potential threats.

McCumber's model (2005) re-enforces that the critical characteristics of information should be maintained regardless of the state of the information.

3.4.2. Information States

As illustrated in Figure 3.1, information has three basic states, namely, transmission, storage and processing. This information is transmitted by, stored within and processed by information systems (McCumber, 2005; NIST SP 800-30, 2002). These basics states of information are defined by Advanced Software Products Group Inc (2016) as follows:

Transmission State

The transmission state refers to information that is moving or travelling from a source to a destination. For example, information contained in an email or file that is moving across a cable and wireless transmission to a source. It is important for this information to be encrypted so that it cannot be manipulated or read by a machine or hacker while it is in the state of being transmitted from the source to the destination.

Storage State

The storage state refers to information that is at rest. This means that this information is not travelling between source and destination, it is not active, being read or being processed by any application. This information is simply stored on a device or on any form of backup medium.

Processing State

The processing state refers to information that is actively being generated, updated, changed or being erased. This information can be processed by one or more applications. In addition, this state also refers to information that is being accessed and viewed by users from various endpoints.

According to the Advanced Software Products Group Inc (2016), understanding the various states in which information resides can assist with selecting the appropriate security measure for protecting the information from various threats that can potentially cause harm to the information.

The third dimension, which is security measures is used to ensure that the critical characteristics of information are maintained while it is stored, processed or transmitted between information states (McCumber, 2005). Regardless of the state information is in, it should always be protected. The protection thereof is achieved through the implementation of the security measures dimension. The following section introduces the security measures dimension and provides a detailed discussion of the three layers of the dimension, namely: Technology; policies and practices and human factors.

3.4.3. Security Measures

According to Safa et al. (2016), various security measures play a crucial role in the protection of organisational information systems. These security measures include technological measures, organisational measures (policies and practices) and human factors (education, training and awareness) (Safa et al., 2016).

This subsection introduces the third dimension of McCumber’s model, security measures. The three layers of the dimension are discussed to provide an understanding of the individual layers of the security measures dimension. Furthermore, the relevance of information security education to this research is highlighted.

Technological Measures

The first layer of the security measures dimension is technology. Technology is defined as any physical device or technique that can be implemented in a physical form specifically to ensure that the critical characteristics of information are maintained to achieve the security of information systems and related information assets in any of the information states. This technology can be implemented in hardware, software, or firmware (McCumber, 2005; Venter & Eloff, 2003). Examples of technological security measures include biometrics, digital signatures, firewalls, intrusion detection systems, anti-virus packages, amongst many others (Venter & Eloff, 2003). However, employees could make configuration errors, leave network ports open, leave firewalls vulnerable and systems unprotected (Hinson, 2003). This could lead to vulnerabilities that can be exploited by those seeking to cause harm to the organisation through these information systems.

Hinson (2003) states that there are a number of drawbacks to a pure technological security measure approach, including:

- Technological security measures are unreliable as hackers could find backdoors, unchecked buffers and unexpected exceptions;
- Very few organisations understand their information security problems enough to specify the appropriate technological security measures;
- Technological security measures require significant financial resources; and
- A human has to develop, implement and maintain the technological security measures (Hinson, 2003).

Although some organisations can afford to implement these technological security measures, they still experience security breaches. This is attributed to information security being primarily a human issue and not solely a technological one. Although a number of these technologies are designed to function without human interference, these technological security measures are still designed to be used and managed by humans (Lacey, 2009; Schultz, 2005). According to Schultz (2005), this human interference with the technology leaves ample opportunity for human errors that can have detrimental results. Hinson (2003) argues that it is, therefore, important to invest in the human aspect in as much as one invests in technology. This is due to the fact that the use of technology on its own cannot protect organisations against potential information security threats. Various researchers, such as Hinson, (2003); Lacey, (2009); and Yngström and Bjorck, (1999) have argued that the most significant determinant of the overall success of information security within an organisation is the human factor. However, according to McCumber (2005), enforcing a policy can assist immeasurably in protecting information as it does not make sense to wait for technology to solve a problem that is not solely a technological one. The following subsection, therefore, discusses organisational measures, which encompass policies and practices.

Organisational Measures

The second layer of the security measures dimension is that of organisational measures, this dimension incorporates organisational policies and practices.

Policy is defined as the overall intention and direction as formally expressed by management to direct and control an organisation. Company procedure is defined as the way in which an activity or a process is carried out within an organisation. Examples of policies may include but are not limited to the acceptable use of assets, information transfer and protection from malware (ISO/IEC 27000, 2012).

ISO/IEC 27002 (2013) states that information security policies should be communicated to all organisational employees in a form that is relevant, accessible and understandable, such as through information security education, training and awareness programmes (ISO/IEC 27002, 2013). According to McCumber (2005), technology and policy security measures rely heavily on the education, training, and awareness of employees. As employees are often the "weakest link", it can be argued that the protection of information systems and information assets through the implementation of technological and organisational (policies and practices) security measures alone may be hindered by these employees if they are not information security educated, trained and aware.

The following subsection discusses and compares information security education, training and awareness.

Human Factors

The third layer of the security measures dimension of McCumber's model is that of the human factor. As stated earlier, the human factor incorporates education, training and awareness. According to McCumber (2005), this dimension may be the most important security measure as it is only by ensuring that employees understand the threats and vulnerabilities associated with the increasing use of information systems, that organisations can begin to attempt to deal effectively with security measures, such as, technological and organisational security measures that were discussed in Subsections 3.4.3.1 and 3.4.3.2, respectively.

Table 3.3 highlights and compares the differences between information security awareness, training and education programmes in terms of the attributes, level, learning objectives, purpose, method of delivery, test measure and the impact time-frame.

Framework	Awareness	Training	Education
Attribute	'What'	'How'	'Why'
Level	Information	Knowledge	Insight
Learning Objective	Recognition and retention	Skills and knowledge	Understanding
Purpose	Ensure that every employee is aware of their role and responsibility towards protecting the organisation's information	Equip employees with information security skills and knowledge specific to their roles and responsibilities within organisations	Equip employees with the skills and ability needed to ensure the Confidentiality, Integrity, Availability (CIA) of organisational information.
Method of delivery	Media • Videos • Newsletters • Posters	Practical Instruction • Lectures • Workshops • Hands-on Practice	Theoretical Instruction • Seminars • Literature Study
Test Measure	Identify learning	Apply learning	Interpret learning
Impact Time-frame	Short-term	Medium-term	Long-term

Table 3.3: Comparative Framework of Information Security Awareness, Training and Education (adapted from (Amankwa, Loock, & Kritzinger, 2014; NIST SP800-12, 1995; Von Solms & Von Solms, 2009, p. 116)

According to NIST SP800-50 (2003) and Katsikas (2000), in terms of knowledge, learning is a continuum that consists of three levels. It starts with awareness, builds to training and evolves into education. These levels of learning increase in comprehension and detail as one moves from awareness towards education. Thus, this discussion begins by presenting information security awareness, this is followed by information security training and the discussion concludes with information security education.

Amankwa, Loock and Kritzinger (2014); Von Solms and Von Solms (2009, p. 116) state that from an organisational perspective, the differences between information security awareness, training and education need to be clear in order to identify the focus of each of these programmes. Identifying the focus of each of these information security programmes could assist in the identification of the appropriate information security programme that can be implemented by an organisation to ensure the security of organisational information systems and the related information assets.

Information security awareness is defined as the attempt to focus employees' attention on information security in order to ensure that they are all aware of their roles and responsibilities in securing organisational information assets. This can be done through the use of methods of delivery, such as videos, newsletters, posters and information security days (Amankwa et al., 2014; ISO/IEC 27002, 2013). An awareness programme should be in line with the organisation's policies and relevant procedures (ISO/IEC 27002, 2013). According to Von Solms and Von Solms (2009), an information security awareness programme only addresses the *"what"* aspect of information security. This is to improve employees' awareness of the importance of information and the need to protect organisational information assets (Von Solms & Von Solms, 2009, p. 116). This is done by reminding employees about basic security practices such as logging off a computer or locking doors (NIST SP800-12, 1995). This only highlights the importance of information assets and addresses the need to protect information assets. This, therefore, means that an information security awareness programme is not enough to ensure the protection of organisational information assets and the information systems that house these assets. Furthermore, awareness programmes do not provide organisational employees with the skills, knowledge and understanding needed to ensure the efficient and effective protection of information systems and related information assets.

Furthermore, information security awareness only provides short-term impact and will not educate employees on how to remediate the habits they may have towards the protection of information systems. This will, therefore, not provide organisational employees with the knowledge, skills and understanding required to design, develop, maintain and implement information systems that protect organisational information systems and related information assets from potential threats.

The skills that employees acquire during training programmes are those built upon the awareness programme foundation. The purpose of information security training is to provide employees with the relevant and necessary information security skills and knowledge on *"how"'* to securely perform their roles and responsibilities within the organisation (NIST SP800-100, 2006; NIST SP800-12, 1995; NIST SP800-50, 2003; Von Solms & Von Solms, 2009, p. 116). Training can thus be defined as any endeavour undertaken to ensure that all employees are equipped with information security knowledge and skills that are specific to their roles and responsibilities within the organisation by using practical instructional methods such as lectures, workshops and hands-on practice (Amankwa et al., 2014; NIST SP800-12, 1995).

According to Whitman and Mattord (2010), training can be seen in two different ways. The first type of training should be aimed at all employees. However, the more closely the training is designed to match the roles and responsibilities of a specific employee, the more effective it will be. This type of training also includes showing the employee how to perform certain tasks, as opposed to only what they should and should not do. The second type of training should be aimed at employees whose aim it is to become information security professionals within the organisation. This training is, more often, too technical for the average employee. Employees who want to become information security professionals could attend industry training which is offered through various professional agencies. These agencies include the Global Information Assurance Certification (GIAC), Security Certified Program (SCP), Information Systems Security Certification Consortium (ISC^2), Information Systems Security Association (ISSA) and the Computer Security Institute (CSI), amongst many others (Whitman & Mattord, 2010, p. 193).

The purpose of information security education is to produce information security specialists and professionals who are capable of proactive response (NIST SP800-100, 2006). It can be argued that this proactive response is to ensure the protection of information systems and related information assets from possible threats, as the occurrence could cause harm to the organisation’s reputation and result in the loss of financial resources.

Information security education can be defined as the attempt to provide insight and understanding of information security documents to ensure that all employees are equipped with the essential information security skills, knowledge and understanding to protect the organisation’s information by using academic instructional methods. It is important to ensure that these employees have the insight to and an understanding of *“why”* the protection of organisational information assets is essential (Amankwa et al., 2014; Von Solms & Von Solms, 2009, p. 116).

Education integrates all the security skills and knowledge of the various functional specialities into a common body of knowledge. The functional specialities are listed and explained as follows:

- **Manage** – For the employees that manage IT-based functions within the organisation;
- **Acquire** – For those employees who are involved in the acquisition of IT products and/or services;

- **Design and develop** – For the employees who design and develop organisational systems and applications;
- **Operate** – For those employees who administer IT systems within the organisation (e.g. web servers, email servers, file servers, local area network, wide area network, mainframe);
- **Review and evaluate** – For those employees who review or evaluate (audit) the IT functions of an organisation as part of the internal controls program or an external audit program (e.g. inspector general); and
- **Use –** for those employees who access and use IT resources and IT to do their jobs (NIST SP800-16, 1998).

Information security education is obtained through a qualification that is offered at a higher education institution (NIST SP800-12, 1995; NIST SP800-16, 2013; NIST SP800-50, 2003).

According to NIST SP800-12 (1995), there are major cost considerations and time constraints to implementing awareness, training and education programmes within organisations. These cost considerations and time constraints may include:

- The cost to prepare and update the awareness, training and education programme material;
- The cost of those providing the programmes;
- Employees time attending the awareness, training and education programmes or watching videos; and
- The cost of outside programmes and consultants (both of which can include travel costs).

Although the implementation of information security awareness, training and education programmes could have a positive impact on organisations, it might not be feasible for those organisations that cannot afford to implement them due to financial constraints. Financial resources would be required for the cost considerations listed above. The implementation of these programmes by organisations will also require time where these employees will be educated, trained and made aware of how to secure organisational information systems. Owing to the time constraints and cost considerations, it can be argued that, the implementation of awareness, training and education programmes within organisations means that employees may not have enough time to be taught how to adequately secure organisational information systems and their related information assets. This is because as organisational employees they will be required to go back to perform their roles and responsibilities within organisations. Furthermore, these employees may not possess the skills, knowledge and understanding to perform their organisational roles and responsibilities in a secure manner from the first day they are employed by the organisation. This could lead to them becoming the “weakest link” within their organisation. It can be argued that relevant information security education obtained at a higher education institution could ensure that computing graduates become a stronger link in securing organisational information systems and related information assets.

The focus of this research is, therefore, on information security education as it applies to computing students since once graduated they typically work closely with organisational information systems and information assets as organisational employees. Information security education within higher education institutions could provide these computing graduates with the information security skills, knowledge and understanding to ensure the protection of the information systems and information assets they work with from the first day as organisational employees.

The following section discusses the various levels of organisational employees who are responsible for the protection of the organisation’s information systems and information assets.

3.5. Information Security within Organisations

This section discusses the responsibility of information security within an organisation from the strategic level to the operational level where the actual day-to-day operations of protecting organisational information systems and related information assets are conducted. This section also discusses where computing graduates typically fit into an organisation as employees graduating from higher education institution.

The board of directors and executive management of an organisation are responsible for the overall well-being of the organisation (King, 2009; Von Solms & Von Solms, 2009). However, Whitman and Mattord (2014) state that everybody who comes into contact with sensitive, valuable, and critical information is required to possess adequate information security knowledge to ensure the well-being of the organisation, through the appropriate protection of information assets (Whitman & Mattord, 2014, p. xxv). Although the board of directors and executive management are responsible for the corporate governance of information security within the organisation, organisational employees also have a responsibility towards securing organisational information assets. This means that all three levels of management should play an active and critical role in the protection of organisational information assets (Von Solms & Von Solms, 2009). It can, therefore, be argued that computing graduates entering organisations as employees graduating from a higher education institution have a responsibility towards securing organisational information systems and the information assets housed within these systems.

Figure 3.2 illustrates the direct control nature of corporate governance within an organisation. The diagram illustrates the division of organisational employees into three levels, namely:

- The board of directors and executive management at **strategic level**;
- Senior and middle management at **tactical level**; and
- Lower management and administration at the **operational level**.

In terms of this research, it is important to highlight that computing graduates typically enter organisations at the operational level. These graduates are responsible for the design and development of organisational information systems; the maintenance of these systems and implementing the technological controls that ensure the protection of the organisation's information assets from possible threats and threat agents.

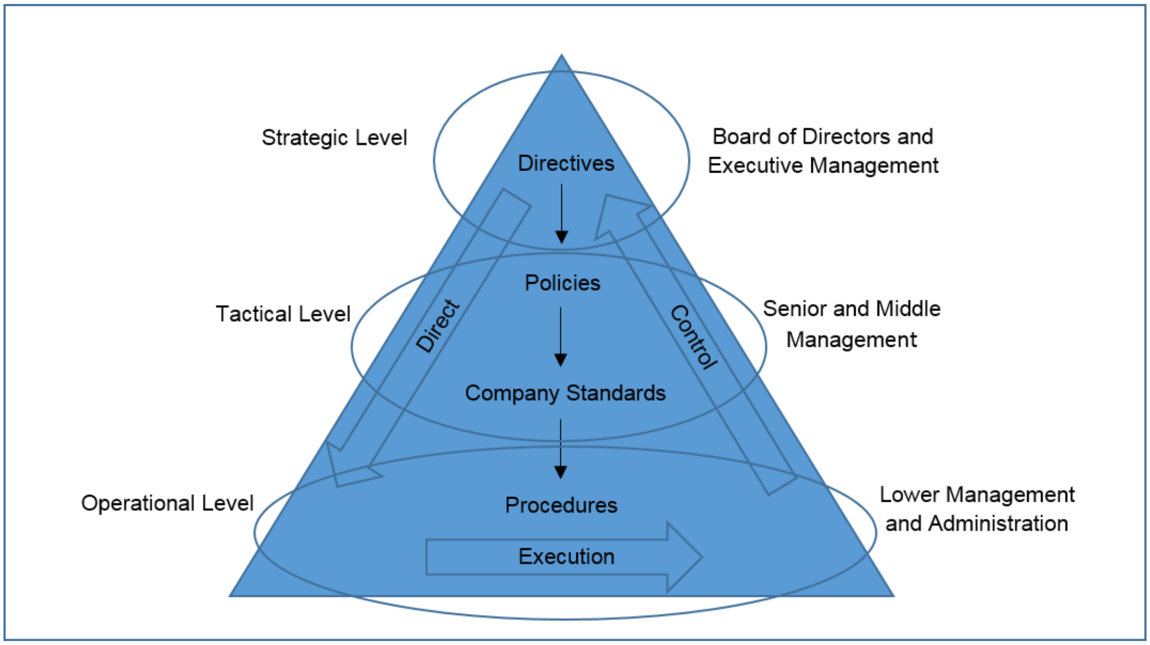

Figure 3.2: Corporate Governance - The Direct/Control Cycle and Core Model (Adapted from (Von Solms & Von Solms, 2009, p. 3, p. 35))

As illustrated in Figure 3.2, the directives mandating the objectives to be carried out by the organisation are issued by the board of directors and executive management. These directives are received by senior and middle management and are developed into policies and company standards. Furthermore, these policies and company standards are received by lower management and administration at the operational level where these policies and company procedures are implemented in the day-to-day operations of the organisation (Von Solms & Von Solms, 2009, p. 34, p. 35).

ISO/IEC 27002 (2013) states that these policies should be communicated to organisational employees by means of a regular and role specific information security education, training, and awareness programme. It is the organisation's responsibility to develop and update these programmes, to ensure that awareness, training and education are conducted effectively and that the programmes are in line with the organisation's current policies and practices (ISO/IEC 27002, 2013).

This research proposes for computing graduates to receive information security education at higher education level. This could ensure that the organisations that employ these graduates do not have to spend excessive time and financial resources designing, developing and implementing information security awareness, training and education programmes for these graduates. Furthermore, this could ensure that organisational information systems and information assets are appropriately protected by these computing graduates from the first day as organisational employees. These graduates could also champion various information security initiatives in the organisations that will employ them by influencing the security behaviour of other employees and by leading the organisation's information security awareness, training and education programmes.

3.6. Conclusion

This chapter highlights information as an important asset in the day-to-day running of business activities within an organisation. It discusses the critical characteristics of information and that information should be maintained in all information states. Furthermore, the security measures that should be employed by organisations in order to ensure the protection of information systems and related information assets are discussed.

It can be concluded that although information assets should be effectively protected by all levels of management within an organisation, computing graduates who become organisational employees at operational level upon graduating from higher education institutions, design, develop, maintain and implement controls that ensure the protection of organisational information systems and related information assets from potential threats. It should, therefore, be essential to ensure that computing graduates have the appropriate information security education to conduct their organisational roles and responsibilities securely. Failure to properly secure these information systems and related information assets could have a negative impact on the organisation thus leading to undue interruption of the business operations which could lead to financial loss.

The following chapter discusses and explores information security education as it relates to computing students at higher education institutions.

Chapter 4 – Information Security within Higher Education

This chapter examines the literature for the integration of information security into computing curricula. It introduces computing curricula guidelines and recommendations and also addresses the graduate requirements for the Computer Science, Information Systems and Information Technology disciplines. In addition, it presents various approaches and challenges for integrating information security into the curriculum.

4.1. Introduction

It is impossible to develop secure IT systems unless high-quality information security education is available to system developers (Yngström & Bjorck, 1999). Irvine, Chin, and Frincke (1998), state that the goal of information assurance and security is to ensure that the next generation of IT employees builds secure systems. This can be achieved by cultivating an appropriate knowledge of security, thereby increasing the likelihood that these IT employees will possess the appropriate security knowledge to design, develop and implement reliable and secure systems. From the onset, security should be considered during the design, development and implementation of these systems and not as an afterthought (Irvine et al., 1998).

Similarly, Futcher, Schroder and Von Solms (2010) state that, information security cannot be adequately dealt with without considering the people whose roles and responsibilities are to attain the goals of information security. It can, therefore, be argued that since it is the role and responsibility of computing graduates to ensure the security of organisational information systems, it is important to ensure that the higher education institutions that produce these graduates provide them with the necessary information security education. For higher education institutions to produce computing graduates with the necessary information security skills, knowledge and understanding that enables them to ensure the protection of organisational information systems and related information assets, it is important to ensure that information security education is taught to all undergraduate computing graduates.

Futcher and Van Niekerk (2013) state that South African higher education institutions do not get sufficient curricula guidelines to ensure that information security is included in the curriculum. These institutions, therefore, need to self-regulate through measuring against international norms and standards and by relying on curricula guidance from other relevant sources.

To determine guidelines for information security education in computing curricula, it is therefore, important to conduct a literature review of the key role players responsible for providing such guidance for computing curricula.

The following section, Section 4.2 provides an introduction of the various role players that have been providing computing curricula guidelines and recommendations over many decades. Section 4.3 provides computing graduate requirements for the Computer Science (CS), Information Systems (IS) and Information Technology (IT) computing disciplines. The way in which information security relates to the computing disciplines is discussed in Section 4.4, this discussion is divided into five subsections. The significant impact the pervasive integration of information security provides is discussed in Section 4.5, while Section 4.6 concludes this chapter.

4.2. Computing Curricular Role Players

Over the years, considerable attention has been given to the recommendation and guidance to computing education. Four major professional societies in the United States have developed computing curricula guidelines and recommendations for higher education institutions. These include the Association for Computing Machinery (ACM), the Association for Information Systems (AIS), the Association of Information Technology Professionals (AITP) and the Computer Society of the Institute for Electrical and Electronic Engineers (IEEE-CS). According to Dodge (2013) these aforementioned key role players are a community effort with representation from academia and industry. Furthermore, he states that the computing curricula recommendation documents published by these key role players are fully reviewed, revised and enhanced every ten years, with a minor interim assessment at the fifth year mark.

South African higher education institutions that offer CS, IS and IT qualifications rely on the guidelines and recommendations provided by these key role players for their curricula development.

The ACM is concerned with the development and sharing of new knowledge about all aspects of computing. It is a scientific and professional organisation founded in 1947. It has traditionally been the professional home of computer scientists who devise new ways of using computers and who advance the science and theory that underlies both computation itself and the software that enables it.

The AIS is a global organisation that serves academics that specialise in Information Systems. Founded in 1994, the AIS began providing curricula recommendations for Information Systems in cooperation with the ACM and the AITP in 1997.

The AITP was founded in 1951 as the National Machine Accountants Association. It became the Data Processing Management Association in 1962 and its present name was adopted in 1996. AITP serves those who focus on the professional side of computing and who use computer technology to meet business needs and other organisations.

The IEEE-CS was formed in 1946 as the Committee on Large-Scale Computing Devices of the American Institute of Electrical Engineers (AIEE) and, in 1951, as the Professional Group on Electronic Computers of the Institute of Radio Engineers (IRE). In 1964 the AIEE and IRE merged to form the IEEE and the two subunits joined to become the Computer Society (ACM/AIS/IEEE - CS, 2005).

Each society produced and published its own curricula recommendations prior to the 1990s. Over time, the advantage of these societies' cooperative work became obvious. In the late 1990s, the ACM and IEEE-CS joined forces again to produce an up-to-date curriculum report to replace the 1991 Computing Curricula (CC'91) which was published by the joint task force in the late 1980s. The CC'91 provided curricula guidelines for four-year Bachelor's degree programmes in CS and computer engineering. In the late 1990s, the ACM and IEEE-CS joined forces again to produce an up-to-date curriculum report to replace the CC'91 report. The ACM and IEEE-CS's goal was to produce a single report, Computing Curricula 2001 (CC2001) that would provide curricula recommendations for various computing disciplines.

Computing grew into so many dimensions that no single view seemed adequate. The days when the computing disciplines only consisted of CS, Computer Engineering and ISs were over (ACM/AIS/IEEE - CS, 2005). In response to the CC2001 model, other discipline-specific volumes were published. In 2002, the Information Systems community published an updated IS2002 report. The CC2001 prediction of additional emerging computing disciplines proved correct. A report on degree programmes in IT was under development and it had been anticipated that it would be published in 2006 and thus was referred to as IT2006 (ACM/AIS/IEEE - CS, 2005).

The curricula body of knowledge recommended by the key role players is structured in a three-tiered hierarchy. This structure is illustrated in Figure 4.1.

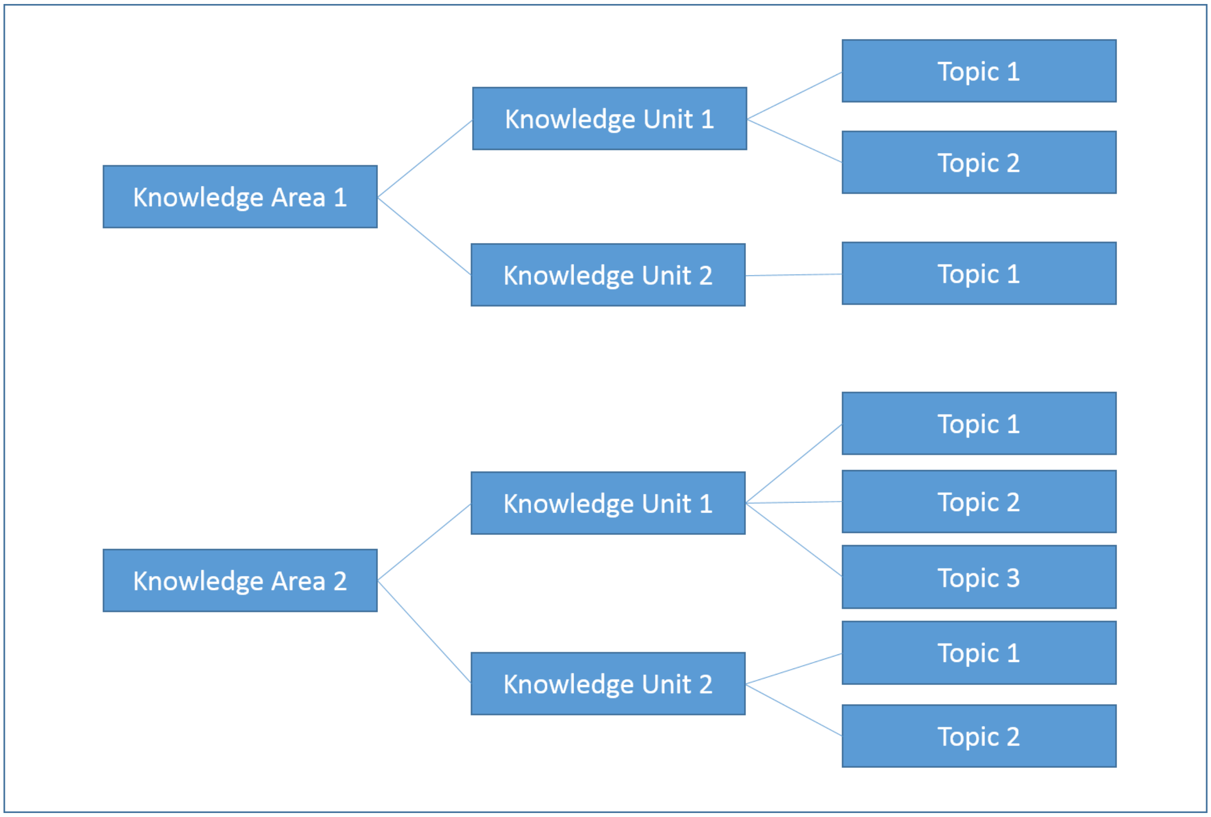

Figure 4.1: Body of Knowledge Structure (Dodge, 2013)

As shown in Figure 4.1, the highest level of the hierarchy is the knowledge area. It comprises of knowledge units, which form the middle tier of the hierarchy. The knowledge units represent a thematic module within a knowledge area. The thematic modules are defined in terms of a set of topics and learning outcomes, which help define the topics. These topics are at the lowest tier of the hierarchy (ACM/IEEE - CS, 2008b, 2013).

CS, IS and IT all fall under computing discipline qualifications. Computing includes designing and building hardware and software systems for an extensive variety of purposes that include processing, structuring and managing various kinds of information. It further includes but is not limited to conducting scientific studies using computers; making computer systems behave intelligently; creating and using communications and entertainment media and finding and gathering information that is relevant to any particular purpose (ACM/AIS/IEEE - CS, 2005). The focus of this research is in the CS, IS and IT computing disciplines, attesting to the fact that these are the three most common discipline qualifications available at South African higher education institutions.

4.3. Computing Graduate Requirements

The learning outcomes of any qualification should reflect the expected characteristics of graduates. The subsections below discusses the requirements and characteristics of computing graduates in the CS, IS and IT disciplines.

4.3.1. Computer Science

The characteristics of CS graduates span a wide range of areas within the computing discipline, from theoretical and algorithmic foundations to cutting-edge developments in robotics, computer vision intelligent systems, bioinformatics, amongst many other areas. Some of these characteristics are expressed by the ACM/IEEE - CS (2008a, 2013) as follows:

- **System-level perspective:** CS graduates must develop a high-level understanding of systems as a whole. This high-level understanding must go beyond the implementation details of the various components and should thus include the structure of computer systems and the processes involved in their construction and analysis;
- **Interplay between theory and practice:** An important aspect of the CS discipline is the balance and link between theory and practice. CS graduates should therefore not only understand the theoretical underpinnings of the discipline but also have an understanding of how the theory influences practice;
- **Familiarity with common themes and principles:** In the CS discipline, students will encounter a number of recurring themes such as abstraction, complexity and evolutionary change. They will also encounter principles such as those associated with ***security***, caching, sharing common resources, amongst many others. Students, therefore, need to realise that these themes and principles have a broad application and they should not only be seen to be relevant to the domains in which they were introduced;
- **Project experience:** To ensure that CS graduates can successfully apply the knowledge they have gained, it is important to ensure that all CS students are involved in a software project to demonstrate a practical implementation of the knowledge they have acquired; and
- **Adaptability/Commitment to life-long learning**: CS graduates must possess the ability to adapt to change as the history of the discipline has shown an enormous pace of change and rapid evolvement of the field (ACM/IEEE - CS, 2008a, 2013).

In addition, there are competencies that CS graduates should possess that are not explicitly listed in the body of knowledge. Professionals in the discipline typically embody a characteristic style of thinking and problem solving. This style emerges from experience obtained through the study of the discipline and professional practice. These characteristics will enable their success and further professional development in the discipline (ACM/IEEE - CS, 2013).

The work of computer scientists falls into three career paths, namely:

- **Designing and implementing software** – CS graduates take on challenging programming jobs. This refers to the work of software development that has grown to include aspects of web design, interface design, ***security issues***, mobile computing, and others. They also supervise other programmers, keeping them aware of new programming approaches;
- **Devising new ways to use computers** - This refers to the innovation in the application of computer technology; and
- **Developing effective ways to solve computing problems** - This refers to the application or development of computer science theory and knowledge of algorithms to ensure the best possible solutions to computationally intensive problems (ACM/AIS/IEEE - CS, 2005).

CS graduates should also possess fundamental competencies in the areas described in the body of knowledge, particularly the core topics contained therein. The ACM/IEEE - CS (2013) CS body of knowledge is organised into a set of eighteen knowledge areas. ***Information Assurance and Security (IAS)*** is one of the four new knowledge areas added in response to the importance of computer and network security growing significantly since the ACM/IEEE - CS (2001) and ACM/IEEE - CS (2008a) publications. IAS has since become an integral part of computing studies (ACM/IEEE - CS, 2013).

4.3.2. Information Systems

IS are an integral component of the products, services, operations and management of an organisation. The IS qualification at higher education institutions emerged in response to organisation’s extensive use of information processing and communication technology to operating processes, project management, decision support and enterprise and industry strategy (ACM/AIS, 2010). IS focuses on the integration of IT solutions and business processes to meet the information needs of organisations, enabling them to achieve their business objectives in an efficient and effective manner. The IS discipline views technology as an instrument to generate, process and distribute information and thus focuses on the information aspect of IT. IS graduates should, therefore, be able to understand both technical and organisational factors. In addition, they should also be able to assist an organisation to determine how information and technology-enabled business processes can provide the organisation with a competitive advantage (ACM/AIS/IEEE - CS, 2005).

The ACM/AIS (2010) model curriculum is based on expectations regarding the capabilities of IS graduates when entering organisations. The outcome expectations of the curriculum have been re-evaluated and articulated in the form of high-level IS capabilities and in three knowledge and skills categories which are listed below.

The high-level IS capabilities that the curriculum specifies as the highest level outcome expectations include:

- Improving organisational processes;
- Exploiting opportunities created by technology innovations;
- Understanding and addressing information requirements;
- Designing and managing enterprise architecture;
- Identifying and evaluating solution and sourcing alternatives;
- ***Securing data and infrastructure***; and
- Understanding, managing and controlling IT risks (ACM/AIS, 2010).

IS specific knowledge and skills are divided into four main categories, namely:

- Identifying and designing opportunities for IT-enabled organisational improvement;
- Analysing trade-offs;
- Designing and implementing information systems; and
- Managing ongoing IT (ACM/AIS, 2010).

The ACM/AIS (2010) curriculum is designed to educate graduates who are prepared to enter organisations equipped with the knowledge and skills specified in these categories. IS graduates are further required to possess knowledge and skills related to the management of ongoing information systems operations as well as, the securing of IT infrastructure and designing ***secure*** systems. IS graduates are required to be experts in high-level design and management of IT-based solutions that are in alignment with the organisation's goals. These graduates should also be able to ensure the security of organisational data and IT infrastructure resources from potential threats that can cause significant loss to the organisation’s image and financial resources. An understanding of ***security*** threats and high-level solutions could lead to the protection of organisational IT infrastructure and resources as IT solutions are closely integrated with all aspects of modern organisations, thus making the management of risks a necessity for all organisations (ACM/AIS, 2010).

IS graduates are expected to work closely with organisational information assets, information systems and IT infrastructure. The security of these information systems and related information assets was highlighted in Chapter 3. It is, therefore, essential to ensure that IS curricula at higher education level includes information security education to ensure that IS graduates can become employees that possess the knowledge, skills and understanding to ensure the protection of organisational information systems and related information assets from potential threats.

4.3.3. Information Technology

In contrast to IS, IT focuses more on technology, than on the information that it conveys. Within organisations, IT graduates assume a number of organisational responsibilities such as the installation of networks; network administration and ***security***; the design of web pages; development of multimedia resources; installation of communication components; oversight of email systems and the planning and management of the technology lifecycle by which an organisation’s technology is maintained, upgraded and replaced. These systems are required to work properly, be ***secured*** and upgraded and they must be maintained and replaced as necessary. Employees throughout an organisation require the support of IT professionals who understand the systems and the related software and are committed to solving computing problems. IT graduates who eventually become employees are required to respond to the everyday IT needs of organisations (ACM/AIS/IEEE - CS, 2005; ACM/IEEE - CS, 2008b).

According to the ACM/IEEE - CS (2008b), the integration of various technologies into organisations is fundamental to IT. IT graduates should, therefore, acquire skill sets that enable them to perform the integrative tasks successfully, including:

- An understanding of professional, ethical, ***security*** and social issues and responsibilities;
- The ability to apply knowledge of computing and mathematics appropriate to the discipline;

- The ability to analyse a problem and identify and define the computing requirements appropriate to its solution;
- The ability to design, implement and evaluate a computer-based system, process, component, or program to meet desired needs;
- The ability to use current techniques, skills and tools necessary for computing practice; and
- ***The ability to address IAS*** **concerns** (ACM/IEEE - CS, 2008b).

It is clear from the roles and responsibilities that IT graduates undertake as organisational employees that they will require information security skills, knowledge and understanding to ensure the protection of the various information systems that they will be responsible for within organisations. This security should be maintained in the design, development, maintenance and upgrade of these information systems.

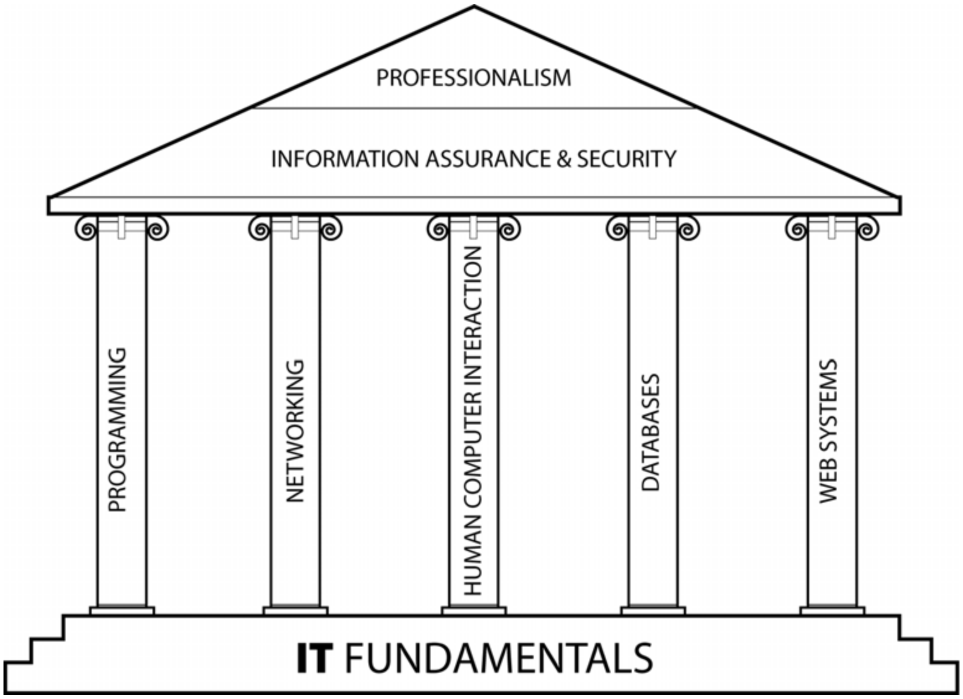

Figure 4.2: The IT Discipline (ACM/IEEE - CS, 2008b)

Figure 4.2 depicts the IT discipline. It is important to note that this figure does not depict all the aspects of the discipline. It does, however, help describe the relation of the key components of IT. The pillars of the IT discipline include programming, networking, human-computer interaction, databases and web systems. These pillars are built on the knowledge of the IT fundamentals. IAS together with professionalism overarch the pillars of this discipline (ACM/IEEE - CS, 2008b). It can, therefore, be argued that this highlights the need for information security to be addressed across the full scope of the IT discipline.

The following section discusses how information security relates to the computing curricula of the CS, IS and IT disciplines.

4.4. Information Security in Computing Curricula

This section presents information security as it relates to computing curricula of the CS, IS and IT disciplines and as a pervasive theme. The information security concepts that should be integrated are derived and introduced. This is followed by the approaches that can be used to integrate information security into computing curricula. This section concludes by identifying the challenges related to the integration of information security into computing curricula.

4.4.1. Information Security in CS, IS and IT

This subsection provides literature on information security as it relates to the CS, IS and IT disciplines.

The world’s reliance on IT and computing fuelled the addition of IAS as a new knowledge area within the CS and IT discipline’s body of knowledge, but not in the IS discipline. IAS is defined as a set of controls and processes that are intended to protect and defend information systems and related information assets by ensuring their confidentiality, integrity, availability, authentication and non-repudiation. Assurance carries a confirmation that the past and present processes and information are valid, while security ensures the protection of these processes and information. IAS education, therefore, includes all efforts to prepare computing graduates with the required information security skills, knowledge and competencies to protect organisational information systems and attest to the assurance of the past and present state of the processes and information assets (ACM/IEEE - CS, 2013).

A survey reported by Dodge (2013) was conducted to gather information on knowledge areas that had either increased or decreased in importance. The survey was sent to over 1500 institutions in the United States and to 2000 international institutions. The survey was primarily addressed to CS and to related disciplines’ department chairs and directors of undergraduate studies. However, only 201 participants responded to the survey. Despite the low response rate, valuable input was produced. The results of the survey and the analysis from the ACM/IEEE - CS (2013) steering committee clearly showed that the broad range of concepts defined by information security are an integral component of any undergraduate CS discipline. Information security was further refined and discussed during the World Conference on Information Security Education (WISE 7) in June 2011, organised by an internationally focused International Federation for Information Processing (IFIP) technical working group (WG 11.8) and a decision was made that it would be referred to as 'IAS' (Dodge, 2013).

IAS is explicitly included in the CS and IT bodies of knowledge as a knowledge area, however, it is not explicitly included as a knowledge area in the IS body of knowledge. Information security is, however, highlighted in the IS curricula guidelines and recommendations provided by the ACM/AIS (2010) as seen in Subsection 4.3.2. It can, therefore, be argued that due to the inclusion of information security in the IS curricula guidelines and recommendations it, therefore, highlights the importance of information security to IS graduates. IS graduates also focus on the integration of IT solutions to meet the needs of organisations, thereby enabling the organisation to achieve its business objectives effectively and efficiently. The IS discipline also views technology as an instrument to generate, process and distribute information, thus focusing on the information aspect of IT. It can, therefore, be argued that since information is an important organisational asset that IS graduates work closely with, it is important for IS graduates to be information security educated. It can, therefore, be argued that information security is taught to all undergraduate students in the CS, IS and IT computing disciplines.

Table 4.1 depicts the IAS knowledge units in the CS and IT discipline's IAS body of knowledge. Although different terminology is used across the two computing disciplines, it is clear that some of the knowledge units depicted in Table 4.1 are duplicated across both the CS and IT disciplines. For instance, similarities can be seen in the *'Digital forensics'* and *'Forensics'*; *'Threats and attacks'* and *'Attacks',* and *'Threat analysis model'; and 'Security policy and governance'* and *'Policy'.*

Computer Science - IAS Knowledge Units	Information Technology - IAS Knowledge Units
Foundational concepts in security	Fundamental aspects
Principles of Secure Design	Security mechanisms
Defensive Programming	Operational issues
Threats and attacks	Attacks
Network security	Threat analysis model
Cryptography	Security domains
Web security	Security services

Platform security	Information states
Security policy and governance	Policy
Digital forensics	Forensics
Secure software engineering	Vulnerabilities

Table 4.1: Information Assurance and Security Knowledge Units in the Computer Science and Information Technology Disciplines (adapted from (ACM/IEEE - CS, 2008b, 2013))

Each of the IAS knowledge units contains a collection of concepts and each concept has an associated learning outcome with the desired level of comprehension (familiarity, usage and assessment). Familiarity refers to students' understanding of what a concept is, or what it means. Usage refers to students being able to use or apply a concept in an appropriate manner, while assessment refers to students being able to consider a concept from multiple perspectives and being able to justify the use or selection of a concept for a particular solution (Dodge, 2013).

Table 4.2 provides an example of the concepts and learning outcomes for the knowledge unit *foundational concepts in security* according to the ACM/IEEE - CS (2013).

Concepts	Learning outcomes
1. CIA (Confidentiality, Integrity, Availability)	1. Analyse the trade-offs of balancing key security properties (Confidentiality, Integrity, and Availability). [Usage]
2. Concepts of risk, threats, vulnerabilities, and attack vectors (cross-reference Software Engineering/Software Project Management/Risk)	2. Describe the concepts of risk, threats, vulnerabilities and attack vectors (including the fact that there is no such thing as perfect security). [Familiarity]
3. Authentication and authorisation, access control (mandatory vs. discretionary)	3. Explain the concepts of authentication, authorisation, access control. [Familiarity]
4. Concept of trust and trustworthiness; Ethics (responsible disclosure). (cross-reference Social Issues and Professional Practice/Professional Ethics/Accountability, responsibility and liability)	4. Explain the concept of trust and trustworthiness. [Familiarity]; Describe important ethical issues to consider in computer security, including ethical issues associated with fixing or not fixing vulnerabilities and disclosing or not disclosing vulnerabilities. [Familiarity]

Table 4.2: Concepts and Learning Outcomes Relating to the Foundational Concepts in Security (ACM/IEEE - CS, 2013)

Table 4.2 depicts that the learning outcome associated with the CIA concepts is that computing students should be able to analyse the trade-offs of balancing these concepts. Furthermore, usage is the desired level of comprehension for the aforementioned learning outcome. This means that after learning about this learning outcome, computing students are expected to possess the skills to use or apply the fundamental information security concepts of CIA.

In Section 4.4, it was stated that the learning outcome of any qualification should reflect the expected characteristics of graduates.

The following subsection introduces and discusses information security as a pervasive theme.

4.4.2. Information Security as a Pervasive Theme

During the deliberations of the Special Interest Group for Information Technology Education (SIGITE) Curriculum Committee, several themes emerged that were considered essential. Furthermore, these essential themes did not seem to belong to a single specific knowledge area or unit and they were referred to as pervasive themes. Those themes referred to as pervasive themes include:

- User- centeredness and advocacy;
- ***Information Assurance and Security (IAS);***
- The ability to manage complexity through abstraction and modelling, best practices, patterns, standards, and the use of appropriate tools;
- A deep understanding of information and communication technologies and their associated tools;
- Adaptability;
- Professionalism (life-long learning, professional development, ethics, responsibility); and
- Interpersonal skills (ACM/IEEE - CS, 2008b; SIGITE Curriculum Committee, 2005).

IAS is unique in the collection of knowledge areas as it is defined as both a pervasive theme and knowledge area. Furthermore, the concept of pervasive themes also refers to the overlap that can and sometimes should, exist between knowledge areas and knowledge units. This overlap is not only considered necessary but is also valuable. Pervasive themes should, therefore, be addressed multiple times, in multiple modules (ACM/IEEE - CS, 2008b, 2013; SIGITE Curriculum Committee, 2005). Futcher, Schroder and Solms (2010) state that information security is a broad area of study. However, according to Massart (2015), students learn better when they focus on small information at a time. Since information security is said to be a broad area of study, it can, therefore, be argued that IAS as a pervasive theme could allow students to focus on small pieces of information security at a time. This could enable them to learn better as they will not be focusing on the entire scope of information security information at the same time.

In order for students to focus on small pieces of information security at a time, this research proposes that information security be broken up into information security concepts that can be integrated into multiple modules. This could enable them to be addressed multiple times from multiple perspectives in each module.

The following subsection presents an example of information security concepts that could be derived from literature and integrated into computing curricula.

4.4.3. Integration of Information Security Concepts

There are many information security concepts that could be pervasively integrated into a computing department's undergraduate modules. These could be derived from multiple literature sources. A high-level content analysis was conducted to derive common information security concepts. According to Krippendorff (2013, p. 24) a content analysis is a research technique that is used for "making replicable and valid inferences from texts to the context of their use". Within the context of this research, a content analysis was used to derive common information security concepts as depicted in Table 4.3 from the four sources listed in bullet form below and depicted in Table 4.3.

For this particular example, the following literature sources were used to derive the information security concepts as shown in Table 4.3.

- '*Information Technology 2008, Curriculum Guidelines for Undergraduate Degree Programmes in Information Technology*' document (ACM/IEEE - CS, 2008b);
- '*Computer Science Curriculum 2013*' document (ACM/IEEE - CS, 2013);
- ISO Standards (ISO/IEC 7498-2, 1989); and
- Management of Information Security authored by (Whitman & Mattord, 2014).

The ACM/IEEE - CS (2008b, 2013) literature sources specifically provide Curriculum Guidelines for Undergraduate Degree Programmes in CS and in IT, thus an analysis of the IAS knowledge area within the ACM/IEEE-CS was conducted. The ISO/IEC 7498-2 (1989) standard provides the basis of information security through five security services. The security services can be put into place to address a threat. Furthermore, at the researcher's institution, the prescribed information security textbook is the *'Management of Information Security'* authored by Whitman and Mattord (2014). This textbook was also used to derive the list of information security concepts. This list of derived information security concepts is depicted in Table 4.3.

		Source			
Information Security Concepts		ACM/IEEE-CS – Information Technology 2008	ACM/IEEE-CS – Computer Science Curriculum 2013	ISO/IEC 7498-2 (1989) standard	Whitman & Mattord (2014)
1.	Authentication	X		X	X
2.	Availability	X	X		X
3.	Backup and Recovery	X			
4.	Confidentiality	X	X	X	X
5.	Copyright	X			
6.	Cryptography	X	X		X
7.	Digital Forensics		X		
8.	Disaster Recovery	X			
9.	Information States	X			
10.	Integrity	X	X	X	X
11.	Intellectual Property				X
12.	Intrusion Detection	X			
13.	Legal and Ethical Behaviour Issues		X		
14.	Non-repudiation/Non-denial	X		X	
15.	Privacy				X
16.	Security Awareness	X			
17.	Secure-Coding		X		
18.	Secure Principles		X		
19.	Security Policies and Procedures	X	X		
20.	Secure Software Development		X		
21.	Security Standards				X
22.	Security Threats and		X		
23.	Security Vulnerabilities.	X			

Table 4.3: Information Security Concepts (derived from ACM/IEEE - CS (2008b, 2013); ISO/IEC 7498-2 (1989); and Whitman and Mattord (2014))

It must be noted that the list depicted in Table 4.3 does not include all possible information security concepts that could be derived from the ACM/IEEE - CS (2008b, 2013); ISO/IEC 7498-2 (1989);

and Whitman and Mattord (2014) documents. However, the concepts depicted in Table 4.3 can be used as a starting point in addressing information security especially in computing departments where information security was not previously integrated. The aim is, therefore, not to address everything as the number of concepts would be too long to address within this research. This research, therefore, proposes for the identified information security concepts to be narrowed down to a more manageable number to ensure that those information security concepts deemed more important by the computing department are integrated and addressed first. These information security concepts deemed more important would be referred to as fundamental information security concepts. These fundamental information security concepts would need to be identified by the department through a survey or discussion held with the department's computing educators.

Yang (2001) asks the following questions: "*How would we prepare our students so that they would be security literate?*" and "*Should computer security be integrated throughout the curriculum, or should special courses and/or tracks be integrated to address the needs?*" The following subsection addresses these questions by discussing the various approaches for integrating information security into undergraduate computing curricula.

4.4.4. Approaches for Integrating Information Security into Computing Curricula

Over a decade ago it was stated that computing graduates need to learn about information security to ensure that they design and build secure information systems (Conti et al., 2003). The identification of an appropriate approach could assist in ensuring that computing graduates are taught information security in a manner which could enable them to perform their roles and responsibilities securely within the organisation that will employ them.

There are various approaches for integrating information security into computing curricula. Whitman and Mattord (2004) identified five such academic approaches including:

1. **Add information security concepts to existing modules** – This approach refers to adding information security concepts to various existing modules. For example, programming could include the information security concept *'Secure software development',* and *'Secure-coding'*. Whitman and Mattord (2004) state that this is the most used and preferred approach as it is more effective to thread information security throughout various modules rather than to add it as a single module

2. **Add information security concepts to a capstone module or modules** – This approach refers to adding specific information security concepts to a capstone module or modules. For example, in the capstone project module in the final year of the undergraduate IT qualification in the School of Information Communication and Technology (School of ICT) at the Nelson Mandela Metropolitan University (NMMU), students could be required to demonstrate how they have integrated information security concepts they have been taught over the years in the network, software program, or game that they have designed, developed and implemented
3. **Independent security-related module** – This approach is the most common used approach where single security-related modules are created (for example, Computer Security, Information Security, Network Security). However, these security-related modules tend to fail to address the entire comprehensive scope and depth of information security. In addition, information security modules are usually offered as electives meaning that not all computing students are guaranteed to elect such a module
4. **Information security certificates** – This approach refers to the implementation of a cohesive set of certification classes. This approach requires detailed planning based on the objective and the desired focus of the specific qualification
5. **Information security qualification** – This approach refers to information security education at baccalaureate level. However, it takes a great deal of effort to develop a qualification of this magnitude and it requires numerous resources to offer it (Whitman & Mattord, 2004).

To decide on which approach to implement, a department has to evaluate the available resources, time, faculty, money, technology and student demand. Whitman and Mattord (2004), therefore, suggest beginning with the first two approaches and then the additional approaches as demand presents itself (Whitman & Mattord, 2004).

Similarly, Perrone, Aburdene and Meng (2005), describe three approaches for integrating computer security into the curriculum, namely: Single module approach, track approach and thread approach. Although Perrone et al. (2005) relate to computer security, it can easily be applied to information security. The approaches recommended by Perrone et al. (2005) include:

1. **The single module approach** is the creation or offering of one module in the attempt to provide undergraduate students in the computing discipline with the most relevant information security concepts. This module is mostly offered as an elective module at undergraduate or

postgraduate level. It is of limited effect in producing graduates with the necessary information security education. This approach is similar to the *independent security-related module* approach as suggested by Whitman and Mattord (2004);

2. **The track approach** is highly effective in educating undergraduate computing students with information security and assurance skills. It is, however, difficult to implement in a small undergraduate qualification where the faculty is small and where there is a lack of resources such as laboratories and equipment, to implement the track approach. This approach requires extensive resources that most departments cannot afford; and
3. **The thread approach**, on the other hand, can be integrated into the curriculum without drastically changing the core content of the module. This approach does not require computing educators in the department to be information security trained at the same time, but rather enables individual educators to develop material at their own pace and change the curriculum gradually. This approach would require material on information security to be embedded into the current curriculum and therefore, does not require additional isolated information security modules. The thread approach provides exposure to smaller units of knowledge over a longer period of time allowing students to reflect and better assimilate the basic concepts of information security. It enables students to appreciate the importance of information security as an underlying cross-curricular theme, which helps students avoid the isolation of concepts. Perrone et al. (2005) argue that this approach could meet the information security needs of undergraduate CS students.

According to Chung et al. (2014), the integration of information security concepts across existing CS and IS curricula has proven to be effective, while not impacting higher education institutions with limited resources with a complete curriculum change. Department educators only need to spend a small amount of time making the necessary changes to their curriculum.

This research supports the, "*add information security concepts to existing modules"* approach as suggested by Whitman and Mattord (2004) and the above-mentioned *"thread approach"* suggested by Perrone et al. (2005) as they are similar and support the *"pervasive theme"* suggested by the (ACM/IEEE - CS, 2008b, 2013). It can, therefore, be argued that by integrating information security concepts as a pervasive theme in multiple modules, computing educators and students could achieve the benefits provided by the thread approach.

The following section discusses the challenges related to integrating information security into computing curricula.

4.4.5. Challenges of Integrating Information Security into Computing Curricula

Various approaches relating to the integration of information security into the curriculum were discussed in Subsection 4.4.4. Thus the challenges related to integrating such a theme into the curriculum cannot go unmentioned.

Based on the literature studied, the following challenges were identified:

1. Department educators lack adequate knowledge in security (Yang, 2001);
2. Students are unable to transfer knowledge to new situations as learning is often compartmentalised and is highly contextual (Davis & Dark, 2003);
3. Teaching information security as an information security module in the final year is inefficient as students have already learned how to use computers with little to no regard for information security, therefore, meaning that information security is then considered an afterthought (Hentea, 2005; Irvine et al., 1998);
4. The existing undergraduate computing curriculum is already over-extended (Taylor & Azadegan, 2008); and
5. Information security is a broad area of study (Lynn Futcher et al., 2010). This makes it challenging for departments to address all information security concepts if the curriculum is already over-extended.

Higher education institutions and their various computing departments should address these challenges to ensure the effective and efficient integration of information security into undergraduate computing curricula. Taylor and Azadegan (2008) state that in order for the integration of information security into the curriculum to be feasible, it should be as seamless as possible. This, therefore, highlights the need to address any challenges identified by the department in order to make the integration of information security as seamless as possible.

4.5. The Significant Impact that Pervasive Integration Provides

This section discusses the significant impact that the pervasive integration of information security into undergraduate computing curricula could provide to computing graduates.

The pervasive integration of information security means that information security is integrated into a number of existing modules. In Subsection 4.4.4, other approaches similar to the pervasive theme were discussed. Particular attention was given to the "*add information security concepts to existing modules"* approach and the *"thread approach".* It was stated that this research supports both the above-mentioned approaches as they are similar to and both support the *"pervasive theme".* It was argued that due to the similarities between the *"pervasive theme"*; the "*add information security concepts to existing modules"* approach and *"thread approach"*, they could share the benefits provided by each. These benefits include, but are not limited to the following:

- Information security can be addressed in more than one module since it has a lot of scope and depth;
- Information security can be introduced gradually over a prolonged period of time, as opposed to overwhelming students with the scope and depth of information security in a single isolated information security module;
- Students will not consider information security as an isolated theme but rather a pervasive theme;
- Information security can be taught from a different perspective in each of the modules that it is pervasively integrated into, thereby showing the students how information security relates to other modules and the omnipresence of information security;
- Pervasively integrating information security will not require computing educators in the department to be trained simultaneously, but rather enable individual educators to develop material at their own pace and change the curriculum gradually; and
- Undergraduate computing students could potentially exit higher education institutions with the required information security skills, knowledge and understanding when it is pervasively integrated into multiple modules, as opposed to when it is taught in a single isolated elective module that not all students will elect.

As discussed, there are many benefits provided by the pervasive integration of information security into undergraduate computing curricula. When undergraduate computing students exit higher education institutions and enter into various organisations, these computing graduates could possess the required information security skills, knowledge and understanding to protect organisational information systems and related information assets from potential threats from the first day they are employed. It can, therefore, be argued that the pervasive integration of information security into undergraduate computing curricula, could enable computing graduates to become a stronger link in securing organisational information systems and related information assets.

4.6. Conclusion

Information security education is vital to undergraduate computing CS, IS and IT students. The pervasive integration of information security concepts into undergraduate computing modules could ensure that all undergraduate CS, IS and IT students possess the required information security knowledge, skills and understanding upon graduating from higher education institutions. This could ultimately ensure that these computing graduates become a stronger link in securing organisational information systems and related information assets from potential threats.

The successful and seamless integration of information security into undergraduate computing curricula depends on various stakeholders in a higher education environment. These stakeholders include Directors of Schools, Heads of Department and Computing Educators. In terms of this research, it was necessary to determine their perspectives in this regard. The following chapter provides the results and findings of the survey conducted to determine the stakeholders' perspectives regarding the integration of information security into undergraduate computing curricula.

Chapter 5 – The Integration of Information Security into Computing Curricula: A South African Perspective

The purpose of this chapter is to provide an introduction to the survey and the manner in which it was conducted. Furthermore, it presents significant results and findings from the survey. The primary aim of the survey undertaken was to determine computing educators' perspectives on information security education in a South African context.

5.1. Introduction

Organisational employees have often been cited as the "weakest link" in securing organisational systems. Computing graduates often take on roles and responsibilities within organisations that involve designing, developing, implementing, upgrading and maintaining the information systems that house organisational information assets. It is, therefore, important for information security education to be taught to Computer Science (CS), Information Systems (IS) and Information Technology (IT) graduates. The education of these computing graduates could ensure that they become a stronger link in securing organisational information systems and related information assets.

In order for computing graduates to be able to perform the roles and responsibilities mentioned above, it is necessary for higher education institutions to equip them with the required information security skills, knowledge and understanding to protect organisational information systems and related information assets from potential threats. However, the existing curricula guidelines do not provide much guidance in terms of "***how"*** this can be done.

In terms of this research, it was, therefore, necessary to conduct a survey with computing educators to determine their perspectives regarding information security and the various challenges regarding its integration into undergraduate computing curricula. Furthermore, the survey helped determine the fundamental information security concepts and ideas on "***how"*** to pervasively integrate them into computing curricula. This survey aimed to meet one of the three secondary objectives, as stated in Section 1.3. Secondary Objective 3 aimed, ***"to determine computing educators' perspectives on information security education in a South African***

context". In order to meet this secondary objective, four survey objectives were identified as depicted in Chapter 1, Table 1.2.

Section 5.2 provides the detailed results and findings of the survey, while Section 5.3 discusses the key findings and Section 5.4 concludes this chapter.

5.2. Questionnaire Results and Findings

The survey was conducted as semi-structured interviews supported by a questionnaire. The survey had 21 participants, all of whom were educators in CS, IS or IT disciplines. The participants were from nine departments in seven higher education institutions in South Africa. The subsections below report on the results and findings of this survey according to each survey objective.

5.2.1. Survey Objective 1

The first survey objective was, ***to determine computing educators' perspectives on the integration of information security into undergraduate computing curricula***. Detailed questions for survey objective 1 of this study can be seen in Chapter 2, Table 2.2.

Question 1: What is your perspective on the importance of information security education to undergraduate computing students?

All 21 (100%) participants indicated that information security education is important to computing students and that it should be part of the undergraduate computing curriculum. In support of this, it was mentioned that information security education is critical from the first to the final year of study. In doing so, it could assist with equipping computing students with the skills needed to protect themselves, their personal information, as well as organisational information. In addition, it was stated that computing students need to understand the various threats that exist pertaining to information security in order for them to be able to combat such threats within organisations.

Question 2: What is your perspective on the pervasive integration of information security into undergraduate computing curricula?

18 (86%) of the participants indicated that it is necessary for information security to be pervasively integrated into undergraduate computing curricula. In support of this, it was stated that no single module could cover the scope and depth of information security. Another participant mentioned that by pervasively integrating information security, one could demonstrate the omnipresence of

information security, thereby showing that information security is not an isolated theme. Similarly, it was stated that by pervasively integrating information security into various modules, it would enable students to relate it to all such modules. This could, in turn, enable them to implement information security into their projects, work and everyday lives. Despite the general consensus that information security education is important to undergraduate computing students (Question 1), 3 (14%) of the participants were not sure as to whether information security should be pervasively integrated into computing curricula. A comment was made that a module should focus on teaching the content of that particular module. Some participants also suggested that it could be difficult for information security to be integrated into certain modules.

Question 3: What is the department/colleagues perspective on the pervasive integration of information security into undergraduate computing curricula?

With regards to their colleagues, it was generally agreed that they would consider integrating information security concepts into their modules. However, it was mentioned that in many cases, the curriculum was already overloaded and therefore time would not allow for such integration. In some cases, it was mentioned that some colleagues were under the impression that information security is addressed in another module within the department, while others were of the notion that addressing information security is not their duty nor the purpose of their module.

Some of the participants indicated that their colleagues may not be aware of the importance of information security in computing education and would, therefore, need to be convinced. In addition, it the study participants mentioned that educators are often resistant to change and some may perceive the integration of another theme such as information security into their modules as additional work.

Question 4: Has your department ever had a formal discussion regarding information security?

Responses regarding formal information security discussions highlighted that the extent to which this is done varies extensively across the various departments and higher education institutions. 8 (38%) of the participants indicated that a formal discussion regarding information security had been held within their department, while 13 (62%) of the participants indicated that no such discussion had been held.

Table 5.1 depicts a summary of computing educators’ perspectives that were reported on in this subsection.

Computing Educators' Perspectives
Information security education is important
Information security should be pervasively integrated into undergraduate computing curricula
No single module can address the scope and depth of information security
The pervasive integration of information security could demonstrate the omnipresence of information security
A module should focus on teaching the content of that particular module
Information security could be difficult to integrate into some modules
The curriculum is overloaded, therefore, time will not allow for the integration
Computing educators are under the impression that information security is addressed in another module
Computing educators are of the notion that addressing information security is not their duty or purpose of their module
Computing educators need to be convinced about the importance of information security in computing education
Computing educators are resistant to change and they perceive the integration of another theme such as information security into their module as additional work
The majority of departments have not held a formal information security discussion

Table 5.1: Summary of Perspectives Regarding the Integration of Information Security

The following section presents the results and findings of survey objective 2.

5.2.2. Survey Objective 2

Survey objective 2 aimed, ***to determine computing educators' perspectives on the current integration of information security into their curricula***. Table 5.2 depicts the three questions related to this survey objective, as well as the corresponding responses.

Detailed Question		Yes	No
Question 5	Does the department have a security-related module that is taught to all undergraduate computing students?	**4 (19%)**	17 (81%)
Question 6a	Do you integrate information security into your module?	14 (67%)	7 (33%)
Question 6b	If Yes, do you assess information security within your module?	**11 (79%)**	3 (21%)

Table 5.2: Survey Objective 2 Responses

Question 5: Does the department have a security-related module that is taught to all undergraduate computing students?

From Table 5.2, it is clear that most departments do not have a security-related module that is taught to all undergraduate computing students, as only 4 (19%) of the 21 participants indicated that such a security-related module exists within their department. 17 (81%) of the participants indicated that no such security-related module exists within their department. Some participants indicated that a security-related module is only offered to computing students at fourth year level, also referred to as Honours or Bachelor of Technology (BTech) level. However, this module is often offered as an elective. This means that not all students who proceed to fourth year level would take this module. It would be necessary for them to select the relevant security-related module in order to develop the necessary information security knowledge, skills and understanding required upon graduating from the particular higher education institution. Some students simply do not proceed to this level and they exit higher education institutions without being exposed to information security education. Another participant highlighted that, an undergraduate security-related module was offered in their department, but was discontinued when the curriculum was redesigned.

Question 6a: Do you integrate information security into your module?

Question 6b: If Yes, do you assess information security within your module?

Only 14 (67%) of the participants integrated information security into their own module and 11 of these participants actually assess it. The 7 (33%) participants who do not integrate information security into their modules indicated that they did not integrate it as they did not regard it as being important or relevant to their module, while others mentioned that they were already forced to integrate Human Immunodeficiency Virus (HIV) and Acquired Immune Deficiency Syndrome (AIDS) education into their modules. Furthermore, others indicated that they did not have enough time to cover the content that is already included in their module curriculum. This means that they do not have the capacity to include any additional themes such as information security into their curriculum. In addition, some participants indicated that they would prefer to retain the core focus of their modules.

Table 5.3 illustrates a summary of the current integration of information security as reported within this subsection.

Computing Educators' Perspectives
Most departments do not have a security-related module that is taught to all undergraduate computing students
A security-related module is offered as an elective at fourth year level at some universities

Some computing students do not proceed to fourth year level
Educators do not integrate information security into their modules as they do not regard it as being important or relevant to their modules
Educators are already forced to integrate other themes (e.g. HIV and AIDS) into their modules
Educators do not have enough time to cover the content of their modules, therefore, they would not have time to cover other content from themes such as information security
Educators would like to retain the core focus of their modules

Table 5.3: Summary of Perspectives Regarding the Current Integration of Information Security

The following section reports on the results and findings of survey objective 3.

5.2.3. Survey Objective 3

This survey objective was, ***to determine which fundamental information security concepts should be integrated into undergraduate computing curricula as a pervasive theme***. The question for survey objective 3 of this study can be seen in Chapter 2, Table 2.4.

Question 7: What fundamental information security concepts do you think should be pervasively integrated into undergraduate computing curricula?

This question was supported by an information security concept checklist (see Appendix B2). 2 participants were unable to complete this checklist due to time constraints. Therefore, only 19 of the 21 participants completed it. When completing the checklist, participants were encouraged to provide a brief comment for their reasoning when indicating whether a concept should be considered a fundamental information security concept that should be pervasively integrated into computing curricula. However, not all participants provided reasons for their information security concept selections.

In terms of this research, any information security concept where 17 (89%) or more participants indicated that the concept should be pervasively integrated into undergraduate computing curricula was considered as a fundamental information security concept.

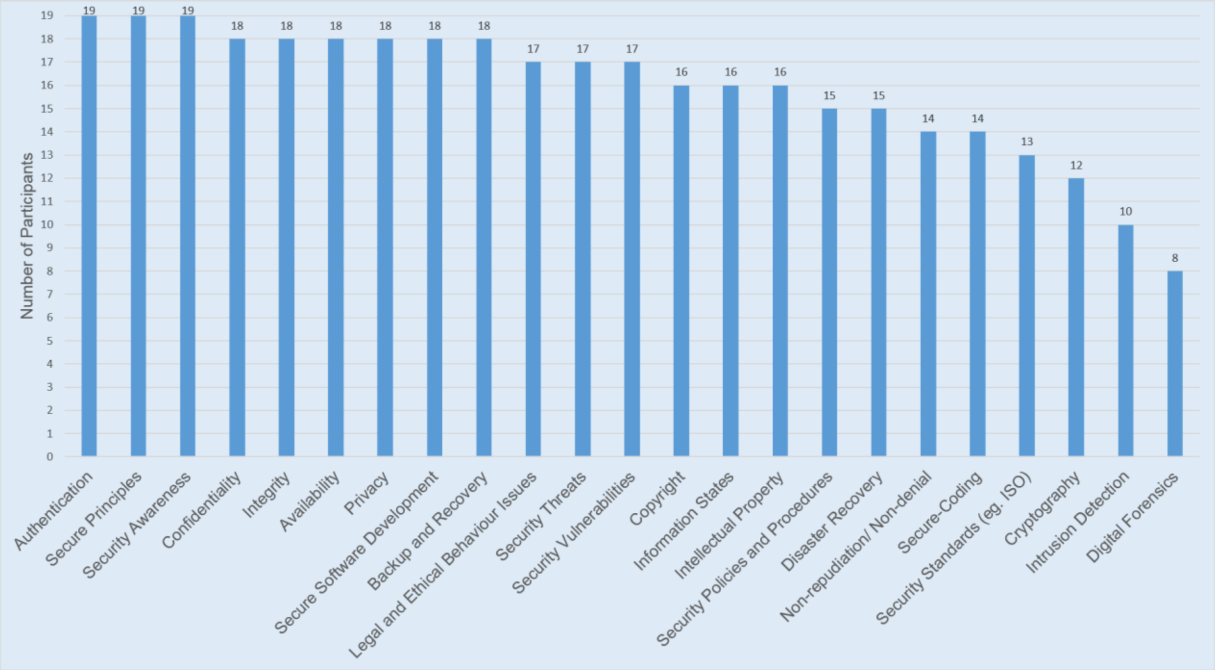

Figure 5.1: Information Security Concepts

As depicted in Figure 5.1, 19 (100%) of the participants indicated that *authentication*, *secure principles* and *security awareness* should be pervasively integrated into undergraduate computing curricula. Furthermore, 18 (95%) of the participants regarded *confidentiality*, *integrity* and *availability* to be fundamental information security concepts. Some participants indicated that the three critical characteristics cannot be separated and thus should be taught together and combined with *authentication*. Computing students should be taught these concepts from first to final year level as they are important and ensure that the graduates know-how to ensure that information remains confidential, is not altered and that it is available to those authorised to gain access to it. In addition, 18 (95%) of the participants regarded *privacy*, *secure software development* and *backup and recovery* as fundamental information security concepts. Participants indicated that *privacy* is important in ensuring the protection of one's own information, especially in the social media era. The study participants also stated that *secure software development* is especially important to the development of any software system and that it should be pervasively integrated particularly at third year level. *Backup and recovery* were regarded as fundamental as it is important to ensure that students can perform the *backup and recovery* of data to prevent data loss. Some participants indicated that although *backup and recovery* are an advanced information security concept, they should still be regarded as fundamental concepts to be pervasively integrated from the first year to the final year.

In total, 17 (89%) of the participants indicated that *legal and ethical behaviour issues in computing* are important concepts to teach computing students as they relate to the required *legal and ethical behaviour issues* when designing, developing, implementing and maintaining systems. A participant also highlighted that it is important to ensure that computing students are aware of and understand that various countries may have different legal and ethical standards.

Furthermore, 17 (89%) of the participants indicated that is important that students are taught about *security threats* and *security vulnerabilities* to ensure that they can identify and understand the various security threats and vulnerabilities relating to information systems. The participants suggested that the integration of these concepts could enable them to develop, design, maintain and update systems to ensure that they are secure from potential security threats and vulnerabilities.

In terms of this research, any information security concept where 16 (84%) of the participants or less indicated that it is a fundamental information security concept was considered to be non-fundamental. This is to limit the number of fundamental information security concepts to integrate to a manageable number. At this time, this research does not want to address every information security concept, as this is a starting point.

16 (84%) of the participants indicated that the knowledge of *information states* is important for computing students. Similarly, 16 (84%) participants also indicated that *copyright* and *intellectual property* are important, as both these concepts relate to each other and could assist computing students in avoiding plagiarism and other issues relating to *copyright* and the protection of *intellectual property*. Furthermore, the participants suggested that these concepts must be taught together from the first to the final year. However, 3 (16%) of the participants indicated that *copyright* and *intellectual property* are non-fundamental concepts and should only be addressed in an advanced security-related module.

A total of 15 (79%) of the participants indicated that it is vital to ensure that computing students understand and are aware of *security policies and procedure*, while 4 (21%) participants regard this concept to be too advanced, therefore, indicating that it is a non-fundamental concept. Furthermore, 15 (79%) of the participants indicated that *disaster recovery* is an important concept for recovering a computing student’s own work and that it should be integrated from the first year through to the final year of study. Some participants, however, suggested that the integration of this concept requires practical implementation and physical infrastructure, while 4 (21%) of the participants indicated that is a non-fundamental concept. A comment was made that *disaster recovery* should be regarded as a specialist area in the industry.

The concepts of *non-repudiation/non-denial* and *secure-coding* were considered to be fundamental by only 14 (74%) of the participants. These participants indicated that *non-repudiation/non-denial* should be integrated into computing curricula from the first year to the final year of study. However, 5 (26%) of the participants indicated that these concepts are non-fundamental information security concepts, thus indicating that they should not be pervasively integrated into computing curricula. The participants who indicated that *secure-coding* should be pervasively integrated indicated that it should be integrated into programming-related modules from the first year to the final year of study.

A further 13 (68%) of the participants regarded *security standards* to be an important information security concept. A total of 12 (63%) participants regarded *cryptography* as an important information security concept. Furthermore, 10 (53%) of the participants regarded *intrusion detection as a* fundamental information security concept, while only 8 (42%) participants regarded *digital forensics* as a fundamental information security concept.

A further comment indicated by the participants who considered *non-repudiation/non-denial*, *secure-coding, security standards, cryptography, intrusion detection and digital forensics* as non-fundamental information security concepts indicated that these concepts should rather be taught in a more advanced information security module. Furthermore, *cryptography* and *digital forensics,* similar to *disaster recovery*, were regarded as specialist areas in industry and therefore the participants argued that they should not be pervasively integrated into undergraduate computing curricula.

From the results and finding of this subsection, it is evident that only 12 information security concepts can be deemed as fundamental information security concepts that should be pervasively integrated into undergraduate computing curricula. These 12 fundamental information security concepts are depicted in Table 5.4.

Fundamental Information Security Concepts	
1.	Authentication
2.	Secure Principles
3.	Security Awareness

4.	Confidentiality
5.	Integrity
6.	Availability
7.	Privacy
8.	Secure Software Development
9.	Backup and Recovery
10.	Legal and Ethical Behaviour Issues
11.	Security Threats
12.	Security Vulnerabilities

Table 5.4: Fundamental Information Security Concepts

The following section reports on the results and findings of survey objective 4.

5.2.4. Survey Objective 4

This survey objective aimed ***to identify possible ideas and challenges for integrating information security concepts into computing curricula***. The questions for survey objective 4 of this study can be seen in Chapter 2, Table 2.5.

Question 8: Do you have any ideas on how to pervasively integrate information security concepts into various undergraduate computing modules?

Many participants indicated that a good way to pervasively integrate information security concepts into various modules would be to contextualise these concepts to make them as relevant as possible for each particular module. For example, when teaching a Networks module, *confidentiality, integrity and availability* could be discussed within the context of firewalls and intrusion detection and prevention systems. It is also important to integrate the fundamental information security concepts in a manner that the students will find to be interesting. It was suggested that social or interactive discussions related to the students' experience with regards to information security may be beneficial, thereby integrating the concepts through discussion as well as into the theory of the modules. In addition, some participants proposed that it would be beneficial to integrate practical concepts through application to equip computing students with the skills required to implement them. Furthermore, it was proposed that information security concepts should be pervasively integrated from the first year to the final year of study and should be assessed through a capstone project in their final year. Other participants suggested that various information security concepts could be grouped and taught together to show computing students how they relate to one another.

Participants also suggested that social media and smartphones could be used as frames of reference to convey certain information security concepts, thereby engaging students through platforms they are familiar with. A further proposal was that each fundamental information security concept must be covered in at least one of the undergraduate computing modules, while other participants suggested that all concepts be taught in all modules.

Table 5.5 depicts the ideas for integrating information security concepts into computing curricula.

Computing Educators' Ideas
Contextualise information security concepts
Practically apply information security concepts where possible
Relate information security concepts to students by using frames of reference common to computing students (e.g. social media, mobile phones)
Integrate information security concepts from the first year to the final year
Information security should be included in departmental plan
Information security should be pervasively integrated from the first year to the final year and assessed through a capstone project in the final year
Information security concepts should be grouped and taught together to show computing students how the information security concepts relate to one another
An information security concept should be covered in at least one of the undergraduate computing modules
An information security concept should be covered by all modules

Table 5.5: Ideas for Integrating Information Security Concepts

Question 9: What challenges do you foresee in the pervasive integration of information security concepts into undergraduate computing curricula?

The challenge that participants highlighted was that there is often not enough time to work through current module content. Any additional content, for example, information security concepts, needing to be included would prove very challenging from a time perspective. Participants suggested that the planning of how and where these concepts could be integrated should be done at the beginning of each year to ensure that each concept is addressed multiple times in multiple modules. A few of the participants indicated that a further challenge may be resistance from computing educators as some could be reluctant to change. Considering their "buy-in", it would be important to convince computing educators about the value of information security education in order to increase their willingness to integrate information security concepts into their modules. Their "buy-in" would be necessary for the pervasive integration of information security to be successful. Furthermore, other participants indicated that the "buy-in" of the computing educators could be dependent upon the manner in which the department approaches and plans for such integration. Participants also suggested that a directive should come from top management within the higher education institution or department in order to increase the willingness of computing educators to pervasively integrate information security into their modules. Furthermore, the participants mentioned that some computing educators may be unaware, or lack knowledge, regarding information security concepts, or may not be confident in teaching these concepts. Therefore, it was suggested that, in order to facilitate their integration, the fundamental information security concepts should be provided to educators in a format that would make it easy for them to understand and convey to students. A further challenge would be the lack of or limited availability of infrastructure or resources (for example, laboratories, educators and time) at certain institutions to ensure that students can practically implement some of the fundamental information security concepts that can be implemented practically.

Question 10: Do you think computing educators would be able to pervasively integrate these fundamental information security concepts into their various modules?

17 (81%) of the participants indicated that computing educators would be able to integrate the fundamental information security concepts into their various modules. Furthermore, it was indicated that those information security concepts, which complement the module, rather than take away from its main focus, would be more easily integrated. One of the participants mentioned that educators in their department do possess the necessary knowledge and expertise and would therefore easily be able to integrate fundamental information security concepts into their modules. However, 4 (19%) of the participants indicated that they did not think that computing educators within their department would be able to integrate the fundamental information security concepts into their modules.

Table 5.6 illustrates the perceived challenges for integrating information security concepts into computing curricula.

Perceived Challenges
Not enough time to work through the current curriculum – educators are already overloaded
Computing educators resistant to change – “buy-in” and convincing of information security education value needed
Directive should come from top management to increase the willingness of computing educators to pervasively integrate information security
Computing educators lack information security “know-how”

Lack or limited number of resources (e.g. laboratories, educators)

Table 5.6: Perceived Challenges for Integrating Information Security

The following section discusses the key findings pertaining to the survey undertaken to elicit perspectives of the South African computing educators' who participated in the survey, their ideas and challenges regarding the pervasive integration of information security into undergraduate computing curricula.

5.3. Discussion of Key Findings

In order for information security to be successfully integrated, it needs to be done in a manner that complements the module rather than taking away from the main focus and content of that module. Pervasive integration implies that fundamental information security concepts should be taught in multiple modules to ensure that relevant information security skills, knowledge and understanding are transferred to the students across multiple modules. This, however, was deemed an unnecessary duplication by some participants. These participants did not understand that fundamental information security concepts could be addressed from a different perspective within various modules. For example, the fundamental information security concepts of *privacy, backup and recovery, security threats, security vulnerabilities, and legal and ethical behaviour issues* can be integrated and taught from different perspectives to ensure that they relate to each specific module. By integrating fundamental information security concepts in this manner, it could be ensured that they complement the module, rather than detract from the focus and purpose of that specific module.

Furthermore, the participants suggested that fundamental information security concepts must be gradually introduced from the first year to the final year modules. This would ensure that computing students understand them better to prevent them from being taught all the fundamental information security concepts at once in a single module. Although a single module cannot address the scope and depth of information security, it is also understandable that not all fundamental information security concepts can be integrated into all modules. It would be essential, therefore, for the computing departments to identify the fundamental information security concepts that can be integrated into the various modules within their department and to discuss how each fundamental information security concept could be integrated into various modules from the first year to the final year of the qualification. This could, therefore, enable the scope and depth of information security to be covered by various modules in the curriculum. Furthermore, it is essential for computing educators to understand that integrating information security concepts as a pervasive theme, instead of isolating it in a single information security module, could assist students with understanding information security from various perspectives. This could help ensure that it is not considered as an afterthought or abstract concept after designing, developing or implementing information systems.

To further assist with the pervasive integration of fundamental information security concepts into computing curricula, it was suggested that examples of how computing educators could integrate the fundamental information security concepts into their modules and how to make these examples relevant to their specific module and context would benefit educators, particularly those whose modules are not security focused. They further indicated that it would be beneficial for the department to support the integration and to give a directive to educators within the department that they need to pervasively integrate the various fundamental information security concepts into their modules. Many participants also highlighted that for any of these ideas or strategies to work, educators must be motivated and willing to integrate these information security concepts into their particular modules. It would, therefore, be ideal to ensure that all computing educators within a department are aware of information security and the current integration thereof within the department. Computing educators should be convinced that information security concepts can be integrated into their module without changing the core content of their module.

In most higher education institutions where no security-related module is currently taught to undergraduate computing students, information security is taught as a single module at fourth year level. This module is often an elective, meaning that although students may study beyond a diploma or undergraduate qualification if the student does not elect information security as a module, they may graduate and enter organisations without ever being exposed to information security. This, therefore, highlights the significant impact that the pervasive integration of information security education could have on undergraduate computing students. It can, therefore, be argued that by pervasively integrating information security into undergraduate computing curricula, all computing students would be exposed to information security from various perspectives in different modules. This could ensure that these computing students graduate having acquired information security skills, knowledge and understanding to perform their organisational roles and responsibilities in a secure manner.

5.4. Conclusion

This chapter provided the results and findings of the survey undertaken with Heads of Departments and computing educators at various South African higher education institutions that were surveyed. From the results and findings reported in this chapter, it is clear that the South African computing educators who participated in this survey regard information security education of undergraduate computing students as important. However, from the results and findings provided, it is evident that not all of the educators support the pervasive integration of information security into undergraduate computing curricula. A number of suggestions on how one can practically integrate information security into their curriculum were provided as well as the challenges that could be encountered when doing so.

The lack of undergraduate information security education of all computing students that graduate from South African higher education institutions could be detrimental to the organisations that might employ them. This lack of information security education could compromise the security of the organisation's information systems and related information assets that they will work on. It is, therefore, necessary to develop a framework to assist computing educators with ***"how"*** information security can be pervasively integrated into undergraduate computing curricula. This framework will be developed by using some of the suggestions provided by the participants of this survey and from suggestions identified through the literature review of this research.

The following chapter introduces the framework to assist higher education institutions, departments and computing educators to pervasively integrate fundamental information security concepts into their curriculum. This could assist in ensuring that departments are able to integrate information security into their curricula. This could lead computing departments to being able to produce computing graduates who possess the necessary information security skills, knowledge and understanding to be a stronger link in securing organisational information systems and related information assets from potential threats.

Chapter 6 – Information Security Education Framework

This chapter provides a solution to the research problem stated in Chapter 1, Section 1.2. It is presented as a framework that can be implemented by higher education institutions' computing departments and computing educators to pervasively integrate information security into their undergraduate computing curricula.

6.1. Introduction

In Chapter 1, it was stated that the ACM/AIS/IEEE-CS provides computing curricular guidelines and recommendations for the development of higher education institutions' educational content, as well as the recommendation that information security should be pervasively integrated into computing curricula. However, it does not provide enough guidance to computing educators on **"*how*"** to pervasively integrate information security into various modules. This led to the identification of the problem stated in Chapter 1, Section 1.2 which is, ***"Currently, no generally used framework exists to aid the pervasive integration of information security into undergraduate computing curricula".***

As stated in Chapter 3, Section 3.1, information is an important and valuable asset in all modern-day organisations. It is, therefore, important that organisations protect their information from potential threats as a lack of protection could cause undue business interruptions and damage to an organisation's reputation. In Section 3.2, it was stated that although organisations entrust their employees to provide an appropriate and adequate level of security to information systems, employees do not always provide this level of security. This has been argued in research, where employees have been cited as the "weakest link" in protecting information systems. Furthermore, it was stated that this often results in employees being one of the biggest and closest threat agents that could cause harm to an organisation's information systems and information assets. In addition, it was argued that employees will remain the "weakest link" unless the appropriate security measures such as awareness, training and education, organisational security measures (policy) and technological security measures (technology) are properly implemented. It was further emphasised in Subsection 3.4.3 that relying on organisational and technological security measures alone is not enough as these rely heavily on humans to design, develop, implement and maintain these information systems. It was, therefore, stated that awareness, training and education are the most important security measures that can address the human aspect of information security. This is because it is only by ensuring that employees understand the threats and vulnerabilities associated with the increasing use of information systems that organisations can begin to attempt to deal effectively with other security measures. Furthermore, in Subsection 3.4.3.3, participants argued that it would be beneficial for information security education to be provided by higher education institutions. This could save organisations on costs and time when it comes to educating their employees regarding information security.

In Section 3.5, it was argued that computing graduates entering organisations as employees have a responsibility towards securing organisational information systems and related information assets. It was further argued that it is vital that once computing graduates become organisational employees that they perform their roles and responsibilities within organisations in a secure manner. Furthermore, it was stated that it is ideal for higher education institutions to produce computing graduates who possess the required information security skills, knowledge and understanding. This could ultimately enable these computing graduates to become a stronger link in securing organisational information systems and related information assets from potential threats.

The aim of this chapter is to propose a framework to assist higher education institutions' computing departments and computing educators with ***"how"*** to pervasively integrate information security into undergraduate computing curricula.

A framework was found to be an appropriate method to solve this problem. Tomhave (2005) defines a framework as, *"a fundamental construct that defines assumptions, concepts, values, and practices and that includes guidance for **implementing** itself". He* further states that a framework is linked to demonstrable work. From the definition provided above, it can be argued that a framework is an appropriate method to use in solving an identified problem, as it provides the implementation guidance of ***"how"*** higher education institutions' computing departments and educators could pervasively integrate information security into undergraduate computing curricula.

The proposed framework is structured according to three phases, namely: Guideline development, planning and implementation. The guideline development phase aims to provide computing departments with an approach for the development of guidelines for the integration of information security into their computing curricula. Furthermore, the guideline development phase helps determine fundamental information security concepts to pervasively integrate into the computing department's undergraduate curriculum. The planning phase provides guidance to computing departments on planning for the pervasive integration of the identified information security concepts into their undergraduate computing curricula. The implementation phase aims to ensure that the fundamental information security concepts identified are pervasively integrated into various modules.

Section 6.2 presents the proposed information security education framework according to the above-mentioned three phases. To illustrate how the proposed framework can be implemented, Section 6.3 contextualises the proposed framework to an IT Department. Review cycle recommendations for the proposed framework are recommended in Section 6.4, while Section 6.5 concludes this chapter.

6.2. Proposed Information Security Education Framework

This section presents the proposed information security education framework in three phases, namely: Guideline development, planning and implementation. Each of the aforementioned phases is discussed in-depth in Subsections 6.2.1, 6.2.2 and 6.2.3, respectively.

6.2.1. Phase 1: Guideline Development

This subsection introduces the first phase of the proposed framework, the guideline development phase. It provides details of how the guideline development for pervasively integrating information security into various undergraduate computing curricula was modelled. To model this phase of the framework the key aspects shown in Table 6.1 were considered.

Key Aspects	Sections
Information Security	Section 3.3, Section 3.4, Section 4.4
Information Security Education Guidelines, Information Security Standards and Information Security Best Practices	Section 3.4, Section 4.4
Information Security Concepts	Section 4.4
Fundamental Information Security Concepts	Section 4.4
Computing Graduate Requirements	Section 4.3, Section 4.4
Learning Outcomes	Section 4.4

Table 6.1: Key Aspects for Modelling the Guideline Development Phase

As seen in Table 6.1, each key aspect has been discussed in sections in previous chapters. These considered key aspects as depicted in Table 6.1 are reiterated below.

Information Security

In Section 3.3, various definitions for information security were provided, one of which is the active protection of information systems and information assets from potential threats that can compromise the information's critical characteristics. Information security can be considered as the 'umbrella' concept that includes information systems and information assets. In Section 4.4, it was argued that information security should be taught to all undergraduate students in the Computer Science (CS), Information Systems (IS) and Information Technology (IT) computing disciplines. Information security is, therefore, considered an overarching discipline for the framework.

As information security education is important to undergraduate computing students, it is important to review the literature on information security education guidelines. In addition, information security standards and best practices could aid in determining information security concepts to be considered in the development of a computing curriculum.

Information Security Education Guidelines, Information Security Standards and Information Security Best Practices

In Section 4.4, the key role players such as the Association for Computing Machinery (ACM), the Association for Information Systems (AIS) and the Computer Society of the Institute of Electrical and Electronic Engineers (IEEE-CS) provided recommendations and guidelines for the development of computing curricula. These recommendations and guidelines recommended that information security must be taught as a pervasive theme. To identify the information security concepts that should be pervasively integrated, a literature review should be conducted to derive a list of information security concepts that could be integrated into computing curricula. Literature that can be used to derive information security concepts includes:

- Information Security Education Guidelines – These can include documents provided by the key role players that recommend and provide computing curricular guidelines for higher education institutions. An example of such a document would be the ACM/AIS/IEEE-CS;
- Information Security Standards – These can include documents that provide information security standards such as the International Organization for Standardization (ISO); and

- Information Security Best Practices – These can include reviewing literature pertaining to information security best practices such as those published by the National Institute of Standards and Technology (NIST).

From reviewing the literature regarding information security education guidelines, standards and best practices, one can identify information security concepts that are important to undergraduate computing students. An example of these information security concepts could be the critical characteristics of information which should be maintained in order to ensure the protection of information systems and related information assets as mentioned in Section 3.4.

Information Security Concepts

As stated in Section 4.4, the challenges that computing educators are facing regarding the integration of information security into computing curricula is that existing undergraduate computing curricula are over-extended and information security is a broad area of study. In Section 4.4, it was, therefore, argued that the pervasive integration of information security could allow students to focus on small pieces of information at a time, which could enable them to better assimilate knowledge as they will not be focusing on the entire scope and depth of information security at once. Furthermore, the pervasive integration allows for multiple modules to address information security as opposed to having an isolated information security module added to a curriculum that is already over-extended. Therefore, in order to pervasively integrate information security into undergraduate computing curricula, information security concepts need to be identified.

Pervasively integrating all information security concepts derived from the aforementioned literature could also prove to be challenging, as a department's curriculum may not be able to accommodate all the derived information security concepts as it may already be over-extended.

Fundamental Information Security Concepts

In order to address this challenge, this research proposes that the information security concepts be narrowed down to a manageable number by indicating which of the identified information security concepts are fundamental and should be pervasively integrated into the undergraduate computing curriculum within the department. This framework provides a starting point for computing departments that are not currently integrating information security into their undergraduate modules but would like to do so. By narrowing down the list of the identified information security concepts, a department could pervasively integrate the fundamental information security concepts that they deem to be a priority. After the department has pervasively integrated information security into their computing curriculum, the department could review their pervasive integration of information security after a period of time, for example, a year later, during which they could add or remove fundamental information security concepts as deemed necessary.

This research proposes for a department to elicit the perspectives of their computing educators to narrow down the list of the identified information security concepts to a list of the fundamental information security concepts. As stated in Section 4.4, this could be done through an investigation such as a discussion or a survey carried out amongst the computing educators. From conducting this investigation, a list of the identified fundamental information security concepts that should be pervasively integrated into various modules within a department could be derived.

Computing Graduate Requirements

In Section 4.3, Information Assurance and Security (IAS) is explicitly included in the CS and IT bodies of knowledge as a knowledge area. However, it is not explicitly included as a knowledge area in the IS body of knowledge although it is highlighted in the IS curricula guidelines and recommendations provided by the ACM/AIS. Relating to this, in Section 4.4, it was argued that it is important that information security is taught to all undergraduate students in the CS, IS and IT computing disciplines.

It was mentioned in Section 4.3 that computing graduates in the CS, IS and IT disciplines are required by industry to possess information security skills, knowledge and understanding.

Learning Outcomes

In Section 4.4, it was stated that each of the IAS knowledge units that come from the ACM/IEEE-CS contains a collection of information security concepts and each information security concept has learning outcomes associated with it. Table 6.2, provides an example of the learning outcomes for the *foundational concepts of security* knowledge unit according to the ACM/IEEE-CS (2013).

Concepts	Learning outcomes
1. CIA (Confidentiality, Integrity, Availability)	1. Analyse the trade-offs of balancing key security properties (Confidentiality, Integrity, and Availability). [Usage]

2. Concepts of risk, threats, vulnerabilities, and attack vectors (cross-reference Software Engineering/Software Project Management/Risk)	2. Describe the concepts of risk, threats, vulnerabilities and attack vectors (including the fact that there is no such thing as perfect security). [Familiarity]
3. Authentication and authorisation, access control (mandatory vs. discretionary)	3. Explain the concepts of authentication, authorisation, access control. [Familiarity]
4. Concept of trust and trustworthiness; Ethics (responsible disclosure). (cross-reference Social Issues and Professional Practice/Professional Ethics/Accountability, responsibility and liability)	4. Explain the concept of trust and trustworthiness. [Familiarity]; Describe important ethical issues to consider in computer security, including ethical issues associated with fixing or not fixing vulnerabilities and disclosing or not disclosing vulnerabilities. [Familiarity]

Table 6.2: Foundational Concepts in Security Learning Outcomes (ACM/IEEE - CS, 2013)

Familiarity and *usage* are desired levels of comprehension of the learning outcome as stated in Subsection 4.4.1. For example, relating to *usage*, as depicted in Table 6.2, after learning about *CIA*, an undergraduate computing student should be able to analyse the trade-offs of balancing the *CIA* of information and should be able to use or apply the fundamental information security concepts of *CIA*. Relating to *familiarity*, students should know and be able to understand the concepts of authentication, authorisation and access control as shown in Table 6.2.

In conclusion, computing graduate requirements and the fundamental information security concepts' learning outcomes could be used to get the "buy-in" of all stakeholders. This is to ensure that all the stakeholders in the department support the pervasive integration of information security into their undergraduate qualification's curriculum. The typical stakeholders in a higher education environment could include Directors of Schools, Heads of Department, Advisory Board Members and Computing Educators. The manner in which the "buy-in" of the stakeholders can be achieved is further explained in Subsection 6.2.2.

Based on the key aspects considered from Table 6.1, Figure 6.1 depicts an illustration of the first phase of the proposed framework.

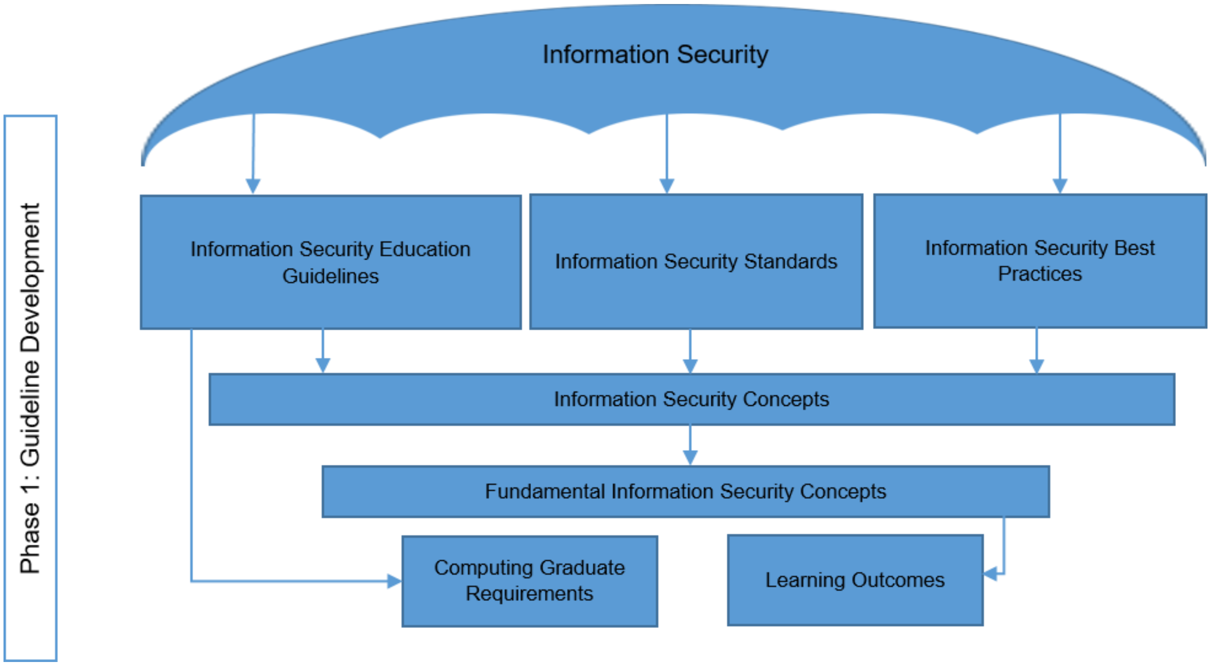
Phase 1: Guideline Development
Information Security
Information Security Education Guidelines
Information Security Standards
Information Security Best Practices
Information Security Concepts
Fundamental Information Security Concepts
Computing Graduate Requirements
Learning Outcomes

Figure 6.1: Phase 1 - Guideline Development

Information security is depicted as the overarching discipline of this framework. As information security should be pervasively integrated into the undergraduate curriculum, information security concepts should be derived. Figure 6.1 depicts that information security concepts could be derived from various literature sources such as information security education guideline documents, information security standards and information security best practices. The information security concepts derived from these literature documents may be too many to integrate into some departments where the curriculum is already over-extended. The department could, therefore, select those information security concepts that they deem fundamental to pervasively integrate them into their undergraduate curriculum. Computing graduate requirements and learning outcomes are all used during discussions or meetings with stakeholders to get their "buy-in" or support regarding the pervasive integration of information security into undergraduate computing curricula. These stakeholders include the Director of School, Head of Department and computing educators. Furthermore, computing graduate requirements and learning outcomes feed into the next phase of the proposed framework, which is the planning phase by providing the basis for the "buy-in" or support of all stakeholders.

In order for the guideline development phase to effectively integrated into computing curricula, top management support is required. Within a higher education context, top management could include Directors of School and Heads of Departments.

The following subsection introduces the planning phase of the proposed information security education framework.

6.2.2. Phase 2: Planning

This subsection provides details on how the planning phase for the pervasive integration of the identified fundamental information security concepts into a computing department's undergraduate curricula was modelled.

Table 6.3 depicts the key aspects that were considered for modelling this phase of the proposed framework. The design of the planning phase is based upon the need to gain "buy-in" of stakeholders through convincing them with regards to what industry requires of computing graduates, the corporate governance direct/control cycle illustrated in Chapter 3, Figure 3.2, as well as from the findings of the survey reported in Chapter 5.

Key Aspects	Sections
Industry requirements	Section 3.5, Section 4.1
The direct/control cycle	Section 3.5, Figure 3.2
Directive should come from top management to increase the willingness of computing educators to pervasively integrate information security	Survey, Table 5.6
Information security should be included in departmental plans	Survey, Table 5.5

Table 6.3: Key Aspects for Modelling the Planning Phase

As shown in Table 6.3, one of the key aspects that was considered for the modelling of the planning phase is industry requirements and this is discussed below.

Industry Requirements

As stated in Section 4.2, the key role players provide fully reviewed, revised and enhanced guidelines and recommendations for the development of undergraduate computing curricula every ten year, with a minor interim assessment at the fifth year mark. In reviewing, revising and enhancing undergraduate computing curricula, the key role players do consider the needs of industry in terms of the necessary information security knowledge, skills and understanding computing graduates are required to possess. According to Smith, Von Solms, Oosthuizen and Kritzinger (2005), it is necessary that computing departments incorporate the needs and requirements of industry when teaching information security. Findings from the study indicated that many higher education institutions were less focused on educating computing students on issues relevant to industry. These authors thus reached the conclusion that there is a need for incorporating the requirements of industry into computing education. Furthermore, the authors stated that information security education at higher education institutions should keep up with the information security requirements of industry.

It can be argued that there could be a gap as threats to information security and technology advance rapidly within a period of five to ten years, since the key role players review, revise and enhance undergraduate computing curricula guidelines and recommendations at these interims. As stated, the needs and requirements of industry when teaching information security could assist higher education institutions to keep up with industry requirements. These industry requirements can be used to review revise and enhance undergraduate computing curricula of various higher education institutions to ensure that they keep up with the information security needs of industry.

In addition to the fundamental information security concepts' learning outcomes and computing graduate requirements, what industry requires of computing students could also be used to get the "buy-in" of all stakeholders. The "buy-in" or support of the stakeholders defined in Subsection 6.2.1 can be achieved by holding a discussion or meeting with the stakeholders to get their "buy-in" regarding the pervasive integration of information security into their undergraduate computing curricula. These industry requirements could be obtained from a meeting held with the Advisory Board to determine what industry requires of computing graduates.

In Section 3.5, it was stated that computing graduates typically enter organisations at the operational level. These graduates are responsible for the design and development of organisational information systems, the maintenance of these systems and implementing the technological security measures that ensure the protection of the organisation's information assets from possible threats and threat agents. Furthermore, in Section 4.1, it was stated that the roles and responsibilities of computing graduates as organisational employees require them to possess information security skills, knowledge and understanding. Therefore, it is important for higher education institutions to stay abreast of the needs of industry and they should adapt their curricula accordingly. Additionally in Section 4.4, it was stated that computing departments should incorporate the needs and requirements of industry when teaching information security. One of the ways in which this can be done is through consultation with an industry Advisory Board.

The Direct/Control Cycle

In a higher education institution context, the Director of School would typically be at the strategic level within their department. As stated in Section 3.5, the strategic level provides directives to the tactical level, mandating what should be carried out. Furthermore, as depicted in Table 5.6, it was suggested that directives should come from top management. Therefore, it is important to note that the strategic level referred to in Chapter 3, Section 3.5 could be equivalent to top management that the participants of the survey referred to in Table 5.6. The directives given by the Director of School regarding the pervasive integration of information security within the department is received by the Head of Department who would typically be at the tactical level. As computing educators execute the day-to-day operations at higher education institutions by educating computing students, it can be argued that they would typically be at the operational level within the department as per the definition provided in Section 3.5. These computing educators would, therefore, receive the directive from their Head of Department mandating that they should pervasively integrate information security into their undergraduate modules.

Key Aspects from Survey

As shown in Table 5.5, it was suggested that information security be included in the departmental plan. This departmental plan could be formulated annually at a departmental course curriculum planning meeting. Without this departmental plan, it could be difficult for computing educators to pervasively integrate information security on their own. During this departmental course curriculum planning meeting, perspectives and challenges relating to the pervasive integration of information security into the department’s curricula can be addressed before the commencement of the academic year ahead. Furthermore, in Table 5.6, it is depicted that the directive for pervasively integrating information security should come from top management to increase the willingness of computing educators to pervasively integrate information security into their modules. In Subsection 5.2.4, it was stated that one of the challenges with pervasively integrating information security into undergraduate computing curricula is that some computing educators are resistant to change and that they need to be convinced about the importance of information security education in order to increase their willingness to integrate information security concepts into their modules. Such challenges can be addressed during the course curriculum planning meeting. This is important as the pervasive integration of information security into a computing department’s undergraduate curriculum should be supported by all stakeholders within the department.

It is important to note that the success of the pervasive integration of information security into undergraduate computing curricula is dependent on the planning phase. Proper planning is essential to ensure that all computing educators are aware of their roles regarding the pervasive integration of information security into the department’s undergraduate curriculum. Furthermore, proper planning is essential to ensure that the various fundamental information security concepts are integrated into the appropriate subject areas and relevant modules.

The second phase of the proposed framework is illustrated in Figure 6.2. The illustration of the figure is adapted from the corporate governance direct/control cycle. The figure depicts where a department’s Director of School, Head of Department and computing educators would typically fit into the corporate governance direct/control cycle.

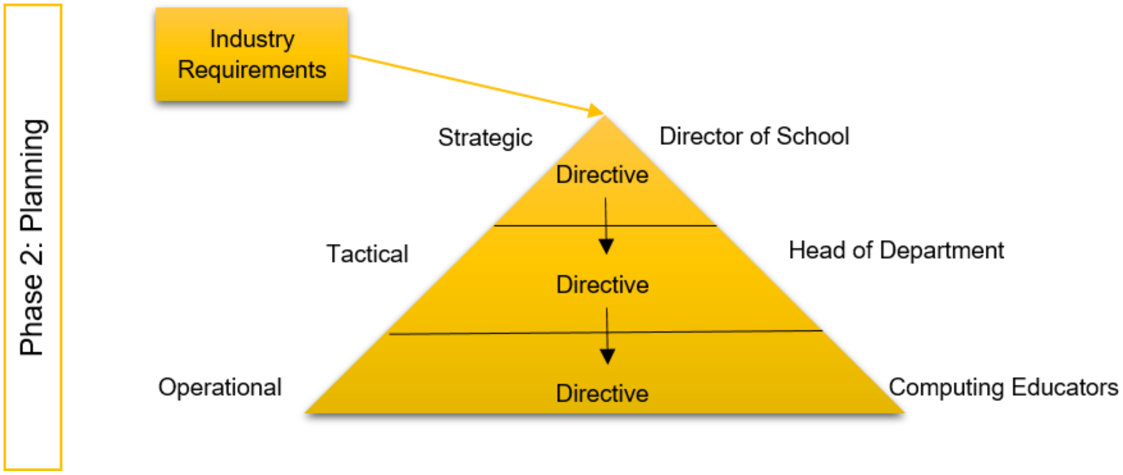

Figure 6.2: Phase 2 – Planning

Figure 6.2, shows that the industry requirements provide the basis for the computing department to move to the planning phase, the directive mandating what should be carried out by the computing educators at operational level is given by the Director of School at the strategic level. This directive is given to the computing educators by the Head of Department.

The following subsection presents the implementation phase which is the final phase of the proposed information security education framework.

6.2.3. Phase 3: Implementation

This phase aims to provide details on how the implementation phase for pervasively integrating fundamental information security concepts into various modules within a computing department was modelled. Table 6.4 depicts a summary of the key aspects that were considered in relation to how information security could be integrated into computing curricula.

Key Aspects	Section
Pervasive theme	Subsection 4.4.2, 4.4.4
Add information security concepts to existing modules approach and thread approach	Subsection 4.4.4
No single module can address the scope and depth of information security	Survey, Table 5.1
Information security should be pervasively integrated into undergraduate computing curricula	Survey, Table 5.1
Integrate information security concepts from the first year to the final year	Survey, Table 5.5
An information security concept should be covered in at least one of the undergraduate computing modules	Survey, Table 5.5
An information security concept should be covered by all modules	Survey, Table 5.5

Table 6.4: Key Aspects for Modelling the Implementation Phase

Pervasive Theme

In addition to IAS being defined as a knowledge area, in Section 4.4, IAS was also defined as a pervasive theme, meaning that it should be addressed multiple times, in multiple modules. It was stated that the overlap that exists with pervasive themes is not only necessary but valuable.

Approach for Integrating Information Security into Curricula

Section 4.4, discussed the "*add information security concepts to existing modules"* approach and the "*thread approach*". It was stated that this research supports both these approaches as they are similar to and support the pervasive theme. The "*add information security concepts to existing modules"* approach refers to adding information security concepts to various existing modules. Similarly, the "*thread approach"* can be used to integrate a theme into existing curriculum without drastically changing the core content of the module. Furthermore, the *"thread approach"* would require material on information security to be embedded into the current curriculum and therefore, does not require additional isolated information security modules.

Addressing the Scope and Depth of Information Security

Table 5.1 stated that due to the scope and depth of information security it cannot be addressed by a single module. Figure 6.3, therefore, depicts how information security can be integrated into a pervasive theme, which will allow for the scope and depth of information security to be addressed by multiple modules from a different perspective in each module.

Pervasively Integrated Information Security into Undergraduate Computing Curricula

Findings from the survey, in Table 5.1, show that participants indicated that information security should be pervasively integrated into undergraduate computing curricula. Furthermore, Table 5.1 shows that during the survey, participants stated that the pervasive integration of information security into multiple modules could demonstrate the omnipresence of information security. In Subsection 5.2.1 it was stated that this could show students that information security is not an isolated theme.

Occurrence of the Pervasive Integration of Information Security Concepts

In addition to information security being addressed multiple times in multiple classes, Table 5.5 shows that findings from the survey suggested that information security should be integrated into modules from the first year to the final year of study. Furthermore, it was suggested that information security concepts be grouped and taught together. An example that was provided was the grouping of confidentiality, integrity and availability (CIA). It was stated that this could show students how these concepts relate to one another. Furthermore, Table 5.5, shows that it was suggested that a concept should be integrated into at least one module while other participants suggested that information security concepts be taught in all modules. However, in Subsection 4.4.2, it was stated that a pervasive theme should be addressed multiple times, in multiple modules. Therefore, addressing an information security concept in one module would not be enough. This research proposes that information security be integrated multiple times, in multiple modules where information security can be related and contextualised in that particular module.

The third phase of the proposed framework is depicted in Figure 6.3. As previously stated, this figure shows that the fundamental information security concepts could be addressed multiple times in multiple subject areas by various modules within the subject areas.

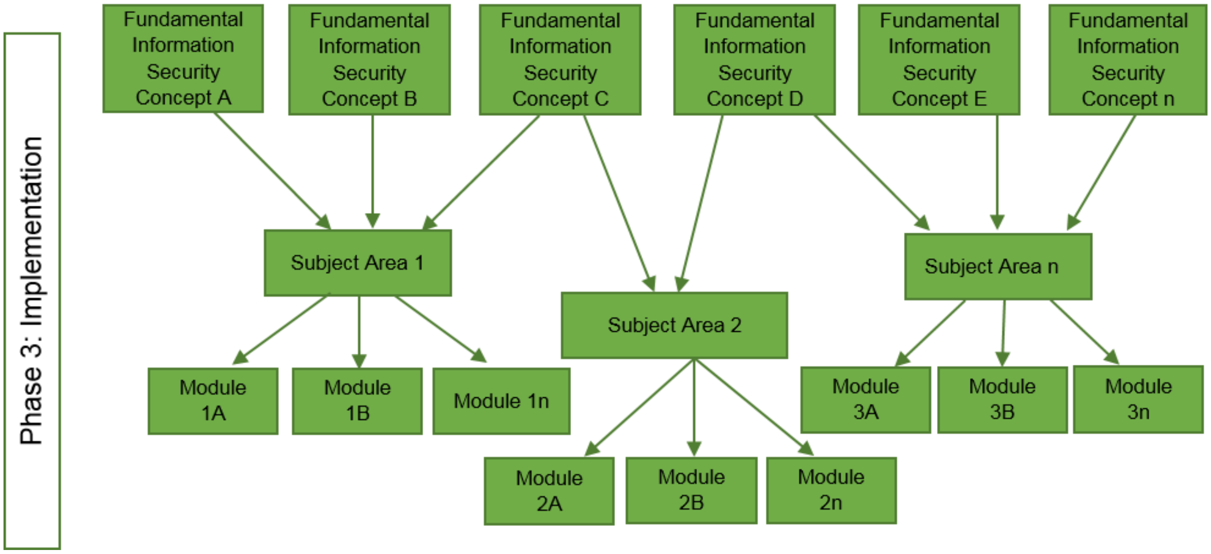
Phase 3: Implementation
Fundamental Information Security Concept A
Fundamental Information Security Concept B
Fundamental Information Security Concept C
Fundamental Information Security Concept D
Fundamental Information Security Concept E
Fundamental Information Security Concept n
Subject Area 1
Subject Area 2
Subject Area n
Module 1A
Module 1B
Module 1n
Module 2A
Module 2B
Module 2n
Module 3A
Module 3B
Module 3n

Figure 6.3: Phase 3 – Implementation

An example of how information security can be pervasively integrated into a department's curriculum is illustrated in Figure 6.3. For example, Subject Area 1 can integrate fundamental information security concepts A, B and C into the relevant modules within Subject Area 1. Fundamental information security concept A and B could be pervasively integrated into Subject Area 1's Module 1A, while Module 1B could pervasively integrate fundamental information security concepts A and C. Module n indicates that a Subject Area can have any number of modules, and within those modules, fundamental information security concepts can be integrated into the relevant modules. Furthermore, in Figure 6.3, for each of the fundamental information security concepts mapped with a specific subject area, it shows that a particular fundamental information security concept could be integrated into various modules within that specific subject area. The number of modules a fundamental information security concept can be integrated into in a specific subject area is only limited by the number of modules in that curriculum.

Figure 6.4 illustrates the complete proposed information security education framework. As shown in Figure 6.4, the guideline development phase of the proposed framework is connected to the planning phase. The arrows from the computing graduate requirements and learning outcomes to the planning phase connect these two phases. These arrows illustrate that the computing graduate requirements and the learning outcomes provide a basis for getting the "buy-in" of stakeholders at all levels in a department. In addition to this, industry requirements also provide the basis for getting the "buy-in" of all stakeholders at the planning phase. The planning phase and the implementation phase are connected using a curly bracket. The curly bracket illustrates that the planning phase contributes to the entire implementation phase, meaning that the “buy-in” at the planning phase influences how successful the implementation of the proposed framework is.

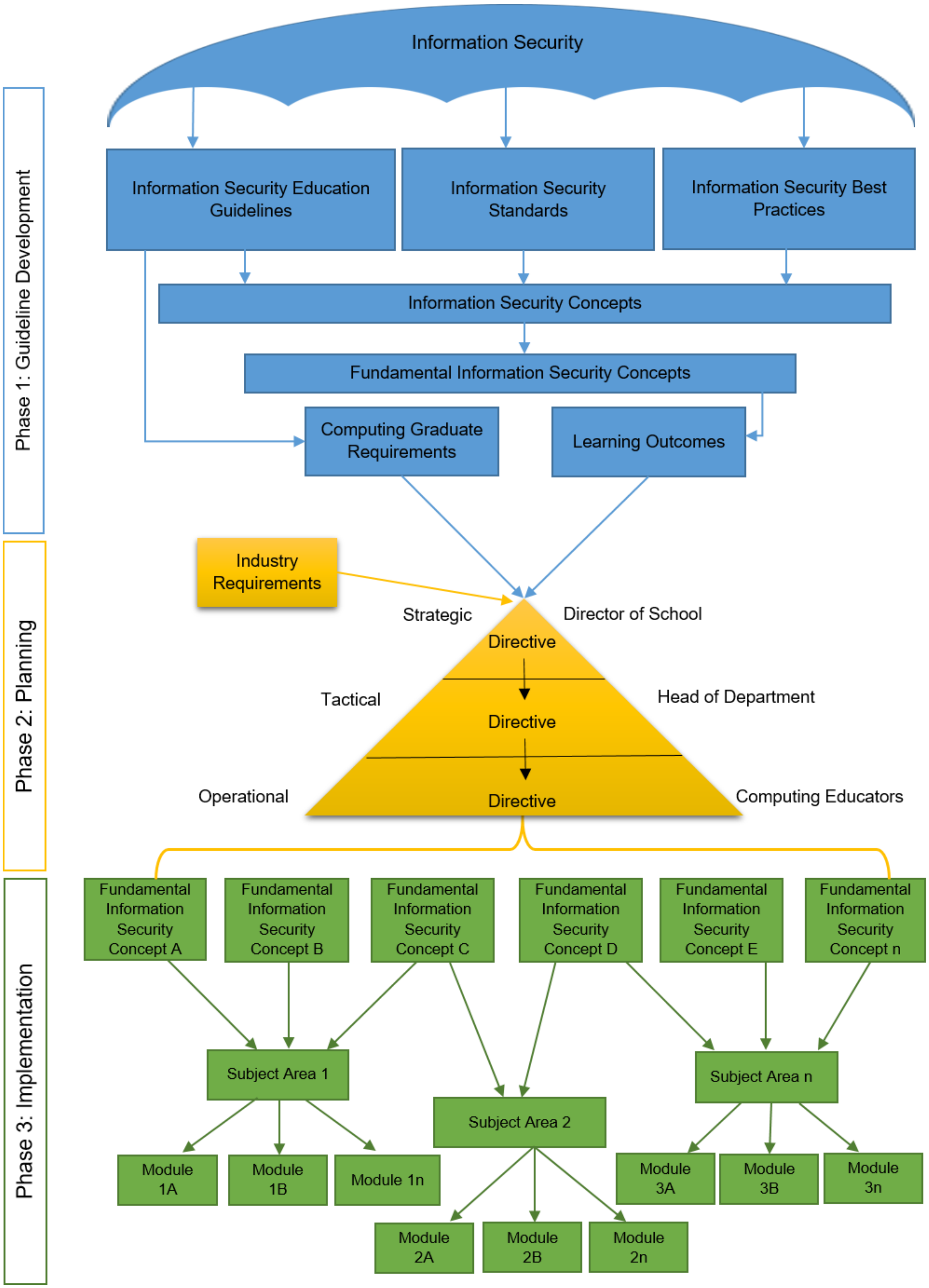
Information Security
Phase 1: Guideline Development
Information Security Education Guidelines
Information Security Standards
Information Security Best Practices
Information Security Concepts
Fundamental Information Security Concepts
Computing Graduate Requirements
Learning Outcomes
Phase 2: Planning
Industry Requirements
Strategic
Director of School
Directive
Tactical
Head of Department
Directive
Operational
Directive
Computing Educators
Phase 3: Implementation
Fundamental Information Security Concept A
Fundamental Information Security Concept B
Fundamental Information Security Concept C
Fundamental Information Security Concept D
Fundamental Information Security Concept E
Fundamental Information Security Concept n
Subject Area 1
Subject Area 2
Subject Area n
Module 1A
Module 1B
Module 1n
Module 2A
Module 2B
Module 2n
Module 3A
Module 3B
Module 3n

Figure 6.4: Proposed Information Security Education Framework

The successful implementation of this proposed framework by a higher education institution's computing department could ensure that information security is pervasively integrated into the undergraduate computing curricula.

Section 6.3 discusses how the proposed information security education framework could be contextualised and utilised by a computing department.

6.3. Contextualised Information Security Education Framework

It must be noted that the proposed framework discussed in Section 6.2 has not yet been implemented by any computing department to pervasively integrate information security into their curriculum. However, in this section, the proposed framework has been contextualised to demonstrate the potential implementation of the proposed framework by a fictional Information Technology (IT) Department.

6.3.1. Phase 1: Contextualised Guideline Development

There are many information security concepts that could be pervasively integrated into an IT Department's undergraduate modules, which could be derived from multiple literature sources. The particular IT Department used in this example has chosen to use the:

- '*Information Technology 2008, Curriculum Guidelines for Undergraduate Degree Programmes in Information Technology*' document (ACM/IEEE - CS, 2008b);
- '*Computer Science Curriculum 2013*' document (ACM/IEEE - CS, 2013);
- ISO Standards ((ISO/IEC 7498-2, 1989) security services; and
- Management of Information Security (Whitman & Mattord, 2014) textbook as it is prescribed to the Information Security module that is already offered within the IT Department's undergradaute qualification.

The above-mentioned literature was used by the IT Department to derive the information security concepts that are best suited for pervasively integrating into their department. From reviewing this literature, the information security concepts depicted in Chapter 4, Subsection 4.3.3 in Table 4.3 are used for this contextualisation as an example of those the IT Department deemed relevant and important to teach to undergraduate students within their department. The source(s) where the various information security concepts were derived are indicated in Table 4.3.

Table 4.3 shows that a number of similar information security concepts were derived from various sources.

The IT Department's stakeholders (Director of IT, Head of IT Department and the IT Educators) indicated that their IT qualification curriculum is already over-extended. The IT Department, therefore, decided to narrow down the list of information security concepts to a list that they deemed manageable for pervasively integrating into their curriculum. To narrow down the list of information security concepts depicted in Table 4.3, the IT Department held discussions with the department's IT Educators to determine which of the identified information security concepts they consider fundamental to their module(s).

Table 6.5 depicts a list of the fundamental information security concepts that were derived from the discussions held. It is important to note that this list is provided for demonstrative purposes only.

Fundamental Information Security Concepts	
1.	Authentication
2.	Secure Principles
3.	Security Awareness
4.	Confidentiality
5.	Integrity
6.	Availability
7.	Privacy
8.	Secure Software Development
9.	Backup and Recovery
10.	Legal and Ethical Behaviour Issues
11.	Security Threats
12.	Security Vulnerabilities

Table 6.5: Fundamental Information Security Concepts

To determine computing graduate requirements, the IT Department reviewed literature published by the key role players that provide the requirements that IT graduates should reflect. For example, the ACM/IEEE-CS stated that IT graduates should possess the skill sets that enable them to address IAS concerns. This clearly indicated that the IT Department should teach their IT students information security skills that will enable them to address IAS concerns.

The IT Department specifically indicated that the twelve information security concepts depicted in Table 6.5 were fundamental to their IT curriculum. Although the IT Department indicated these fundamental concepts shown in Table 6.5, for purposes of demonstrating how these fundamental concepts were integrated into the IT Department's curriculum, the fundamental concepts of *confidentiality, integrity* and *availability (CIA)* and *authentication will be used*.

The learning outcomes associated with the *CIA* and *authentication* concepts are as follows. After learning about the aforementioned fundamental information security concepts, undergraduate students in IT Departments should be able to demonstrate the learning outcomes of:

- Analysing the trade-offs of balancing key security properties (CIA); and
- Explaining the concepts of authentication.

The IT Department adopted these learning outcomes from the, '*Computer Science Curriculum 2013*' document (ACM/IEEE - CS, 2013), as the '*Information Technology 2008, Curriculum Guidelines for Undergraduate Degree Programmes in Information Technology*' document (ACM/IEEE - CS, 2008b) did not provide learning outcomes closely related to the fundamental information security concepts of *CIA* and *authentication*.

The computing graduate requirements and learning outcomes were used to gain the "buy-in" of the IT Department's stakeholders. Once the IT Department's stakeholder support had been gained, planning for the integration of information security into the IT Department's curricula followed.

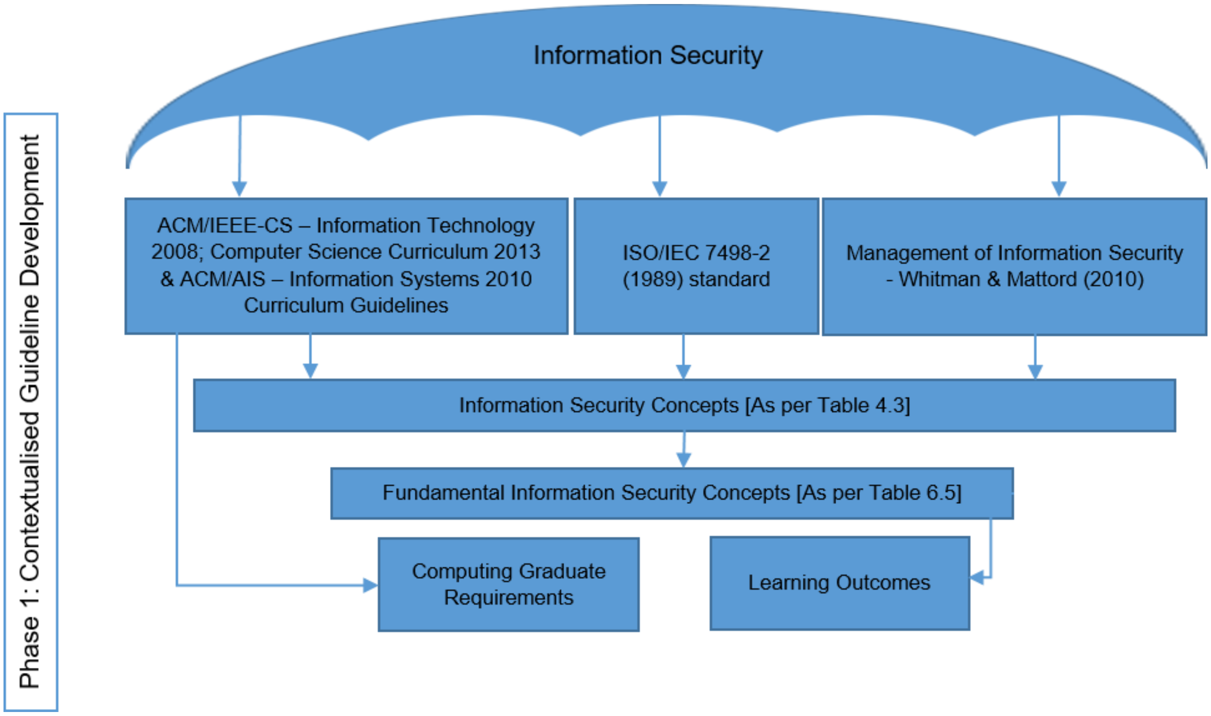
Phase 1: Contextualised Guideline Development
Information Security
ACM/IEEE-CS – Information Technology 2008; Computer Science Curriculum 2013 & ACM/AIS – Information Systems 2010 Curriculum Guidelines
ISO/IEC 7498-2 (1989) standard
Management of Information Security - Whitman & Mattord (2010)
Information Security Concepts [As per Table 4.3]
Fundamental Information Security Concepts [As per Table 6.5]
Computing Graduate Requirements
Learning Outcomes

Figure 6.5: Phase 1 - Contextualised IT Department Guideline Development

Figure 6.5 depicts the guideline development phase contextualised to the IT Department.

The following section contextualises the planning phase of how the IT Department could plan for the pervasive integration of information security into their undergraduate IT qualification, in order to ensure “buy-in” from all its stakeholders.

6.3.2. Phase 2: Contextualised Planning

To further gain the “buy-in” of the IT Department’s stakeholders, the IT Department held annual Advisory Board meetings with ICT industry representatives to elicit what industry requires of IT graduates. During this meeting, it was clearly indicated that industry requires IT graduates that possess information security skills, knowledge and understanding that could enable them to perform their organisational roles and responsibilities in a secure manner.

The Director of IT at the strategic level was responsible for giving directives to the Head of the IT Department mandating that the department should pervasively integrate information security into their undergraduate IT curriculum. Figure 6.6 illustrates that the Head of the IT Department, at the tactical level, was responsible for giving directives to the IT Educators at the operational level, mandating that educators should pervasively integrate information security into their undergraduate IT modules.

After directives indicating the responsibility of the various stakeholders within the IT Department, the Head of the IT Department invited an information security expert to give a presentation on the importance of information security as well as the importance of information security education to the department’s IT students. This was done to further get the “buy-in” of all stakeholders within the department, as this could ensure the successful integration of information security into their IT qualifications. The IT Department thereafter held a course curricula planning meeting before the commencement of the academic year to address any challenges or perspectives the IT Department’s educators held regarding the pervasive integration of information security into their modules.

Figure 6.6 depicts an illustration of the planning phase, as contextualised to the IT Department.

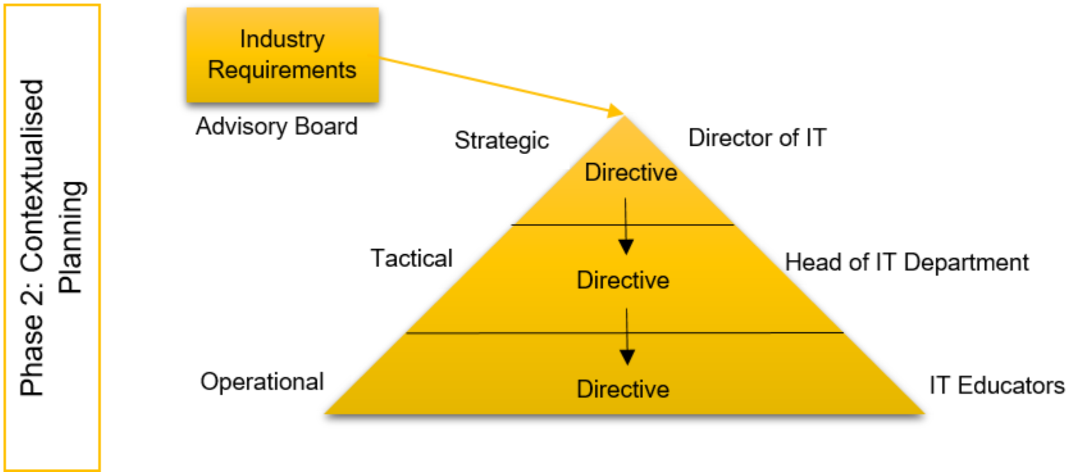

Figure 6.6: Phase 2 - Contextualised IT Department Planning

Figure 6.6 clearly depicts that the directive mandating that information security should be pervasively integrated into the IT Department's curriculum came from the Director of IT. This directive was given to the Head of the IT Department who had to give this directive to the department's IT Educators.

After the planning phase was completed, the next phase was the implementation phase to decide where in the IT Department's curriculum, the fundamental information security concepts would be integrated. This is discussed in the following section.

6.3.3. Phase 3: Contextualised Implementation

The implementation phase is contextualised to the IT Department's undergraduate IT qualification. Although the IT Department may have many subject areas, for the purpose of demonstrating how information security could pervasively be integrated into the IT Department's undergraduate IT qualification modules, three subject areas were chosen, namely: *Development Software*, *Information Systems* and *Networks*. These subject areas were chosen as they all have modules that are taught in each subject area and in each year throughout the department's undergraduate IT qualification, from first year to third year, as shown in Tables 6.6, 6.7 and 6.8.

Year	Module Name	Presented
1	Development Software 1	Year
2	Development Software 2	Year
3	Development Software 3A	Semester 1
3	Development Software 3B: Project	Year

Table 6.6: Development Software Subject Area Modules

Table 6.7 depicts the IT Department's undergraduate Development Software subject area modules.

Year	Module Name	Presented
1	Information Systems 1A	Year
1	Information Systems 1B	Year
2	Information Systems 2	Year
3	Information Systems 3A: System analysis and design	Semester 1
3	Information Systems 3B: Advanced design	Semester 2
3	Information Systems 3C: Project Management	Semester 1

Table 6.7: Information Systems Subject Area Modules

Table 6.7 depicts the modules in the Information Systems subject area that are taught at undergraduate level within the IT Department.

Year	Module Name	Presented
1	System Software 1: Networks	Year
2	Communication Networks 2A	Semester 1
2	Communication Networks 2B	Semester 2
3	Communication Networks 3A	Semester 1
3	Communication Networks 3B	Semester 2

Table 6.8: Networks Subject Area Modules

Table 6.8 depicts the IT Department's undergraduate Networks subject area modules.

Having identified the subject areas within the IT Department's undergraduate IT qualification, the IT Educators mapped the fundamental information security concepts that were identified as shown in Table 6.5 to the various subject areas within their department. For illustrative purposes, the example provided in this subsection will only focus on the mapping of the *authentication*, *secure principles*, *security awareness* and the *CIA* concepts. These fundamental information security concepts were mapped by IT Educators to subject areas where the fundamental information security concepts could be contextualised. This mapping is shown in Table 6.9.

		Subject Areas		
Fundamental information security concepts		Development Software	Information Systems	Networks
1.	Authentication	X	X	X
2.	Secure Principles	X	X	X
3.	Security Awareness	X	X	X
4.	CIA	X	X	X

Table 6.9: Mapping of Fundamental Information Security Concepts to Subject Areas

As shown in Table 6.9, the IT Educators mapped the fundamental information security concepts to all three subject areas, highlighting that these fundamental information security concepts are relevant to all subject areas. After mapping the fundamental information security concepts to the appropriate subject areas, the IT Educators that teach modules in the same subject area held a meeting to decide which fundamental information security concepts will be addressed by which module(s) within their particular subject area.

The IT Educators that teach modules in the Networks subject area indicated that the four fundamental information security concepts shown in Table 6.10 will be addressed by the modules indicated in Table 6.10.

		Subject Area: Networks				
Fundamental information security concepts		First year Networks (Systems Software 1: Networks)	Second year Networks module		Third year Networks module	
			(Networks 2A)	(Networks 2B)	(Networks 3A)	(Networks 3B)
1.	Authentication	X		X	X	X
2.	Secure Principles	X	X		X	X
3.	Security Awareness	X		X		X
4.	CIA	X	X	X	X	X

Table 6.10: Mapping of the Fundamental Information Security Concepts to Modules in Networks Subject Area

During the Networks subject area meeting that was held by the IT Network Educators, the following was agreed upon. IT Network Educators agreed that although the fundamental information security concepts of *CIA* were identified as separate they should be grouped and taught together as they cannot be taught in isolation of one another. The IT Network Educators further agreed that *all* the fundamental information security concepts as shown in Table 6.10 should be integrated into the theory of the first year *Systems Software 1: Networks* module. They indicated that the integration should focus on introducing the fundamental information security concepts to the IT students from a networks perspective. The IT Network Educators also agreed that the fundamental information security concepts of *secure principles* and *CIA* should be integrated into the theory of the *Networks 2A* module. Within the *Networks 2B* module, IT Network Educators decided that the fundamental information security concepts of *authentication, security awareness* and *CIA* should be discussed and used in a scenario to provide IT students with an understanding of the concepts, including how they can be applied in a practical example*.* Furthermore, the IT Network Educators decided that during the third year, in the *Networks 3A* and *Networks 3B* modules, IT students should be taught how to practically design and implement a network that incorporates all the fundamental information security concepts of *authentication, secure principles, security awareness* and *CIA*.

Similarly to the IT Network Educators, the IT Software Development Educators and IT Information Systems Educators that teach modules in their respective subject areas held a meeting to discuss which fundamental information security concepts should be addressed within their subject area. Furthermore, similarly to the IT Networks educators, the IT Educators within the Software Development and Information Systems subject areas discussed how they were going to pervasively integrate the fundamental information security concepts that were assigned to their subject area from the perspective of their modules.

Figure 6.7 depicts the implementation phase as contextualised to the IT Department. As explained in this subsection, the fundamental information security concepts shown in Table 6.9 are mapped against the Development Software, Information Systems and Networks subject areas that the IT Educators indicated they can be pervasively integrated into. Each subject area is mapped to all the modules that belong to the particular subject area.

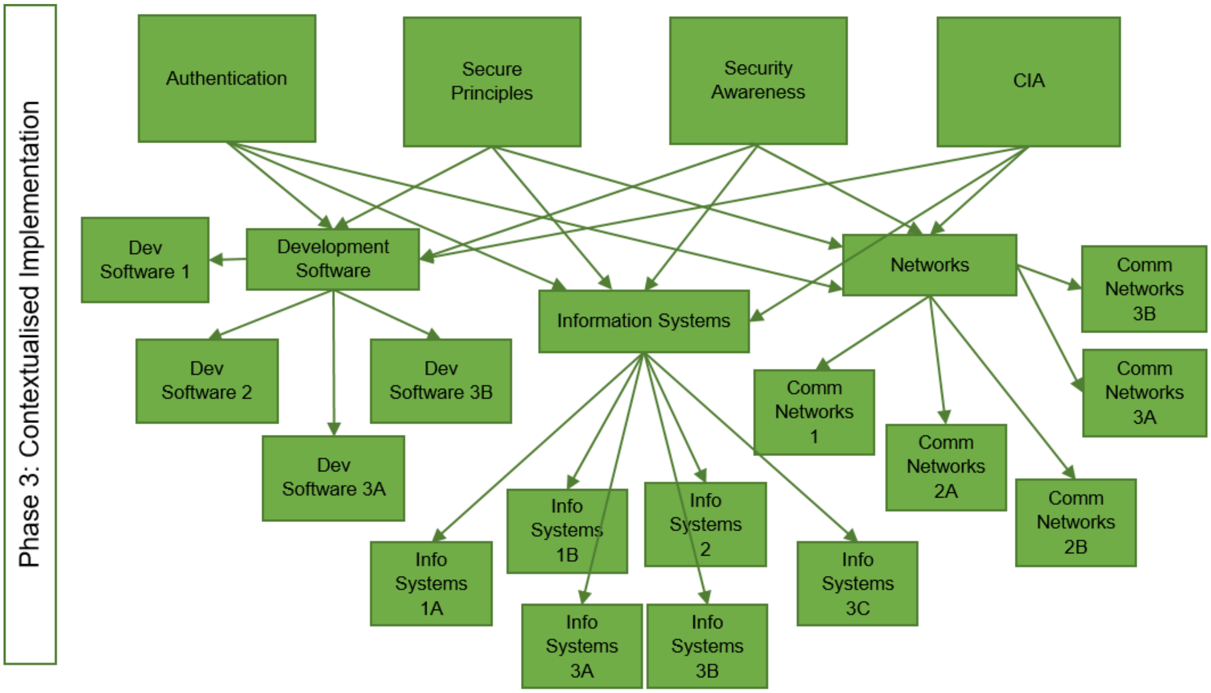

Figure 6.7: Phase 3 - Contextualised IT Department Implementation

A year after the IT Department pervasively integrated information security into their IT qualification’s modules, the IT Department held a course curricula planning meeting to review the pervasive integration of the fundamental information security concepts into various modules within their subject areas. This meeting was held to get feedback from the IT Educators, to determine whether they need to add or remove fundamental information security concepts from subject areas. During this meeting, the IT Department decided to readdress the fundamental information security concepts depicted in Table 6.5 that they had identified by identifying other information security concepts that are current and relevant to their subject areas and modules.

Figure 6.8, depicts the completed information security framework, contextualised to the IT Department.

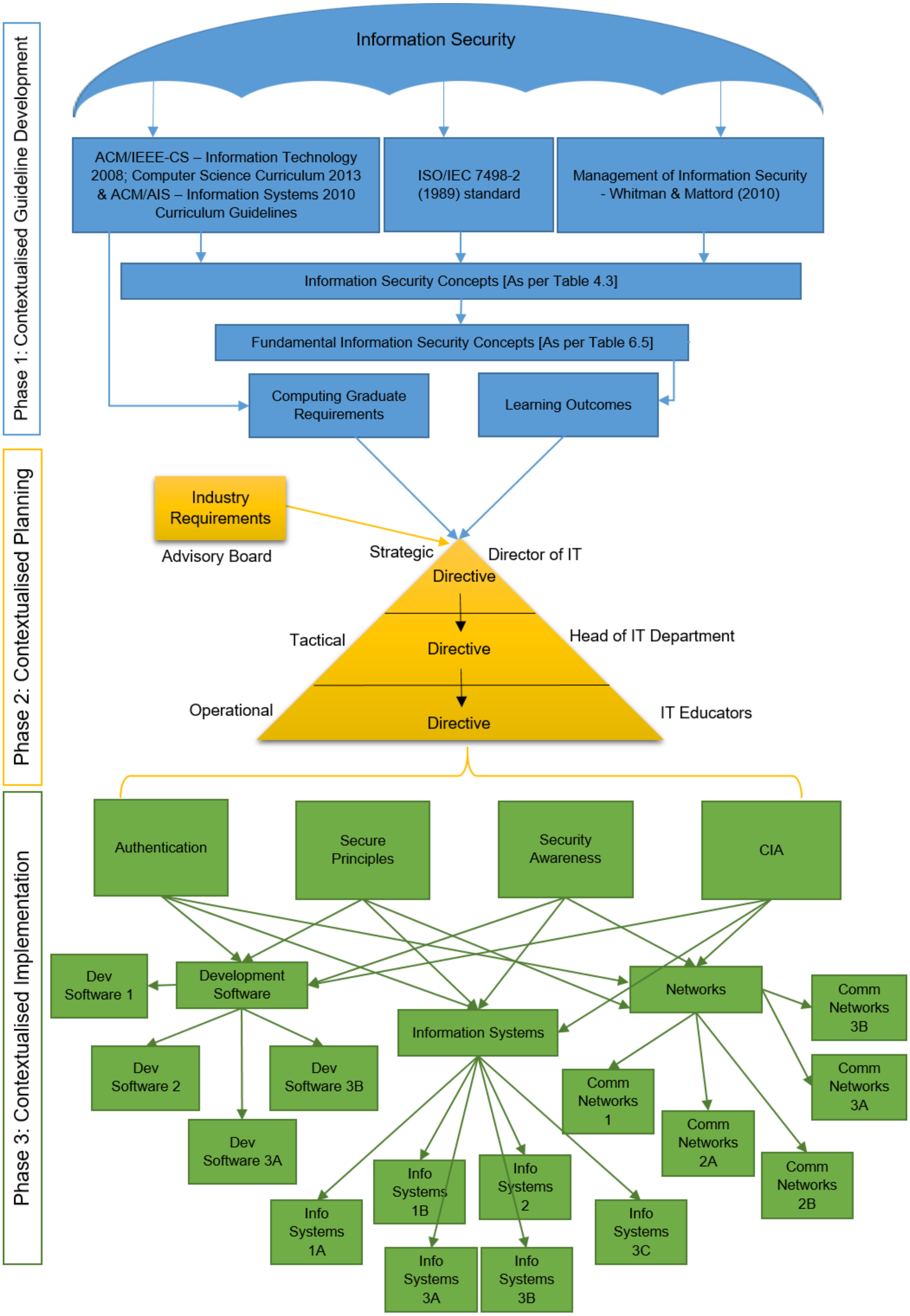

Figure 6.8: Information Security Education Framework Contextualised to an IT Department

Since Futcher et al. (2010) indicated that there is an evident “information security gap” that exists in undergraduate CS, IS and IT curricula at South African higher education institutions. It is hoped that the proposed information security education framework can be used as a good starting point for all these three computing departments (IT, CS and IS) that would like to pervasively integrate information security into their modules and not only for the IT Department. Furthermore, it is hoped that the proposed framework will add value to the integration of information security into computing departments.

6.4. Review Cycle for the Proposed Framework

More than a decade ago Smith, Von Solms, Oosthuizen and Kritzinger (2005) stated that the development of an information security education programme is an on-going process. They further advised for such a programme to be constantly revised to ensure that it remains relevant, up-to-date with international standards and practices and with industry expectations. This section, therefore, provides recommendations of how the proposed framework can be reviewed to ensure that it remains relevant, up-to-date with information security education guidelines, information security standards and information security best practices, as well as with the expectations of industry.

Figure 6.9 depicts the review cycle of the proposed information security education framework.

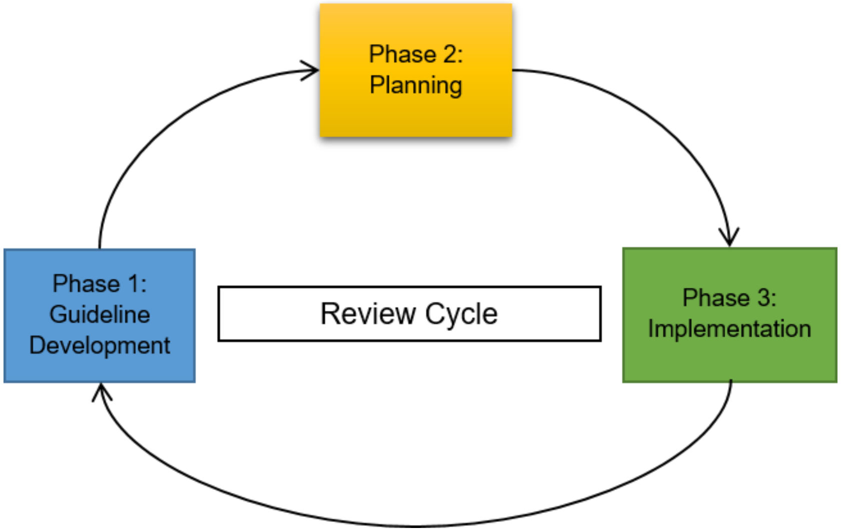

Figure 6.9: Proposed Information Security Education Framework Review Cycle

It is recommended that the pervasive integration of information security into the curriculum is revised periodically and that the different stakeholders are involved in the revision of the pervasive integration. Furthermore, it is recommended that these stakeholders could include the Director of School, Head of Department, Advisory Board members and the computing educators.

The proposed framework is dynamic; it is, therefore, recommended that proposed framework be reviewed as follows:

- Relevant and up-to-date documents should be surveyed to identify the relevant information security concepts
- The Advisory Board members should be consulted regarding the relevant requirements from industry with regards to computing graduate requirements
- The pervasive integration of the fundamental information security concepts should be reviewed to ensure that the relevant concepts are integrated into the appropriate subject areas and modules.

In conclusion, the pervasive integration of information security into a computing department's undergraduate curriculum should not be a once-off activity but it should be an ongoing cycle to ensure the relevance of the information security concepts that are pervasively integrated into the curriculum.

6.5. Conclusion

This chapter presented the proposed information security education framework. The framework was contextualised to provide an illustrative example of how the proposed framework can be contextualised in an IT Department.

The implementation of this information security education framework could ensure that a higher education institution's computing department produce undergraduate graduates who possess the required information security skills, knowledge and understanding to design, develop, implement and maintain organisational information systems. This could enable computing graduates to become a stronger link in securing organisational information systems and related information assets.

The following chapter validates the information security education framework that was proposed in this chapter.

Chapter 7 – Validation of Information Security Education Framework

This chapter provides the feedback that was obtained during the validation of the information security education framework which was proposed in Chapter 6. The framework was validated using elite interviews supported by a questionnaire.

7.1. Introduction

This research proposes a framework for ***the pervasive integration of information security into undergraduate computing curricula***. The proposed information security education framework consists of three phases, namely: Guideline development phase, planning phase and implementation phase. The implementation of the proposed information security education framework could enable computing departments to pervasively integrate information security into their various modules, thereby enabling computing graduates to become a stronger link in securing organisational information systems and related information assets. As stated in Chapter 1, Subsection 1.4.6, the proposed information security education framework was validated through the use of elite interviews, supported by a questionnaire.

Section 7.2 introduces the participants who acted as elites during the validation of the proposed framework, while Section 7.3 presents the manner in which the interviews were conducted. The feedback obtained during the validation of the proposed framework is provided in Section 7.4, while the discussion thereof is presented in Section 7.5. Section 7.6 provides the revised framework according to feedback provided by the elites and finally, this chapter concludes in Section 7.7.

7.2. Elite Participants

In Subsection 1.4.6, it was stated that the term "elite" is applied to a person or group of people that are generally considered to be important as they are typically seen to have knowledge, influence, control and power in a given setting or situation. Therefore, the six elites chosen were from an Information Technology (IT) department including a Director of School, Head of Department and various educators who held senior educator positions within the department. These participants who validated the proposed framework are considered elites as they have the necessary knowledge, influence, control and power within their department. Table 7.1 shows the elites who participated in the validation process. As shown in Table 7.1, **Elite 1** refers to Director of School and the Head of Department is referred to as **Elite 2**.

Elites	Position in Department
Elite 1	Director of School
Elite 2	Head of Department
Elite 3	Networks Educator
Elite 4	Information Systems Educator
Elite 5	Programming Educator
Elite 6	Programming Educator

Table 7.1: Position of Elites

The other four elites were educators; **Elite 3** focused on the Networks subject area, **Elite 4** focused on the Information Systems subject area, while both **Elite 5** and **Elite 6** focused on the Programming subject area as can be seen in Table 7.1. All elites were from the same IT Department.

7.3. Interview Process

As stated in Chapter 1, Subsection 1.4.6, the elite interviews were supported by a questionnaire. Different questions were posed to different elites. Although the validation questionnaires validated the entire framework, the set of questions posed at **Elites 1** and **2** focused primarily on the validation of the planning phase. Questions posed at **Elites 3**, **4**, **5** and **6** focused primarily on the validation of the implementation phase of the proposed framework. These questions can be found in Appendix C1. During the interview process, the researcher had the opportunity to probe for additional feedback based on the response provided by each elite.

7.4. Framework Validation Feedback

A few days before the elite interviews were conducted to validate the proposed framework, an interview brief was sent to all the elites. This brief was a four page document that contained background information on the elite interview that would be conducted, the research, as well as a figure depicting the proposed framework. The brief is provided in Appendix C2. This was to ensure that they understood what was expected of them as elite participants and to provide them with the basis of the research and an illustration of the proposed framework. On the day the elite interview was conducted, before the commencement of the interview, any questions the elite had with regards to the research or the proposed framework were answered as required. This was to further clarify the format of the interview, the background information regarding the research and the proposed framework.

The following subsections present the feedback provided by the elites.

7.4.1. Section 1: Perspectives on Information Security

Section 1 **aimed to elicit the elites' opinions regarding information security**. The questions in this section were posed to top management (**Elite 1**, the Director of School and **Elite 2**, the Head of Department).

Question 1.1: Do you regard information security as important?

Both **Elite 1** and **Elite 2** stated that they regard information security as important.

Additional Comments:

Elite 1 indicated that information security is a core aspect of being able to operate in the industry and therefore cannot be disregarded. **Elite 2** stated that information security is important from a number of aspects, such as in system development and computer networking.

Question 1.2: Is information security important to undergraduate students in your department? Please provide a reason for your response.

Both **Elites 1** and **2** indicated that information security is important to undergraduate students in their department. **Elite 1** stated that in most cases, information security is implemented as an afterthought. However, information security is a core aspect of information systems, more especially in today's technological world. **Elite 1** specifically indicated that, "If technical skills and information security are not taught together, the undergraduate students will also understand information security as an afterthought". **Elite 2** indicated that there are two streams (Support Services (SS) and Communication Networks (CN)) within the department's undergraduate IT qualification where information security is "integrated". **Elite 2** further indicated that the department is aware that information security still needs to be integrated into the Software Development (SD) stream's curriculum. In addition, **Elite 2** stated that the department hopes that the integration of information security can be done through the SD third year project, but they also need to look at ways to make it more formal at the SD stream's undergraduate level. Furthermore, **Elite 2** stated that undergraduate IT students should be aware of threats to information security and the need to implement information security in their information systems.

Addressing Feedback

Although **Elite 2** indicated that information security is integrated into the SS and CN streams through the Support Services module, it must be noted that this module is not pervasive. It is a single isolated module that is taught to students in the SS and CN streams, however, students in the SD stream are not taught this module.

Question 1.3: Should information security be taught as a single module or should it be pervasively integrated into various modules in the IT qualification? Please provide a reason for your response.

Elite 1 stated that there should be a single module where all the theory of the information security concepts is taught. The application thereof should then be split across various modules. **Elite 2** indicated that information security can be a section or a chapter within a module, it does not have to be a module dedicated to information security. There are various modules that information security can be integrated into. For the SD stream, it should be integrated into an already existing module, while the SS and CN streams already have a module dedicated to teaching information security.

Addressing Feedback

As previously stated, it is important to note that there is no evidence of the pervasive integration of information security within the IT department, although the Support Services module provides an introduction to information security.

Question 1.4: Would the pervasive integration of information security into undergraduate curricula within the department benefit students?

Both **Elite 1** and **Elite 2** indicated that the pervasive integration of information security into undergraduate computing curricula would benefit students. **Elite 1** stated that rather than students learning about information security in one module and never learning about it again, if it is pervasively integrated into several modules, students would encounter information security in multiple modules. Pervasively integrating information security rather than teaching it in a single module would ensure that it is reinforced through other modules from varying perspectives. **Elite 2** indicated that the pervasive integration would allow students to learn about the theory in class and they would get to understand the reasons and methods for applying it through practical experience.

7.4.2. Section 2: Perceived Challenges

Section 2 **aimed to determine the perceived challenges regarding the pervasive integration of information security**. This section aimed to determine the perceived challenges from both top management (**Elites 1** and **2**) and the IT Department's computing educators (**Elites 3**, **4**, **5** and **6**).

Question 2.1: What challenges within your **department** would make the pervasive integration of information security difficult?

Elite 1 indicated that one of the challenges would be that there is currently no information security knowledge base for computing educators to refer to. Such a knowledge base could be created by contributions made by each computing educator. **Elite 1** further indicated that students often struggle to make a connection between topics, leaving computing educators with a gap of knowledge to fill, before they can teach new work. **Elite 2** indicated that a challenge with the change of curriculum is that there would be a lot of administrative work to change a module or the structure thereof. New material would have to be researched and included in particular sections within the course material.

Question 2.2: Do you foresee any challenges with pervasively integrating fundamental information security concepts into your **module(s)**? Please provide a reason for your answer.

Elite 3 stated that time is a challenge and further indicated that the implementation of the proposed framework also depends on the expertise of the computing educators. This is because some computing educators may not understand or be interested in information security. Similarly, **Elite 4** indicated that she foresees a challenge relating to an educator's knowledge of information security as it could limit their ability to teach information security or their ability to integrate it into their module. **Elite 5** stated that the challenge he foresees would be deciding which of the fundamental information security concepts should be addressed in which subject area, as there is an overlap in subject areas. **Elite 6** indicated that the challenge he foresees is the unintended repetition relating to what is taught in each module. One educator might unknowingly teach what has already been covered by another educator in another module.

Addressing Feedback:

Unintended repetition could be prevented by having a subject area meeting to determine which modules within the subject area will address each fundamental information security concept and from which perspective. This is to ensure that all computing educators are aware of how the other modules within their subject area will address the identified concepts. As seen in Chapter 6, Subsection 6.3.3, this has already been taken into consideration.

Question 2.3: What measures can be put in place to overcome the challenges stated in *Question 2.2*, if you answered yes?

Elite 3 stated that a measure that can be put into place to overcome the challenge associated with lack of time is to include an incentive that educators could get for the extra work they would put in when integrating fundamental information security concepts into their modules. **Elite 4** indicated that communication would be important to overcome educators' lack of information security knowledge. This communication would need to be done regularly about changes in technology and about what must be updated or included relating to current trends and how technology is evolving. As already mentioned, **Elite 5** stated that the challenge he foresees would be deciding which of the fundamental information security concepts should be addressed in which subject area, as there is an overlap in subject areas. However, **Elite 5** did not provide a measure to address the challenge he foresaw. **Elite 6** indicated that the development of a common information security concepts knowledge base where each computing educator can see which fundamental information security concept has been covered is essential. This could be a website within the department, where there are references to show which of the fundamental information security concepts have been taught, the level at which they were taught and the module. There could be listings of the various subject areas with an indication of which concepts fit in a particular subject area and if there are abstract concepts it can help establish a connection. Furthermore, this could also ensure that computing students see how the fundamental information security concepts relate to one another as well as how they relate to various subject areas and modules.

Addressing Feedback:

Although **Elite 5** did not provide a measure, the challenge he foresaw has already been addressed in Chapter 6, Subsection 6.2.2 where it was stated that proper planning is essential to ensure that the various fundamental information security concepts are integrated into the appropriate subject areas.

Additional Comments:

Elite 5 further indicated that the awareness of information security should be included to educate students on why information security is taught, as it is important from a first year level of study. The first year of the undergraduate computing curriculum provides a very wide perspective on topics making it difficult to go into detail.

7.4.3. Section 3: Proposed Framework

Section 3 **aimed to verify the feasibility of the proposed information security education framework**. Questions regarding the feasibility of the proposed framework section were posed at both top management (**Elites 1** and **2**) and the department's computing educators (**Elites 3**, **4**, **5** and **6**).

Question 3.1: Has the department had a formal or informal discussion about information security?

Both **Elite 1** and **Elite 2** indicated that the department has held an informal discussion regarding information security.

Additional Comments:

Elite 1 stated that during the informal discussion, a decision was taken to incorporate information security into some of the IT undergraduate qualification's modules, within the department. **Elite 1** further stated that information security is also specifically taught in one of the undergraduate qualification modules, which is a theoretical module; however, it is not reinforced in other modules.

Elite 2, elaborating on **Elite 1's** comment, added that information security has been integrated in the second year SS and third year CN streams. However, it is absent in the SD stream's curriculum as it is overloaded, but it is still necessary for information security to be included in the SD curriculum. **Elite 2** further indicated that an information security module is offered at the Bachelor of Technology (BTech) level.

Addressing Feedback:

Elite 2 stated that within the department, information security is addressed at the BTech level of study. However, it is important to note that not all computing students proceed to this level where information security is taught as an elective. This is due to the fact that upon completing their undergraduate IT qualification, students have the option to exit the higher education institution without proceeding to the BTech level.

Question 3.2: Do the educators within your department have information security knowledge that will enable them to pervasively integrate the fundamental information security concepts into their various modules?

Both **Elite 1** and **Elite 2** indicated that educators within their department have information security knowledge that will enable them to pervasively integrate information security into their various modules.

Additional Comments:

Elite 1 indicated that the 12 identified fundamental information security concepts are rather basic and that all computing educators within the department possess information security knowledge, as they have all completed some form of postgraduate studies.

Elite 2 stated that if computing educators do not possess information security knowledge they will have to develop their skills to accommodate the need to pervasively integrate information security into their module.

Question 3.3: Do you (Director of the School or Head of Department) support the integration of information security into various modules within your department?

Both **Elite 1** and **Elite 2** indicated that they support the pervasive integration of information security into various modules within the department.

Additional Comments:

Elite 1 further stated that students' understanding of information security will be reinforced in various modules if information security is pervasively integrated. **Elite 2** stated that there should be a module dedicated to teaching the basic concepts of information security. These information security concepts should thereafter be reinforced in other modules.

Question 3.4: Would the proposed framework be feasible within your **department**?

Both **Elite 1** and **Elite 2** indicated that the proposed framework is feasible for integrating information security into various modules within their department.

Additional Comments:

Elite 1 commented on the appearance of the framework and the procedure the department would need to follow in order to add information security into the educational programmes. **Elite 1** said that the directive and the "buy-in" must feature at the top level of management, which is also represented at the strategic and tactical levels of the planning phase. The direct/control cycle represented in Chapter 6, Figure 6.2 should be changed to represent the subject area specialist below the computing educators who are depicted at the operational level. Firstly, the directive is issued, followed by a departmental meeting and thereafter a specific subject area meeting is held.

Question 3.5: In your opinion, would the framework be feasible for integrating information security into your **module**? Please elaborate on why you think it would or would not be feasible.

All four computing educator elites indicated that the framework is feasible. **Elite 3** elaborated stating that the only problem is that most of the curriculum is already full. **Elite 4** mentioned that the framework appears to be "plug and play" compatible and that if steps are provided on how to implement the framework then it should be easy to implement. **Elite 5** indicated that the framework is feasible, as it considers what computing graduates going into the industry are required to know as well as many relevant information security issues which will be important for computing graduates to know. **Elite 6** stated that the proposed framework is feasible as it includes principles that touch on relevant information security concepts. This is important, as computing students should leave higher education institutions with an information security mindset. With this mindset, computing students could potentially consider information security when working on information systems. This is particularly important because information security plays an important role in every technological system. Additionally, **Elite 6** indicated that he finds the design of the framework pleasing, in that it begins with top management involvement and moves down to the subject areas in which the various fundamental information security concepts should be addressed.

Question 3.6: If answered no in *Question 3.5*, would this framework be feasible for integrating information security into other modules that you do not teach?

All four elites stated in *Question 3.5* that the framework would be feasible for integrating information security into their module, therefore, this question became invalid.

Question 3.7: In your opinion, does this framework need improvements?

Elite 3 and Elite 4 indicated that the framework needs no improvements, while **Elite 5** indicated that this cannot be answered without further thought and consideration. **Elite 6**, however, indicated that the framework does need improvements.

Additional Comments:

Elite 5 indicated that guidelines are given on how to use the framework, however, the biggest challenge is choosing which fundamental information security concepts fit in which subject area.

Question 3.8: If you answered yes to *Question 3.7*, please state how the framework can be improved.

Elite 6 stated that learning outcomes could be included for each fundamental information security concept, to make it easier and more understandable. This will allow linking outcomes to a single specific subject area. In the actual diagram, **Elite 6** suggested that arrows leading to each fundamental information security concept be included to show that the departmental course curricula planning feeds into each fundamental information security concept.

7.4.4. Section 4: Implementation of Proposed Framework

Section 4 **aimed to determine how the computing educator elites would implement the fundamental information security concepts into their modules**. The questions within this section were only posed at the elites who are computing educators (**Elites 3**, **4**, **5** and **6**) within the department where the proposed framework was validated.

The first question within this section determined the subject area in which the computing educator elites teach.

Question 4.1: In which subject area do you teach?	
Elite 3	Networks
Elite 4	Information Systems
Elite 5	Programming
Elite 6	Programming

Table 7.2: Question 4.1 Responses

Table 7.2 shows the subject areas of the four computing educators who participated as elites in the validation of the proposed framework.

The elites were asked to indicate the fundamental information security concepts that could be pervasively integrated into their modules.

Question 4.2: Please select all fundamental information security concepts that could be pervasively integrated into module(s) within your subject area.					
Fundamental information security concepts		**Elite 3**	**Elite 4**	**Elite 5**	**Elite 6**
1.	Authentication	X	X	X	X
2.	Secure Principles	X	X	X	X
3.	Security Awareness		X	X	X
4.	Confidentiality	X	X	X	X
5.	Integrity	X	X	X	X
6.	Availability	X		X	X
7.	Privacy	X		X	X
8.	Secure Software Development			X	X
9.	Backup and Recovery		X	X	X
10.	*Legal and Ethical Behaviour Issues*				
11.	Security Threats	X		X	X
12.	Security Vulnerabilities	X		X	X

Table 7.3: Question 4.2 Responses

Table 7.3 shows the fundamental information security concepts that the four elites indicated could be pervasively integrated into their module(s). As can be seen, none of the elites indicated that legal and ethical behaviour issues can be pervasively integrated into modules within their subject area. This is a concern, as all computing students should understand legal and ethical behaviour.

Question 4.3: Please provide an example of how one of the concepts that you selected in Question 4.2 can be pervasively integrated into one of your modules.

Elite 3 stated that security is officially part of his Networks' module. He further indicated that his Networks module is currently integrating the fundamental information security concepts of *confidentiality, integrity* and *authentication* through the topic of IPsec Virtual Private Network (VPN) tunnels. **Elite 4** indicated that she would teach the fundamental information security concepts of *authentication* in the theory class at second year level. This includes teaching the students about the different user roles which can be used to show that not all users should be allowed to see the same data, have the privileges to change data or to delete data. Authentication can also be taught with *integrity*, looking at which users possess the privileges to change/update data in the database, according to their role and authorisation. This theory can then be implemented in the third year software development project which is a capstone project offered during the final year of the 3 year qualification. **Elite 5** would teach the fundamental information security concepts of *confidentiality* and *authentication* in theory and would thereafter expect the students to practically apply these concepts by designing a web application with the applicable security features. **Elite 6** indicated that they would integrate the fundamental information security concept of *secure principles* by teaching the students theory relating to common security concerns in software system development. This would include; teaching the students what to be aware of, the various security considerations a software developer should take into account when selecting specific system controls, and the consequences of neglecting to address the vulnerabilities of such a control.

7.5. Framework Validation Feedback Discussion

Some of the challenges identified by the elites are similar to those identified and discussed in Chapter 5 and the solution, in Chapter 6. One of these challenges is time. However, it was further stated that to overcome the challenge associated with lack of time, could get an incentive for the extra work they would put in when integrating fundamental information security concepts into their modules. This, however, may not always be feasible in an academic environment. This further highlights the need to get the "buy-in" of all stakeholders within the department in order to ensure the pervasive integration of information security into various modules. It was indicated that a challenge with implementing the proposed framework is that the change of curriculum could result in additional administrative work. It is important to note that with the pervasive integration of the proposed framework, information security is integrated into the existing curriculum and it does not vastly change the existing curriculum. This is one of the benefits provided by the thread approach, where a theme such as information security can be integrated into the curriculum without drastically changing the core content of the module. Relating to one of the challenges that was indicated, an information security concept knowledge base could prove to be helpful for both the computing educators to know what will be addressed in each module and for the computing students to be able to explicitly see the connection between the fundamental information security concepts as they are taught and implemented in various modules.

The fundamental information security concepts that were identified through the survey reported on in Chapter 5 were used in the validation process. It is clear from the feedback provided by the elites who are computing educators that although the fundamental information security concepts they selected to integrate could occur in various modules, they would be addressed from a different perspective in each module. This highlights the significance of the pervasive integration of information security as this could demonstrate the omnipresence of information security to computing students.

Based on the feedback provided from the validation of the proposed framework, it can be concluded that the proposed framework was generally accepted as a viable way for computing departments to pervasively integrate fundamental information security concepts into their curricula.

The following subsection provides the revised framework and it restates the improvements that were recommended by the elites.

7.6. Revised Information Security Education Framework

Based on the feedback received from the elites who validated the proposed framework, it is clear that all the elites found the proposed framework feasible for pervasively integrating information security into undergraduate computing curricula.

7.6.1. Proposed Change 1

However, the participants proposed that the planning phase be changed to reflect the subject area specialist below the computing educators who are depicted at the operational level. In addition, it was suggested that the direct/control cycle be changed to reflect the subject area specialist at the bottom. The recommended change is depicted in Figure 7.1.

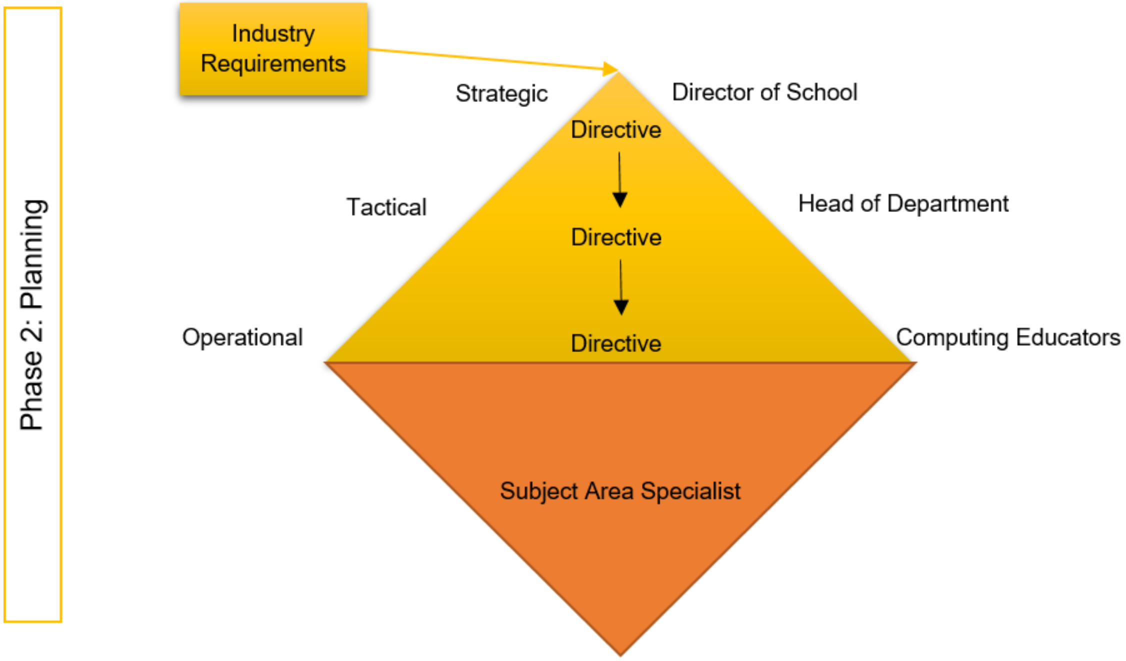

Figure 7.1: Proposed Change 1

The assistance of a subject area specialist within each subject area could assist the computing educators that teach modules within the subject area with how they could integrate various fundamental information security concepts into their modules. The subject area specialist could also ensure that the appropriate fundamental information security concepts are addressed in the appropriate module(s).

Although the suggested change was considered, the change was carried out in the implementation phase of the proposed framework, as can be seen in Figure 7.2. This is due to the fact that the recommendation highlighted the need for a subject area specialist who can map fundamental information security concepts to the appropriate modules, within the specific subject area. This is to show that it is the duty of the subject area specialist to indicate which fundamental information security concepts should be integrated into which module.

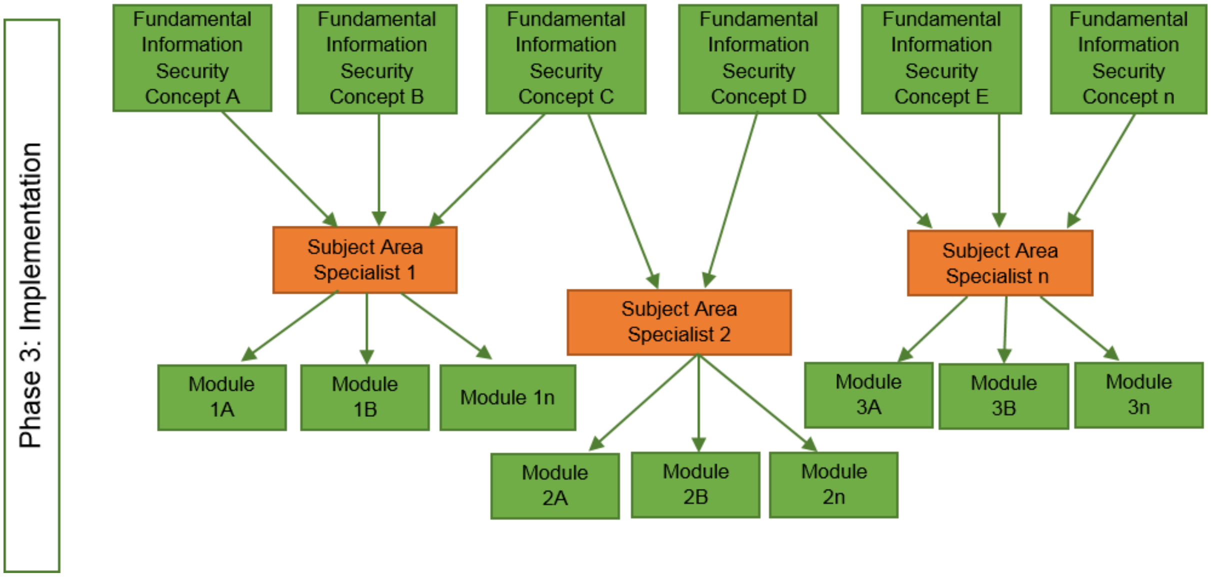
Phase 3: Implementation
Fundamental Information Security Concept A
Fundamental Information Security Concept B
Fundamental Information Security Concept C
Fundamental Information Security Concept D
Fundamental Information Security Concept E
Fundamental Information Security Concept n
Subject Area Specialist 1
Subject Area Specialist 2
Subject Area Specialist n
Module 1A
Module 1B
Module 1n
Module 2A
Module 2B
Module 2n
Module 3A
Module 3B
Module 3n

Figure 7.2: Implementation of Proposed Change 1

Figure 7.2 shows that during the subject area meeting that was recommended, the subject area specialist should indicate which fundamental information security concepts are appropriate to be integrated into which modules within their subject area. To clearly show the change that was implemented, the subject area specialists are depicted in orange in Figure 7.2.

7.6.2. Proposed Change 2

A further recommendation was provided in Subsection 7.4.3, that there should be arrows from the bottom of the planning phase, which is the operational level, linking to each of the fundamental information security concepts. Arrows leading to each fundamental information security concept are necessary to show that the departmental course curricula planning feeds into each fundamental information security concept. This recommendation was considered and it is depicted in Figure 7.3.

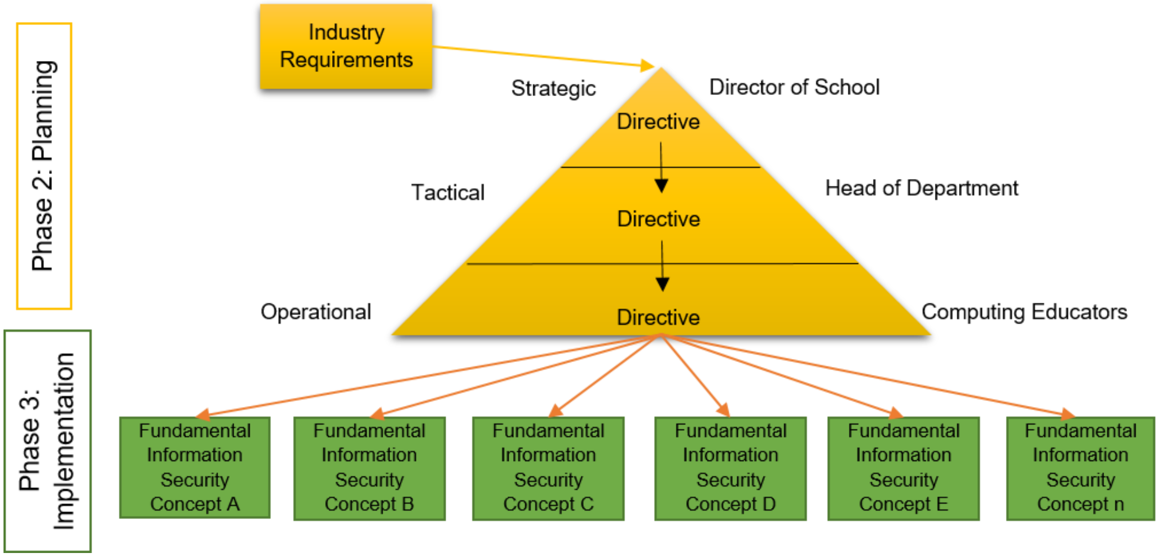
Phase 2: Planning
Phase 3: Implementation
Industry Requirements
Strategic
Director of School
Directive
Tactical
Head of Department
Directive
Operational
Computing Educators
Directive
Fundamental Information Security Concept A
Fundamental Information Security Concept B
Fundamental Information Security Concept C
Fundamental Information Security Concept D
Fundamental Information Security Concept E
Fundamental Information Security Concept n

Figure 7.3: Implementation of Proposed Change 2

Figure 7.3 depicts the change that was carried out regarding the recommendation that was provided, similarly to that change depicted in Figure 7.2, the change is depicted in orange.

Considering the recommendations that were provided by these elites, the changes were applied to the proposed information security education framework and are depicted in Figure 7.4. These changes are highlighted in orange.

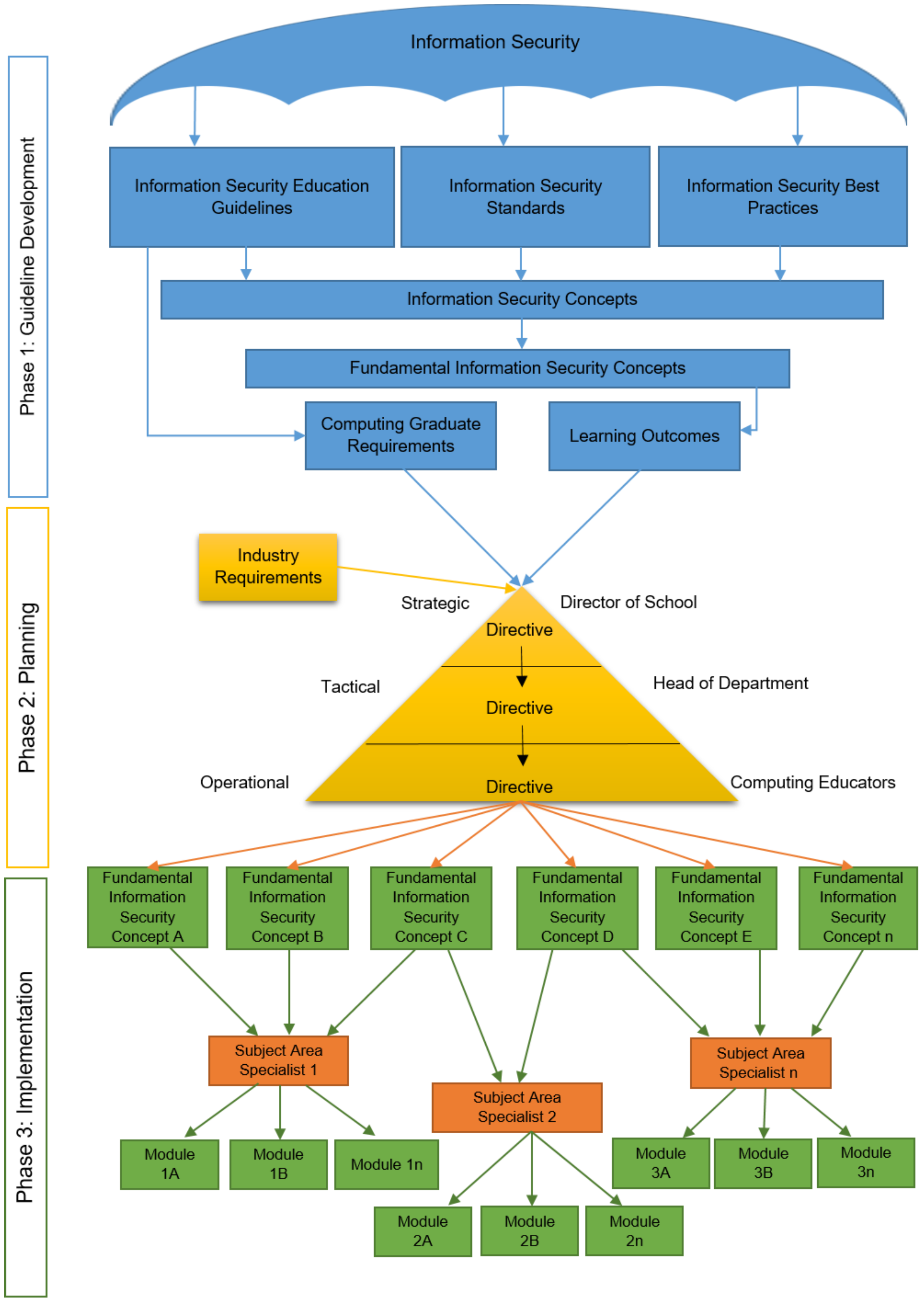
Information Security
Information Security Education Guidelines
Information Security Standards
Information Security Best Practices
Information Security Concepts
Fundamental Information Security Concepts
Computing Graduate Requirements
Learning Outcomes
Phase 1: Guideline Development
Industry Requirements
Strategic
Director of School
Directive
Tactical
Head of Department
Directive
Operational
Computing Educators
Directive
Phase 2: Planning
Fundamental Information Security Concept A
Fundamental Information Security Concept B
Fundamental Information Security Concept C
Fundamental Information Security Concept D
Fundamental Information Security Concept E
Fundamental Information Security Concept n
Subject Area Specialist 1
Subject Area Specialist 2
Subject Area Specialist n
Module 1A
Module 1B
Module 1n
Module 2A
Module 2B
Module 2n
Module 3A
Module 3B
Module 3n
Phase 3: Implementation

Figure 7.4: Revised Information Security Education Framework

Relating to the validity of the above-mentioned recommendations, the proposed framework is thus revised as depicted in Figure 7.4, to reflect the recommendations that were provided by the elites.

7.7. Conclusion

This chapter discussed the validation of the proposed information security education framework. Furthermore, the interview process that was undertaken to conduct the validation of this research was discussed together with the elite feedback. The proposed information security education framework was modified accordingly as discussed in Section 7.6.

The responses for the validation of the proposed information security education framework provided by the elites indicated that the proposed framework is feasible for the pervasive integration of information security into undergraduate computing curricula.

The following chapter concludes this research by discussing how the primary and secondary objectives as outlined in Chapter 1, Section 1.3, were addressed. In addition, the summaries of the preceding chapters are provided. The chapter also provides research limitations and recommendations for future research.

Chapter 8 – Conclusion

This chapter draws conclusions based on the research presented in the preceding chapters. It further mentions what each of the chapters aimed to accomplish by providing a summary of each of the previous chapters. Furthermore, it specifically states how and where in the dissertation each of the primary and secondary research objectives were met. It highlights the primary contribution of this research. Additionally, it discusses the research limitations and it concludes by discussing recommendations for future research.

8.1. Introduction

Information is defined as an important and valuable information asset that requires protection from various threats that can cause undue harm to the information. In an organisational setting, it is the duty of all employees to protect this information asset. Therefore, as computing students upon graduating become organisational employees, they too acquire this duty. Employees are, however, often cited as the "weakest link" in the attempt to protect organisational information assets from potential threats. This research, therefore, focused on the development of an information security education framework to assist higher education institutions' computing departments and computing educators with ***"how"*** to pervasively integrate information security into undergraduate computing curricula. This is to ensure that information security is addressed in various modules from a different perspective in each module. This could ensure that computing graduates possess information security skills, knowledge and understanding which could enable them to appropriately protect organisational information systems and related information assets from potential threats when working with them.

The problem stated in Chapter 1, Section 1.2, that this research aimed to solve is that, ***"Currently, no generally used framework exists to aid the pervasive integration of information security into undergraduate computing curricula"***. To address this problem, it was necessary to develop a framework to aid the pervasive integration of information security into undergraduate computing curricula.

Section 8.2 of this concluding chapter provides a summary of the preceding chapters that were used to solve the above-mentioned problem. Furthermore, in Section 8.3, this chapter describes how this research met the research objectives outlined in Chapter 1. Section 8.4 states the research contribution, Section 8.5 provides the research limitations and Section 8.6 provides suggestions for future research, while Section 8.7 concludes this research.

8.2. Summary of Chapters

Chapter 1 aimed to introduce information security as the domain in which this research is contained and to identify the problem within information security. It was established that employees are often cited as the "weakest link" in the attempt to protect organisational information systems and the related information assets. It was stated that it is the duty of higher education institutions to produce computing graduates who possess the necessary information security understanding that could enable them the ability to handle organisational information assets securely. Although the key role players provide guidelines and recommendations for computing curricula, it was indicated that they do not provide enough guidance to computing educators about ***"how"*** they can pervasively integrate information security into their modules. In order to solve the identified problem, research objectives were identified. Furthermore, Chapter 1 provided the research methods that were used to meet the identified research objectives.

The aim of **Chapter 2** was to introduce the research approach, the research technique and research procedures that were followed in conducting this study. In addition, the systematic process that was followed to conduct the survey reported in Chapter 5 is provided, including the interview process, participants and the questionnaire design thereof.

Chapter 3 discussed and argued that information security is an important and valuable organisational asset. Computing students, upon graduating often become organisational employees with the roles and responsibilities to develop, design, maintain and implement information systems. As employees are often cited as the "weakest link" it is crucial to ensure that these computing graduates become employees that can perform their organisational roles and responsibilities in a secure manner to ensure the protection of organisational information systems and the related information assets. Through discussing the multi-dimensions of information security using McCumber's model, it was established that information security education is an appropriate security measure that can be employed to ensure that undergraduate computing graduates are equipped with the required information security skills, knowledge and understanding to perform their organisational roles and responsibilities securely. Furthermore, it was argued that information security education obtained through a higher education qualification is an appropriate method to use in order to achieve this.

In **Chapter 4,** the key role players who provide computing curricula guidelines and recommendations for higher education institutions stated that Information Assurance and Security (IAS) should be integrated into computing curricula as a pervasive theme. Various other approaches for integrating information security were discussed and it was stated that this research supports both the "*add information security concepts to existing modules*" approach and the "*thread approach*" as they are similar to and support the pervasive theme. Challenges related to integrating information security into the computing curricula were discussed. One of the challenges identified is that information security is a broad area of study. Relating to this, a discussion on the significant impact that the pervasive integration of information security was done. It was stated that pervasive integration allows information security to be addressed multiple times in multiple modules since it has a lot of scope and depth.

Chapter 5 aimed to present the results and findings of the survey conducted to elicit South African computing educators' perspectives regarding the pervasive integration of information security and the current integration of information security into undergraduate computing curricula. Furthermore, it aimed to identify which fundamental information security concepts should be pervasively integrated into undergraduate computing curricula and the ideas and challenges for integrating such concepts. Results and findings of this survey are presented in *Section 5.2*. While all participants indicated that information security education is important to undergraduate computing graduates, some participants still held the perspective that information security should not be pervasively integrated. Some participants felt that a module should focus on teaching the content of that particular module. However, other participants indicated that the pervasive integration thereof could demonstrate the omnipresence of information security to computing students. Furthermore, it was indicated that no single module could address the entire scope and depth of information security. Therefore, the pervasive integration could help in ensuring that information security is addressed multiple times, in multiple modules, thereby ensuring that computing graduates possess the required information security skills, knowledge and understanding.

The aim of **Chapter 6** was to identify a solution to the problem identified in Chapter 1. The solution takes the form of a framework to address ***"how"*** the computing department could pervasively integrate information security into its curricula. Chapter 6, therefore, proposed an information security education framework for the pervasive integration of information security into undergraduate computing curricula. The proposed information security education framework was contextualised to demonstrate ***"how"*** a computing department could implement the proposed information security education framework.

Chapter 7 provided the validation of the information security education framework that was proposed in Chapter 6. Elites including a Director of School, Head of Department and various computing educators validated the framework. From the feedback presented, it is evident that the elites effectively validated the proposed framework, as they stated that the proposed information security education framework was feasible for integrating information security into their curricula. Only two revisions for the proposed information security education framework were recommended. Both revisions were applied to the framework, as they were considered valid by the researcher.

8.3. Meeting the Research Objectives

The primary objective of this research was ***to develop a framework to aid the pervasive integration of information security into undergraduate computing curricula***. To meet this primary objective, three secondary objectives were identified. These secondary objectives are restated and described below. In addition, it is argued that meeting the identified secondary objectives led to the achievement of the primary objective.

Secondary objective 1 aimed **to develop an understanding of the importance of information security**.

In **Chapter 3**, this objective was met through highlighting the need for the protection of information as it is an important and valuable organisational asset. It was further highlighted that information gives organisations a competitive edge over their competitors and it allows the organisation to financially prosper. The multi-dimensions of information security which, include the critical characteristics of information, information states and security measures, were presented by referring to McCumber's model in *Section 3.4*. As the definition of information security indicated that, it is the protection of information from potential threats that can compromise its critical characteristics, the chapter provided further literature to highlight the various security measures that can be used to protect information from potential threats. It was reported that humans are often cited as the "weakest link" in the attempt to protect organisational information systems and related information assets. Furthermore, it was argued that employees will remain the “weakest link” unless security measures (education, training and awareness; policy; and technology) are used properly to prevent employees from intentionally and accidentally causing harm to organisational information assets. Additionally, information security education obtained through a qualification that is offered at a higher education institution was identified as an appropriate security measure that can be employed to ensure the protection of information systems and related information assets by organisational employees.

Secondary objective 2 aimed **to determine the importance of information security education as it relates to undergraduate computing graduates**.

This objective was met in **Chapter 3** where it was stated that computing graduates, upon exiting higher education institutions, become organisational employees at the operational level. Like all organisational employees, these graduates acquire the responsibility to protect organisational information assets. Computing graduates are involved in designing, developing, implementing and maintaining organisational information systems. Furthermore, this objective was met in **Chapter 4**, in *Section 4.3* through the key role players who provide computing curricula guidelines and recommendations that explicitly included IAS as a knowledge area that should be addressed as a pervasive theme within the Computer Science (CS) and Information Technology (IT) bodies of knowledge. Although IAS was not explicitly added as a knowledge area within the Information Systems (IS) body of knowledge, information security was highlighted in the IS curricula guidelines and recommendations provided by the key role players. In *Subsection 4.4.1*, it was argued that it is important for information security to be taught to all undergraduate students in the CS, IS and IT computing disciplines. This could ensure that computing graduates become a stronger link in securing organisational information systems and related information assets from potential threats as stated in *Section 4.5*.

Secondary objective 3 aimed **to determine computing educators’ perspectives on information security education in a South African context.**

This secondary objective was met through the survey reported in **Chapter 5**, which had four survey objectives as shown in Chapter 1, Table 1.2. From the results and findings of the survey, it is clear that all the participants of the survey who included Heads of Departments, Junior and Senior Lecturers regard information security education to be important to undergraduate computing students. While some participants were not of the regard that information security should be pervasively integrated, it was also indicated that the pervasive integration of information security could demonstrate the omnipresence of information security. Additionally, it was indicated that the pervasive integration could enable computing students to see information security as a pervasive theme and not an isolated theme. Furthermore, the results and findings indicated that information security was not integrated into undergraduate computing curricula, but rather, more attention was given to information security at fourth year or Honours level. In addition, it was stated that not all computing students are guaranteed to proceed to this level and those who do would need to specifically select information security as it is mostly offered as a single isolated elective module. The survey results and findings further revealed that some computing educators do not integrate information security into their modules as they, for example, do not even have enough time to cover the content of their modules. Moreover, some computing educators are already forced to integrate other themes into their modules; while others would like to retain the core focus of their modules. These results and findings, therefore, indicated that some of the South African higher education institutions that were surveyed were producing computing graduates from their undergraduate qualifications who do not possess the necessary information security skills, knowledge and understanding.

8.4. Contribution of Research

The primary objective of this research was ***to develop a framework to aid the pervasive integration of information security into undergraduate computing curricula***. Therefore, the primary contribution of this research was to develop this framework.

The primary objective of this research was met in **Chapter 6** where an information security education framework was proposed in *Section 6.2*. The proposed framework is presented in three phases, namely: The guideline development, planning and implementation phases. This framework was developed to aid computing departments in pervasively integrating information security into their undergraduate computing curricula. To illustrate how the proposed framework could be implemented by a computing department, the proposed framework was contextualised to an IT Department in *Section 6.3*. The proposed framework was validated in **Chapter 7,** by six elites who included a Director of School, Head of Department and various educators who held senior educator positions within the department through interviews. Some of the elites provided recommendations for the improvement of the proposed framework thus leading to the revision of the proposed framework being presented in *Section 7.6*.

8.5. Research Limitations

The limitations of this research project are that the survey was only conducted in seven higher education institutions in South Africa with only 21 participants. This can be attributed to cost constraints as the researcher had to travel to the higher education institutions where the participants are employed. Additionally to this, time constraints affected the number of computing educators who were available to participate in the survey. The survey results and findings are based on the higher education institutions surveyed and cannot be generalised to all higher education institutions in South Africa. The framework was developed for the pervasive integration of information security into undergraduate computing curricula. As stated, computing curricula refers to CS, IS and IT curricula. However, the framework was only validated by an IT Department. The framework could, therefore, be implemented by the CS and IS departments as well.

8.6. Suggestions for Future Research

Introducing the proposed framework to computing departments in the CS, IS and IT fields within the South African context to get further input on the proposed framework. Furthermore, to get South African higher education institutions computing departments in the CS, IS and IT fields to use the proposed framework to pervasively integrate information security into their computing curricula.

Although the assessment of information security is outside the scope of this research project, assessment is an important part of education. This is to test through the implementation of the proposed framework that information security has been effectively integrated. It is, therefore, suggested that future research includes this assessment of information security.

8.7. Epilogue

The process undertaken to complete this research project has been fulfilling. It is envisaged that the framework proposed by this research could add value to the South African undergraduate computing department and the body of knowledge within information security education.

References

Ackoff, R. L. (1989). From data to wisdom. *Journal of Applied Systems Analysis*, *16*(1), 3–9. https://doi.org/citeulike-article-id:6930744

ACM/AIS. (2010). IS 2010: Curriculum guidelines for undergraduate degree programs in information systems. *Communications of the Association for Information Systems*, *26*, 359–428.

ACM/AIS/IEEE - CS. (2005). *Computing Curricula 2005*. *ACM Journal of Educational Resources in Computing* (Vol. 1). https://doi.org/10.1145/1140123.1140216

ACM/IEEE - CS. (2001). Computing curricula 2001. *Journal of Educational Resources in Computing*, *1*(3es), 1–es. https://doi.org/10.1145/384274.384275

ACM/IEEE - CS. (2008a). *Computer Science Curriculum 2008 : An Interim Revision of CS 2001 Report from the Interim Review Task December 2008 Association for Computing Machinery IEEE Computer Society*. *Security*. Retrieved from http://www.acm.org/education/curricula-recommendations

ACM/IEEE - CS. (2008b). Information Technology 2008 Curriculum Guidelines for Undergraduate Degree Programs in Information Technology. *Current Practice*, 1–139. https://doi.org/10.1145/362552.362554

ACM/IEEE - CS. (2013). Computer Science Curricula 2013. *Practice*, 1–172. https://doi.org/10.1145/2534860

Advanced Software Products Group Inc. (2016). The Three States of Digital Data. Retrieved November 23, 2016, from http://aspg.com/three-states-digital-data/

Amankwa, E., Loock, M., & Kritzinger, E. (2014). A conceptual analysis of information security education, information security training and information security awareness definitions. In *The 9th International Conference for Internet Technology and Secured Transactions (ICITST-2014)* (pp. 248–252). https://doi.org/10.1109/ICITST.2014.7038814

Andress, J. (2011). *The Basics Of Information Security: Undestanding the Fundamentals of InfoSec in Theory and Practice* (2nd ed.). Oxford: Syngress.

Bellinger, G., Castro, D., & Mills, A. (2004). Data , Information , Knowledge , and Wisdom. *Systems Thinking*, 5. https://doi.org/http://dx.doi.org/10.1016/j.mpaic.2013.11.009

Besnard, P., & Hunter, A. (2008). *Elements of Argumentation*. The MIT Press. https://doi.org/10.1007/978-3-540-75256-1_3

Bhattacherjee, A. (2012). *Social Science Research: principles, methods, and practices*. *Textbooks collection* (Vol. 9). https://doi.org/10.1186/1478-4505-9-2

Boote, D. N., & Beile, P. (2005). Featuresi Scholars Before Researchers : On the Centrality of the Dissertation Literature Review in Research Preparation. *Educational Researcher*, *34*(6), 3–15.

Chung, S., Hansel, L., Bai, Y., Moore, E., Taylor, C., Crosby, M., … Endicott-Popovsky, B. (2014). What approaches work best for teaching secure coding practices? *2014 HUIC Education & STEM Conference*.

Clinch, J. (2009). ITIL v3 and information security. *Clinch Consulting White Paper*, (May), 1–40. Retrieved from http://www.apmg-library.org/Player/eKnowledge/itil_v_and_information_security.pdf

Conti, G., Hill, J., Lathrop, S., Alford, K., & Ragsdale, D. (2003). A comprehensive undergraduate information assurance program. *IFIP Advances in Information and Communication Technology*, *125*, 243–260. https://doi.org/10.1007/978-0-387-35694-5

Davenport, T. H., & Prusak, L. (1997). *Information Ecology : Mastering the information and knowledge environment* (1st ed.). New York: Oxford University Press.

Davis, J., & Dark, M. (2003). Teaching students to design secure systems. *IEEE Security and Privacy*, *1*(2), 56–58. https://doi.org/10.1109/MSECP.2003.1193212

Deloitte. (2009). The 6th Annual Global Security Survey, 60.

Dodge, R. C. (2013). Information Assurance and Security in the ACM/IEEE CS2013. In R. C. Dodge Jr. & L. A. Futcher (Eds.), *IFIP World Conference on Information Security Education* (pp. 48–57). Berlin, Heidelberg: Springer.

Driscoll, D. L. (2011). Introduction to Primary Research: Observations, Surveys, and Interviews. *Writing Spaces: Readings on Writing*, *2*, 153–174. https://doi.org/10.1111/j.1540-5885.2010.00744.x

Drucker, P. F. (1988). The Coming of the New Organization. *Harvard Business Review*, (1), 45–53. Retrieved from http://0-eds.a.ebscohost.com.wam.seals.ac.za/eds/pdfviewer/pdfviewer?sid=8ff6541c-b566-4387-93a5-601c428d0f03@sessionmgr4008&vid=1&hid=4103

Furnell, S., & Clarke, N. (2012). Power to the people? the evolving recognition of human aspects of security. *Computers and Security*, *31*(8), 983–988. https://doi.org/10.1016/j.cose.2012.08.004

Futcher, L., Schroder, C., & Von Solms, R. (2010). Information security education in South Africa. *Information Management & Computer Security*, *18*(5), 366–374. https://doi.org/10.1108/09685221011095272

Futcher, L., & Van Niekerk, J. (2011). Towards a Pervasive Information Assurance Security Educational Model for Information Technology Curricula. In R. C. Dodge Jr & L. A. Futcher (Eds.), *Proceedings of the 8th World Information Security Education Conference* (pp. 164–171). Berlin Heidelberg: Springer.

Hentea, M. (2005). A Perspective on Achieving Information Security Awareness. *Issues in Informing Science and Information Technology*, *2*, 169–178.

Hentea, M., Dhillon, H. S., & Dhillon, M. (2006). Towards Changes in Information Security Education. *Journal of Information Technology Education*, *5*, 221–233.

Hinson, G. (2003). Human Factors in Information Security Methods. https://doi.org/10.1177/154193120004400219

Hinson, G. (2005). The Value of Information Security Awareness. *Noticebored-Creative Help for Your Information Security Awareness Program*, (June), 1–20. Retrieved from http://www.noticebored.com/The_value_of_security_awareness.pdf

Hofstee, E. (2006). *Constructing a good dissertation: A Practical Guide to finishing a Master's,MBA,or PhD on Schedule*. (EPE, Ed.). Johannesburg, South Africa.

Irvine, C. E., Chin, S. K., & Frincke, D. (1998). Integrating security into the curriculum. *Computer*, *31*(12), 25–30. https://doi.org/10.1109/2.735847

ISO/IEC 27000. (2012). *ISO/IEC 27000:2012 Information technology — Security techniques — Information security management systems — Overview and vocabulary*. *ISO/IEC 27000:2012* (3rd ed., Vol. 2012). Switzerland: ISO/IEC.

ISO/IEC 27001. (2013). *Information technology - Security techniques - Information security management systems - Requirements*. Switzerland: ISO/IEC.

ISO/IEC 27002. (2013). *ISO / IEC 27002 : Information technology — Security techniques — Code of practice for information security controls* (2nd ed.). Switzerland: ISO/IEC.

ISO/IEC 27005. (2011). *ISO/IEC 27005 : 2011 South African National Standard Information technology — Security techniques — Information security risk management*. Switzerland: ISO/IEC.

ISO/IEC 7498-2. (1989). *Information Processing Systems - Open Systems Interconnection - Basic Reference Model - Part 2 : Security Architecture* (1st ed.). Switzerland: ISO/IEC.

Kabay, M. E. (2002). *Computer Security Handbook–Using Social Psychology to Implement Security Policies*.

Katsikas, S. K. (2000). Health care management and information systems security: awareness, training or education? *International Journal of Medical Informatics*, *60*(2), 129–135. https://doi.org/10.1016/S1386-5056(00)00112-X

King, M. (2009). *King Code of Governance for South Africa 2009*. *Institute of Directors in Southern Africa*.

Krippendorff, K. (2013). *Content Analysis: An Introduction to Its Methodology* (3rd ed.). United Kingdom - London: SAGE Publications Ltd.

Lacey, D. (2009). *Managing the Human Factor in Information Security*. Retrieved from http://eu.wiley.com/WileyCDA/WileyTitle/productCd-0470721995.html

Landoll, D. J. (2006). *The Security Risk Assessment Handbook*. New York: Auerbach Publications.

Marshall, M. N. (1996). Sampling for qualitative research Sample size. *Family Practice*, *13*(6), 522–525. https://doi.org/10.1093/fampra/13.6.522

Massart, R. (2015). *5 Reasons Why Your Security Education Program isn't Working (and how to fix it)*.

McCumber, J. (2005). *Assessing and Managing Security Risk in IT Systems: A structured methodology*. Washington, DC: Auerbach Publications.

Michalson. (2003). Information security and the law: threats and how to manage them. *The International Journal of Research into New Media Technologies*, *4*(3).

Moore, N., & Stokes, P. (2012). Elite Interviewing and the Role of Sector Context: An Organizational Case from the Football Industry. *Qualitative Market Research : An International Journal*, *15*(4), 438–464. https://doi.org/10.1108/13522751211257105

NIST SP800-100. (2006). *NIST Special Publication 800-100 - Information Security Handbook: A Guide for Managers*.

NIST SP800-12. (1995). *An Introduction to Computer Security: The NIST Handbook*.

NIST SP800-16. (1998). *Information Technology Security Training Requirements: A Role- and Performance-Based Model*. Washington, DC: U.S. Government Printing Office,.

NIST SP800-16. (2013). *A Role Based Model for Federal Information Technology / Cyber Security Training*.

NIST SP800-50. (2003). Building an Information Technology Security Awareness and Training Program. *NIST SP800-50*, (October), 1–38. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf

NIST SP 800-30. (2002). *Risk Management Guide for Information Technology Systems Recommendations of the National Institute of Standards and Technology*. *NIST SP 800-30* (Vol. 30). Retrieved from http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:Risk+Management+Guide+for+Information+Technology+Systems+Recommendations+of+the+National+Institute+of+Standards+and+Technology#1

O'Brien, J. (2002). *Management Information Systems: Managing Information Technology in the E-Business Enterprise* (5th ed.). New York: McGraw-Hill.

Olivier, M. S. (2009). *Information Technology Research: A practical guide for Computer Science and Informatics* (3rd ed.). Pretoria: Van Schaik.

Perrone, L. F., Aburdene, M., & Meng, X. (2005). Approaches to undergraduate instruction in computer security. *2005 ASEE Annual Conference and Exposition: The Changing Landscape of Engineering and Technology Education in a Global World*, 651–663.

Pocock, S., Harrison, M., Wright, P., & Johnson, P. (2001). THEA: A Technique for Human Error Assessment Early in Design. *Proceedings of Eighth IFIP TC.13 Conference on Human–computer Interaction (INTERACT'01)*, 247–254.

Posthumus, S., Von Solms, R., & King, M. (2010). The Board and IT Governance: The What, Who and How. *South African Journal of Business Management*, *41*(3), 23–32.

Rajasekar, S., Philominathan, P., & Chinnathambi, V. (2006). Research Methodology. *Methods*, *68*(1), 23. https://doi.org/10.1097/AAP.0b013e3182208cea

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. *Computers and Security*, *53*, 65–78. https://doi.org/10.1016/j.cose.2015.05.012

Safa, N. S., Von Solms, R., & Futcher, L. (2016). Human aspects of information security in organisations. *Computer Fraud and Security*, *2016*(2), 15–18. https://doi.org/10.1016/S1361-3723(16)30017-3

Saunders, M., Lewis, P., & Thornhill, A. (2012). *Research Methods for Business Students*. London: Prentice Hall.

Schneider, F. B. (2013). Cybersecurity education in universities. *IEEE Security and Privacy*, *11*(4), 3–4. https://doi.org/10.1109/MSP.2013.84

Schultz, E. (2005). The human factor in security. *Computers and Security*, *24*(6), 425–426.

https://doi.org/10.1016/j.cose.2005.07.002

SIGITE Curriculum Committee. (2005). *Computing Curriculum Information Technology Volume*.

Skowronek, D., & Duerr, L. (2009). convenience of nonprobability Survey strategies for small academic libraries. *College & Research Libraries News*, *70*(7), 412–415.

Smith, E., Von Solms, S., Oosthuizen, H., & Kritzinger, E. (2005). Information Security education: Bridging the gap between academic institutions and industry, (1998), 1–14. Retrieved from http://umkn-dsp01.unisa.ac.za/handle/10500/4005

Talib, M. A., Khelifi, A., & Ugurlu, T. (2012). Using ISO 27001 in teaching information security. *IECON Proceedings (Industrial Electronics Conference)*, 3149–3153. https://doi.org/10.1109/IECON.2012.6389395

Taylor, B., & Azadegan, S. (2008). Moving Beyond Security Tracks: Integrating Security in CS0 and CS1. *Proceedings of the 39th SIGCSE Technical Symposium on Computer Science Education*, 320–324. https://doi.org/http://doi.acm.org/10.1145/1352135.1352246

Thomason, S. (2013). People – The Weak Link in Security. *Global Journal of Computer Science and Technology Network, Web & Security*, *13*(11), 7–12. Retrieved from https://globaljournals.org/GJCST_Volume13/2-People-The-Weak-Link-in-Security.pdf

Tipton, H. F., & Krause, M. (2008). *Information Security Management Handbook*. (6, Ed.). New York: CRC Press.

Tomhave, B. L. (2005). Alphabet soup: Making sense of models, frameworks, and methodologies, 1–57. Retrieved from http://egov.ufsc.br/portal/sites/default/files/alphabet_soup.pdf%5Cnwww.secureconsulting.net/Papers/Alphabet_Soup.pdf%5Cnhttp://secureconsulting.net/papers-publications.html

Venter, H. S., & Eloff, J. H. P. (2003). A taxonomy for information security technologies. *Computers and Security*, *22*(4), 299–307. https://doi.org/10.1016/S0167-4048(03)00406-1

Volonino, L., & Robinson, S. (2004). *Principles and practice of Information Security*. New Jersey: Anderson.

Von Solms, R., & Thomson, K.-L. (2002). Corporate Governance : Information Security the Weakest Link ? *Corporate Governance*, 1–10. https://doi.org/http://icsa.cs.up.ac.za

Von Solms, R., & Von Solms, S. H. (2006). Information Security Governance: A model based on the Direct-Control Cycle. *Computers and Security*, *25*(6), 408–412. https://doi.org/10.1016/j.cose.2006.07.005

Von Solms, S., & Von Solms, R. (2009). *Information Security Governance*. New York: Springer.

Whitman, M. E. (2003). Information Security. *Communications of the ACM*, *46*(8), 91–95. https://doi.org/10.1145/859670.859675

Whitman, M. E., & Mattord, H. J. (2004). A Draft Model Curriculum for Programs of Study in Information Security and Assurance. *Information Systems Security Education*, *30114*(770). Retrieved from http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1015&context=sais2004

Whitman, M. E., & Mattord, H. J. (2010). *Management of Information Security* (3rd ed.). Boston: Course Technology, Cengage Learning.

Whitman, M. E., & Mattord, H. J. (2014). *Management of Information Security* (4th ed.). Boston: Course Technology, Cengage Learning.

Yang, T. A. (2001). Computer Security and Impact on Computer Science Education. *Journal of Computing Sciences in Colleges*, *4*(May 2001), 233–246. Retrieved from http://dl.acm.org/citation.cfm?id=378722

Yngström, L., & Bjorck, F. (1999). The value and assessment of information security education and training. *Proceedings of the IFIP TC11 WG11. 8 First World Conference on Information Security Education (WISE1)*, 1–21.

Appendix A1

Integrating Information Security into the IT Undergraduate Curriculum : A Case Study

Integrating Information Security into the IT Undergraduate Curriculum: A Case Study

Lindokuhle G. Gomana
Centre for Research in Information and Cyber Security Nelson Mandela Metropolitan University
Port Elizabeth, South Africa
+27 73 729 7306
s210031492@nmmu.ac.za

Lynn A. Futcher
Centre for Research in Information and Cyber Security Nelson Mandela Metropolitan University
Port Elizabeth, South Africa
+27 41 504 9128
Lynn.Futcher@nmmu.ac.za

Kerry-Lynn Thomson
Centre for Research in Information and Cyber Security Nelson Mandela Metropolitan University
Port Elizabeth, South Africa
+27 41 504 3408
Kerry-Lynn.Thomson@nmmu.ac.za

ABSTRACT

It is clear that information security is an area of vital concern, and that global societies are facing an increasing number of challenges related to security. Attacks on computer systems often succeed because people are not aware of the vulnerabilities of their systems as they lack information security knowledge. Therefore, Information Technology (IT) professionals should be made aware of and educated about information security in order to protect such systems. South African universities, however, do not have guidelines to ensure that essential information security aspects are included in the IT courses that are offered. This paper addresses the problem that the extent to which information security is currently integrated into the IT undergraduate qualification at the NMMU, School of ICT, is unknown. This has been addressed by means of a survey which included structured interviews of the IT lecturers supported by a questionnaire. The argument for integrating information security into the IT curriculum is based on a literature study.

Categories and Subject Descriptors

K.3.2 [**Computer and Information Science Education**]: Computer Science Education, Curriculum

General Terms

Security

Keywords

Information and Cyber Security Education, Information Technology Curriculum, Security Concepts, Case Study Research.

SACLA 2015, 02-03 July, Johannesburg, South Africa

1. INTRODUCTION

The interconnectedness of today's global society has made computer systems vulnerable to information security threats. Incidents related to the disclosure of confidential information, and the major growth in computer viruses is on the increase. Globally, there have already been numerous cases of theft and other economic crimes documented that involve a loss of a substantial amount of money per incident. The greatest threat to the benefits allowed by computers and the Internet is that of security concerns [13].

Information security can be defined as the protection of information and the critical characteristics thereof which are confidentiality, integrity and availability. This also includes the protection of the systems and hardware that use, store and transmit that information. It is further suggested that the protection of this information can be achieved through the application of policy; training, education and awareness programs; as well as technology [11].

The purpose of information security education should be to integrate all of the security skills and competencies of the various functional specialties into a common body of knowledge; to add a multi-disciplinary study of information security concepts, issues and principles (technological and social); and to produce information systems security specialists and professionals capable of vision and pro-active response [9].

Information Technology (IT) is a rapidly evolving career, involving professionals who are increasingly expected to play a key role in contributing towards the information security needs of organizations. It is therefore important that academic institutions offering IT qualifications address this requirement within their curricula. IT lecturers should bring an increased awareness of information security into the classroom to help students gain a better awareness of security implications [6]. This is an ongoing challenge for IT lecturers.

The Association for Computing Machinery (ACM) Special Interest Group for Information Technology Education (SIGITE) also regards Information Assurance and Security (IAS) as one of the knowledge areas that should be defined as a pervasive theme and must therefore be addressed throughout the learning experience. Whereas a knowledge area represents a significant body of knowledge in a discipline, pervasive themes include topics that should permeate the IT curriculum since they are addressed across all knowledge areas. It is also stated that both students and lecturers need to be consistently aware of how these pervasive themes need to be integrated into the curriculum [2].

Topics relating to information security should include the five basic security services as defined by ISO/IEC 7498-2 [8], namely: identification and authentication; authorisation and access control; confidentiality; integrity and non-repudiation. Other topics relating to the availability of information, accountability and privacy are also important to consider. The ACM specifically highlights other key topics including cryptography, redundancy, intrusion detection, social engineering, denial of service, malware, etc. Although the ACM defines IAS both as a knowledge area and as a pervasive theme, there is little guidance provided with respect to assisting IT lecturers in integrating information security as a pervasive theme into their various modules [7]. The ACM [1] regards, IAS as a domain which is the set of controls and processes (which are both technical) and policy intended to protect and defend information and information systems by ensuring their confidentiality, integrity, and availability, and by providing for authentication and non-repudiation [1].

The primary aim of the research conducted as presented in this paper was to determine the extent to which information security is currently integrated into the IT undergraduate qualification at the NMMU, School of ICT. This paper presents the research methodology in Section 2 and highlights the importance of information security in the curriculum in Section 3. Section 4 provides a background to the case study, followed by a description of the questionnaire design in Section 5. While Section 6 presents the results and findings, Section 7 provides a detailed discussion highlighting key issues related to the research undertaken.

2. RESEARCH METHODOLOGY

The research methods used for this research included a literature study, case study research and argumentation.

A literature study was conducted to highlight the importance of information security and to understand the integration of information security within the IT curriculum. This literature study was also conducted in the field of Information Security education in general, and within the IT qualification curriculum using guidelines as suggested by the ACM.

Case study research according to Yin [14] was conducted at the NMMU, School of ICT to determine the extent to which information security and related information security concepts are currently integrated into the IT undergraduate curriculum. To support the case study research, a structured interview with the aid of a questionnaire was conducted. The participants of this study were the IT lecturers responsible for teaching various modules within the IT curriculum.

The main argument for this research is formed based on literature study findings and case study findings. The argument is that information security should be integrated into the IT curriculum as a pervasive theme as advocated by the ACM. However, prior to conducting this research, the extent to which this is currently done within the NMMU, School of ICT, IT undergraduate qualification was not known.

The following section addresses the importance of information security in the IT curriculum.

3. INFORMATION SECURITY IN THE IT CURRICULUM

What cannot be overemphasized in today’s competitive business environment is the importance and value of information security education [4]. Wilson & Hash [12] state that the focus of information security education should be to develop people’s ability and vision to perform complex multi-disciplinary activities and the necessary skills that are needed to further the information security profession and to keep pace with threats and technology changes [12]. The IT curriculum as recommended by the ACM acts as a guideline for any formal qualification in IT. According to the ACM [3], the core of the IT curriculum is the IT Body of Knowledge. There are 13 knowledge areas within the IT Body of Knowledge. Information Assurance and Security (IAS) is one of these knowledge areas and should therefore be included when designing an IT curriculum. In addition, Border and Holden [6] regard IAS as one of the knowledge areas which should be addressed as a pervasive theme.

A pervasive theme is described as those topics that should be ‘considered essential, but that did not seem to belong in a single specific knowledge area or unit’ [3]. These themes should, therefore, be woven into the curriculum by being addressed numerous times and in multiple classes [3]. However, according to Taylor and Azadegan [10], this is not generally the case as the majority of undergraduate computing students learn programming and design with little regard to security issues.

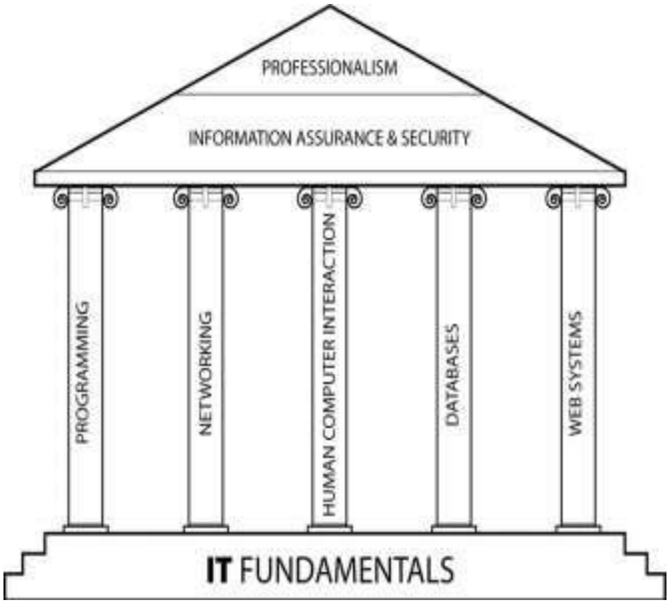

Figure 1: The IT Discipline [3]

From Figure 1, it is clear that IAS is an overarching knowledge area that impacts the total computer system and should therefore be integrated into all pillars of the IT discipline.

The ACM guidelines highlight various information assurance and security topics that should be addressed within the curriculum, together with related learning outcomes as shown in Table 1.

Table 1: Information Assurance and Security – Fundamental Concepts [1]

Topic	Learning Outcome
Nature of the threats	Describe the type of threats to data and information systems. [Knowledge]
Need for Information Assurance	Describe why processes and data need protection. [Knowledge]
Basic terminology (Confidentiality, Integrity and Availability)	Describe the context in which Confidentiality, Integrity and Availability are important to given processes and data [Application]
Threats and Vulnerabilities	Describe the major vulnerabilities present in systems today. [Knowledge] Define the fundamental motivations for intentional malicious exploitation of vulnerabilities.

Despite the relevant topics and related learning outcomes, the ACM guidelines do not adequately address IAS as a pervasive theme; and no further guidance exists to assist IT lecturers in developing curricula to ensure that IAS is effectively integrated into the curriculum at undergraduate level [7].

4. BACKGROUND TO CASE STUDY

At the NMMU, School of ICT, the IT undergraduate qualification has three streams of specialism, namely: the IT Communication Networks stream, the IT Software Development stream and the IT Support Services stream. The IT qualification is a three year diploma course, after which students have the option to continue onto their fourth year which is also referred to as Bachelor of Technology (B Tech).

In the IT Support Services qualification there is a module dedicated to equipping the students with information security skills and knowledge. This module is taught to them at second year level. The same module is taught to IT Communication Networks students at third year level. For the IT Software Development qualification, however, no formal module addressing information security is offered to them at undergraduate level. This research therefore specifically focuses on the integration of information security into the IT Software Development qualification.

For all streams, Information Security is a module offered at fourth year level. Therefore, some students in the IT Software Development qualification will exit the university having never been exposed to information security, as they will not have continued to complete a fourth year qualification. Furthermore, at fourth year level the Information Security module is an elective, meaning it is not a compulsory module. This means that Information Security will only be taken by those students who study towards a fourth year qualification and by those who decide to take Information Security as a module.

Table 2 outlines the first year, second year and third year modules which form part of the curriculum of the National Diploma IT, Software Development (SD) qualification at the NMMU, School of ICT. For the purposes of this study, not all modules were considered, but only those which are core to the IT Software Development qualification.

Table 2: Key Software Development modules at the NMMU, School of ICT

Software Development		
1st Year	2nd Year	3rd Year
ONT1000	ONT2000	ONT3660
WIH1370	ITP2000	ONT3601
	PRT1000	WIH3602
	WIH2100	WIH3661
		PRT2110
		SGU1000

The codes for the modules represented in Table 2 are as follows: ONT1000 - Development Software 1; WIH1370 - Information

Systems 1; ONT2000 - Development Software 2; ITP2000 - Internet Programming 1; PRT1000 - Technical Programming 1; WIH2100 - Information Systems 2; ONT3660 - Project; ONT3601 - Development Software 3; WIH3602 - Information Systems 3; WIH3661 - Project Management; PRT2110 - Technical Programming 2; SGU1000 - Graphical User Interface Design 1.

Being core to the Software Development qualification, these modules were considered as being the ones with the most opportunity for the integration of information security concepts. They therefore formed the basis of the research conducted in order to determine the extent to which information security and related concepts are currently integrated into the IT Software Development curriculum.

The following section discusses the questionnaire design of the study conducted.

5. QUESTIONNAIRE DESIGN

The research study conducted at the NMMU, School of ICT, consisted of two approaches. The aim of Approach 1 was to determine the extent to which *information security (in general)* is integrated into the IT undergraduate diploma at the NMMU, School of ICT in the IT Software Development qualification. The aim of Approach 2, was to determine the extent to which *specific information security concepts* are integrated into the IT undergraduate diploma at the NMMU, School of ICT in the IT Software Development qualification.

For each of these two approaches, twelve participants were interviewed using a structured questionnaire to support the interview process. The participants were the IT lecturers of the modules as presented in Table 2. Each of the questionnaires underwent a pilot test to ensure correctness, conciseness and minimal ambiguity in the phrasing of the questions.

5.1. Approach 1

As mentioned, the aim of Approach 1 was to determine the extent to which *information security (in general)* is integrated into the IT Software Development curriculum at the NMMU, School of ICT.

The questionnaire for Approach 1 was designed using the security services and security aspects adapted from the ISO/IEC 7498-2 [8] standard, as well as those defined by Whitman and Mattord [11].

These security services are essential as they can be put into place to address a threat, namely: Identification and authentication, Authorisation/Access Control, Confidentiality, Integrity, and Non-repudiation/Non-denial. The additional security aspects as suggested by Whitman and Mattord [11] include: Availability, Accountability, and Privacy. These security aspects were also included in the questionnaire design for Approach 1.

The questionnaire for Approach 1 consisted of three sections:

- Section A addressed issues relating to risks associated with information security. The questions asked in this section were related to Information Assets, Threats, Vulnerabilities and Risk Analysis.
- Section B addressed security services associated with information security. The questions asked in this section related to Identification and Authentication, Authorisation/Access Control, Confidentiality, Integrity, Non-repudiation/Non-denial, Availability, and Privacy.
- Section C of the questionnaire addressed general issues related to information security aspects. The questions asked in this section related to secure user behaviour and security controls.

The questionnaire for Approach 1 consisted of three questions for each of the sections highlighted:

- Question 1: Is the particular security aspect/service currently being integrated?
- Question 2: Is the particular security aspect/service currently being assessed?
- Question 3: Are there any ideas for integrating the security aspect/service into the particular module?

There was additional space for comments to provide more qualitative data based on the discussions with each participant.

The results of this approach are discussed in Section 6.1.

5.2. Approach 2

As mentioned, the aim of Approach 2 was to determine the extent to which *specific information security concepts* are integrated into the IT Software Development curriculum at the NMMU, School of ICT.

Some of the information security concepts identified for the questionnaire were derived from an analysis of the IAS knowledge area and their related units within the ACM/IEEE Computer Society IT Curriculum Guidelines [3].

The information security concepts identified within the IAS knowledge included Attacks (e.g. Buffer overflows, Viruses, DOS); Authentication; Confidentiality, Integrity and Availability Concepts; Cryptography; Digital Forensics; Disaster Recovery; Ethical Issues in Computing (Privacy, Copyright); Information Backup and Recovery; Information States (Transmission, Storage, Processing); Intellectual Property; Intrusion Detection; Legal Issues in Computing (Hackers/Crackers); Secure Principles; Secure Software Development (SDLC); Secure-Coding; Security Awareness; Security Policies and Procedures; Security Standards (eg. ISO); and Security Threats and Vulnerabilities. All of these information security concepts were addressed within the questionnaire that supported the interviews with the various participants.

Further to this, the questionnaire aimed to determine at which level of Bloom's taxonomy each of the concepts should be addressed. The first and lowest level of Bloom's taxonomy is 'Knowledge'. Knowledge is the remembering of previously learned material. This is where the student knows common terms and specific facts. The second level is ‘Comprehension’. Comprehension is the ability to grasp the meaning of the material. The student should be able to explain or summarise the material, predict consequences or effects. Comprehension is the lowest level of understanding. The third level is ‘Application’. Application is the ability to use the material that has been learned in new and concrete situations. With this the student should demonstrate the correct usage of methods and procedures, apply laws and principles to new situations, etc. This level of learning requires a higher level of understanding than that of comprehension. The ‘Analysis’ level is at the fourth level. Analysis is the ability to break down the material into its different component parts in order to understand its organizational structure. The student should be able to identify and analyse the relationships of the various parts. The ‘Synthesis’ level is the fifth level. This level is the second highest in the taxonomy and it deals with the ability to judge the value of something based on specified criteria and standards. The ‘Evaluation’ is the sixth level. This is the highest level in the taxonomy and it refers to the ability to put together various parts in order to formulate a plan or an idea that is new to the student [5].

The questionnaire for Approach 2 consisted of three questions for each of the security concepts highlighted:

- Question 1: How applicable is the specified IAS concept to the particular module?
- Question 2: Is the specified IAS concept currently being integrated within the particular module?
- Question 3: If the specified IAS concept is currently being integrated, at which level of Bloom’s Taxonomy is this taking place?

There was additional space for comments to provide more qualitative data based on the discussions with each participant.

The results for this approach are discussed in Section 6.2.

The following section presents the results of the case study research conducted.

6. RESULTS AND FINDINGS

This section provides the results and findings of both Approach 1 and Approach 2 as described in Sections 5.1 and 5.2 respectively. After conducting the structured interviews, the results were carefully analysed.

6.1. Approach 1 Results and Findings

Section A addressed the issues relating to risks associated with information security. The questions asked in this Section were related to Information Assets, Threats, Vulnerabilities and Risk Analysis. Figure 2 depicts the results and findings of Section A of Approach 1’s questionnaire.

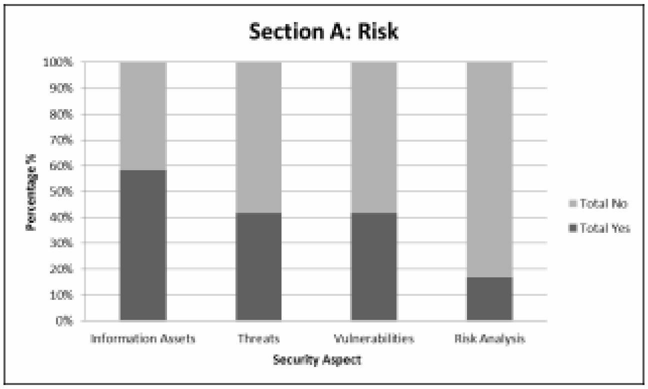

Figure 2: Information Security Risk Aspects (Overall)

As can be seen in Figure 2, 58% of the participants indicated that they do consider Information Assets within their modules (WIH1370, WIH2100, WIH3661, WIH3602, ONT2000, ONT3660, and PRT2110). Some of the reasons why it is not integrated into the rest of the modules are due to the lack of time to integrate it into the curriculum, and it not being relevant to some modules. Only 17% of the modules (WIH2100 and WIH3661) integrate Risk Analysis within their individual modules, while 42% of the modules (WIH1370, WIH2100, WIH3661, ONT3660 and PRT1000) address Threats. Similarly, only 42% of the modules (WIH1370, WIH3661, ONT3660, ONT3601 and PRT2110) address Vulnerabilities.

Section B addressed the various security services. As shown in Figure 3, 50% of the modules (ONT2000, ONT 3660, ONT3601, ITP2000, PRT1000 and PRT2110) are currently integrating Identification/Authentication. Similarly, 50% of the modules (WIH1370, WIH2100, WIH3602, ONT3660, ONT3601 and PRT2110) integrate Integrity into their modules whilst only 33.3% of the modules (WIH1370, WIH2100, ONT3660 and ITP2000) are integrating Confidentiality and 33.3% of the modules (WIH1370, WIH2100, ONT3660 and PRT2110) integrate Availability/Accountability.

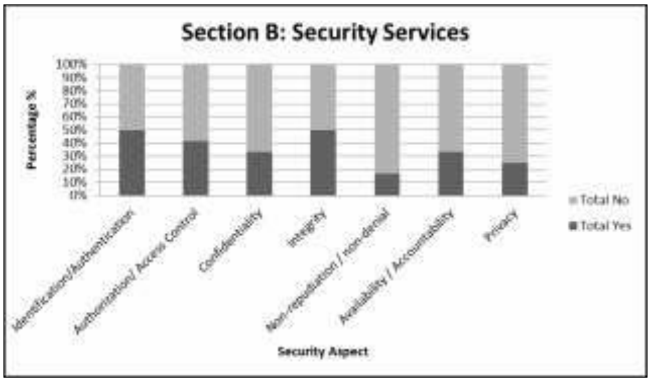

Figure 3: Security Services (Overall)

From these results it is clear that many of the security services are not currently being addressed by the existing modules. One of the main reasons why these security services are not being addressed is due to the fact that there is not enough time to integrate them into the current curriculum. In addition, most of the lecturers are under the impression that they are being addressed by at least one of the other modules, while some of the lecturers believe that addressing information security services is not the purpose of their particular module. Although some of these security aspects in Section B are being addressed, most of them are not being assessed as they are being addressed informally. In the first year none of the modules in the curriculum address any issues surrounding Identification and Authentication. At second year level only 75% of the modules (ONT2000, ITP2000 and PRT1000) are currently integrating Identification and Authentication into the curriculum. At third year level 50% of the modules (ONT3660, SGU1000 and PRT2110) integrate Identification and Authentication into the curriculum.

The first year curriculum also has no modules which cover Authorisation / Access Control. The second year has two modules (WIH2100 and PRT1000), and at third year three modules (ONT3660, ONT3601 and PRT2110) educate students on Authorisation / Access Control. The third aspect being Confidentiality is only covered in one module of both the first year (WIH1370) and third year (ONT3660). Two modules (WIH2100 and ITP2000) of the second year curriculum integrate Confidentiality into the curriculum. Integrity is covered by three modules (WIH3602, ONT3660, and ONT3601) in the third year curriculum and only one module (WIH1370) of each the first year curriculum and the second year module that addresses information security Integrity is WIH2100.

Non-repudiation is only covered by two modules (ONT3601 and PRT2110) in the third year curriculum, but none of the first or second year curricula cover this security service. Availability is integrated into the first year by one module (WIH1370) and at second year curricula with also one module (WIH2110) covering Availability/Accountability. The third year curriculum has two modules (ONT3660 and PRT2110) which cover Availability/Accountability with respect to information security. The first year curriculum does not cover Privacy. The second year curriculum has one module (WIH2100) which deals with Privacy and the third year curriculum has two modules (ONT3660 and PRT2110) which integrate this security service into the curriculum.

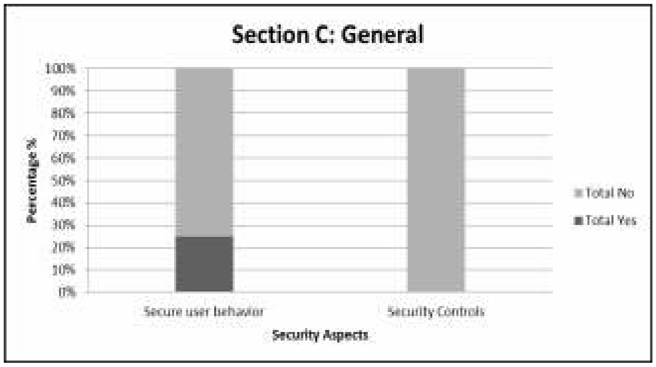

Figure 4: General Security Aspects (Overall)

Figure 4 shows the results and findings of Section C of the questionnaire. As shown in Figure 4 only 25% of the modules (WIH2100 and ONT3660) address Secure User Behaviour within their individual modules. Some of the lecturers who do not integrate Secure User Behaviour in their modules do not address it as they do not see it as applicable to their individual modules whereas some would consider integrating it if the information on how to integrate it was made available to them.

None of the modules address Security Controls within their modules. Many of the IT lecturers would consider integrating it if a suggestion on how information security can be integrated into their modules was made available.

6.2. Approach 2 Results and Findings

Figure 5 depicts the results and findings of Question 1 of Approach 2's questionnaire which aimed to determine how applicable the IAS concept is to the particular module.

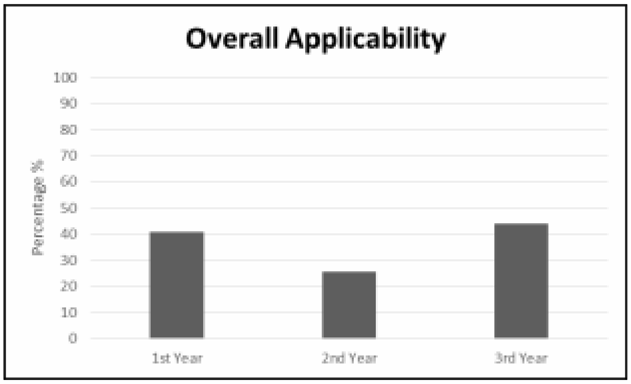

Figure 5: Overall applicability of information security concepts

At the first year of study the individual information security concepts with the highest percentage of applicability of 60% were Disaster Recovery; Ethical Issues in Computing (Privacy, Copyright); Information Backup and Recovery; Information States (Transmission, Storage, Processing); Secure Software Development (SDLC); and Secure Coding. As shown in Figure 5 the overall applicability level at first year for all the information security concepts was 41%. However, none of the IT modules are currently integrating these information security concepts as seen in Figure 6. There is a lack of evidence to suggest the reason for this. This is clearly a problem since many of these concepts are deemed to be applicable.

A further cause for concern is that none of the information security concepts at second year have an overall applicability level higher than 35%, although some of the information security concepts are being integrated. The information security concepts with an applicability level of 35% are Authentication; Confidentiality, Integrity and Availability (CIA) Concepts; Secure Software Development (SDLC); and Security Awareness. The average applicability of the information security concepts at second year is 25.75%; this can be seen in Figure 5. This result is even lower than that at first year level. These information security concepts are not being formally assessed in any of the modules, although they are briefly mentioned.

At third year the applicability levels vary, with the lowest at 20% and the highest being Information States (Transmission, Storage, and Processing) at 70%. While the applicability levels of the information security concepts increase at third year level, they were still very low when combined giving an overall applicability of 44.17% for the entire third year as depicted in Figure 5. It is not being formally assessed in any of the third year modules, but they are being mentioned. In some cases it was also stated that the text books do not even mention the information security concepts. This, however, does not provide a sufficient argument to not integrate these concepts into the various modules.

The year with the highest percentage applicability is the third year with an overall of 44.17%. The results suggest that the overall applicability of the information security concepts throughout the IT undergraduate software development qualification is not high at all being only at 36.97%.

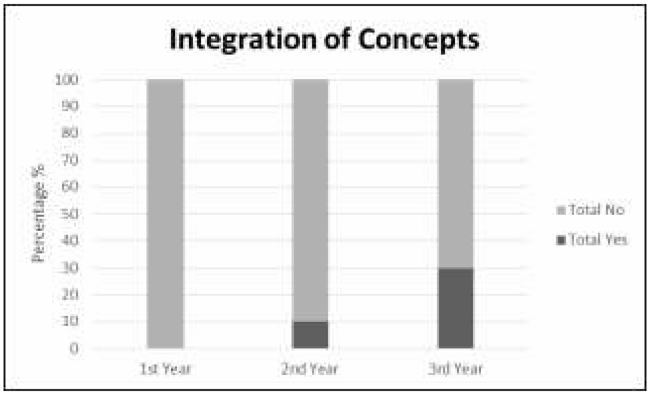

Figure 6: Overall integration of information security concepts

The results from the integration of the information security concepts further increases this concern because 87.78% responded in the negative over all three years. As shown in Figure 6, at first year level none of the modules are integrating any of the information security concepts identified in Section 5.2; at second year level, only 10% of the modules are integrating the information security concepts; and at third year level only 26.67%. This means that the majority of these information security concepts are not being integrated at all.

Some of these information security concepts are only mentioned during the semester or year. From the comments, the IT lecturers did not deem this as proper integration, but it can be a step in the right direction.

The results of the third question "If integrated, at which level of Bloom's Taxonomy would you consider this IAS concept to be?" found that more than half of the modules that answered "Yes" to integrating the various concepts, did it at the Application level. The others were at the Knowledge level with one at Comprehension level. This question is asked to see if the concept is integrated at the right level for the year of study. Most IT modules, no matter the year of study, require that the work should be applied. This is reassuring because at least the information security concepts that are integrated are at the appropriate level of Bloom's Taxonomy.

The results from this approach highlight important concerns with respect to the integration of information security concepts into the IT curriculum. The applicability throughout the years increases, except at the second year where it drops drastically. The integration of the information security concepts shows a slight improvement after each year. The reason for the general lack of integration of security concepts for most of the modules, gathered from the comments, is that the IT lecturers do not have enough time within the already overloaded curriculum. Some IT lecturers stated that although not formally being assessed, some of these concepts are however being mentioned at some stage during their module.

In addition, it was argued by many of the participants that information security is not the main objective of their module. In the first two years of the programming modules the focus is on programming aspects, although in the third year the focus is still on programming aspects, information security does start becoming important in the capstone project. With most other modules (eg. Information Systems), the focus is on the analysis and design of the system. Information security is only mentioned in these modules because it is perceived to be more important in the actual execution phase of the SDLC. However, it is important for IT professionals to realise that information security needs to be integrated into all phases of the SDLC and not as an add-on or afterthought.

The following section provides the discussion of the common comments from the twelve participants of the questionnaires.

7. DISCUSSION

As can be derived from the case study findings, less than 50% of the IT Software Development undergraduate diploma modules are currently integrating security aspects.

IAS is advocated as both a knowledge area as well as a pervasive theme by the ACM but little guidance is given to IT lecturers with respect to integrating information security into their different modules as a pervasive theme. This has also become evident in the comments given by the NMMU, School of ICT undergraduate lecturers during the interviews that were conducted. More guidance should therefore be given by the ACM or at national level as to how IAS can be integrated into the IT undergraduate diploma as a pervasive theme.

A cause for concern is the low percentages throughout the findings of this research. The reason for this outcome, according to the comments, is that many of the security services and information security concepts are not deemed to be applicable by the IT lecturers of the various modules. This is not reassuring as the ACM specifically states that these security services and associated information security concepts should be integrated into the IT curriculum.

The most common response from the twelve participants whom are the IT lecturers at the NMMU, School of ICT is that they do not have time to incorporate information security concepts and information security into their current curriculum. Most of the IT lecturers feel that information security is not the main focus of their module. Most of the IT lecturers are under the impression that there is a module in the Software Development qualification that teaches students about information security concepts and information security. There are however, lecturers that would consider the integration of information security concepts as well as information security into their curriculum, if practical guidelines were made available to them.

8. CONCLUSION

Information security should be integrated as a pervasive theme within the IT Curriculum. This is currently not being integrated as it should at the NMMU, School of ICT. The results from the case study prove this. The results can help identify the problem areas such as the "Secure Coding" concept and thus steps can be taken to improve the overall integration of such concepts.

Some of the comments from the questionnaires mentioned that it could be possible to cross or combine some of the modules for example: Development Software and Information Systems. The content of these modules are complimentary. By crossing or combining these modules they could work together towards a single purpose and by doing so these information security concepts could be integrated easier.

In future, similar research could be conducted in other academic institutions to determine whether there is a general trend with regards the poor integration of information security within undergraduate computer-related curricula. Further research could also consider the development of guidelines to assist lecturers in the integration of these concepts.

9. ACKNOWLEDGEMENTS

- This work is based on the research supported in part by the National Research Foundation of South Africa
- Gert Jacobus Visser for his contribution in collecting and analyzing Approach 2's data;
- The NMMU, School of ICT's Software Development IT lecturers for their involvement in this research project.

10. REFERENCES

[1] ACM. (2013). *Curriculum Guidelines for Undergraduate Degree Programs in Computer Science*.

[2] ACM/IEEE-CS Joint Task Force for Computing Curricula. (2005). *Computing Curricula 2005: An Overview Report*.

[3] ACM/IEEE-CS. (2008). Information Technology 2008, *Curriculum Guidelines for Undergraduate Degree Programs in IT*.

[4] Amankwa, E., Loock, M., & Kritzinger, E. (2014). A Conceptual Analysis of Information Security Education Information Security Training and Information Security Awareness Definitions. *The 9th International Conference for Internet Technology and Secured Transactions.*

[5] Bloom, B. S. (1956). Taxonomy of Educational Objectives, Handbook I: The Cognitive Domain. New York: David McKey Co Inc.

[6] Border, C., & Holden, E. (2003). *Security Education within the IT Curriculum*. (pp. 256-257).

[7] Futcher, L. & Van Niekerk, J., 2011. Towards a Pervasive Information Assurance Security Educational Model for Information Technology Curricula. In F. Ronald C, Dodge Jr & Lynn, ed. Proceedings of the 7th World Information Security Education Conference. Lucerne, Switzerland: Springer Berlin Heidelberg, pp. 47–54.

[8] ISO/IEC. (1989). ISO/IEC 7498-2. Information Processing Systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture. Switzerland: ISO/IEC.

[9] Katsikas, S. K. (2000). Health care management and information systems security. Awareness, training or education.

[10] Taylor, B., & Azadegan, S. (2008). Moving Beyond Security Tracks. Integrating Security in CS0 and CS1.

[11] Whitman, M. E., & Mattord, H. J. (2010). Management of Information security. Course Technology, Cengage Learning.

[12] Wilson, M., & Hash, J. (2003). Building an information technology security awareness and training program. *National Institute of Standards and Technology*.

[13] Yasinsac, A. (2002). Information Security Curricula in Computer Science Departments: Theory and Practice. *The George Washington University Journal of Information Security, 1(2),* 2.

[14] Yin, R. K. (1994). Case Study Research. In Design and Methods. Thousand Oaks: Sage

Appendix A2

An Educators Perspective of Integrating Information Security into Undergraduate Computing Curricula

An Educators Perspective of Integrating Information Security into Undergraduate Computing Curricula

L.G. Gomana, L.A. Futcher and K. Thomson

Centre for Research in Information and Cyber Security, Nelson Mandela Metropolitan University, Port Elizabeth, South Africa

e-mail: {s210031492, lynn.futcher, kerry-lynn.thomson}@nmmu.ac.za

Abstract

Information is an integral part of our everyday lives and organisations need to have their information and related systems protected from various threats that exist. Therefore, information security education is of vital importance to all computing learners. It is the duty of higher education institutions to ensure that information security is pervasively integrated into the undergraduate computing curriculum. This will ensure that security is addressed multiple times, in multiple classes. Furthermore, this could ensure that higher education institutions produce computing graduates that possess fundamental information security knowledge, skills and understanding. This, in turn, will provide computing graduates with the ability to combat information security related threats. This paper briefly reviews existing literature relating to information security in higher education. Furthermore, it explores various South African educators' perspectives on the pervasive integration of information security into undergraduate computing curricula. This was determined through a semi-structured interview supported by a questionnaire. Furthermore, the participants of this research study were educators in the Computer Science, Information Systems, and Information Technology fields. The results indicate that there are various challenges in South Africa regarding the pervasive integration of information security into undergraduate computing curricula.

Keywords

Information Security, Information Security Education, Computing Curricula, Computing Graduates, Pervasive Information Security

1. Introduction

Information as an asset is subject to various security threats, whether deliberate or accidental. The related processes, systems, networks, and people have inherent vulnerabilities which could be exploited by such threats. These threats include viruses, worms, Trojan horses, Denial of Service (DoS) attacks and malware, just to name a few (ISO/IEC, 2013). Information security is the protection of information assets from various threats, which can compromise their confidentiality, integrity, and availability. Whitman & Mattord (2010) suggest that the protection of information cannot only be ensured through the application of security policies, but also through education.

In terms of this research, information security education focuses on providing computing graduates with insight and understanding of information security and should integrate fundamental information security concepts. This research argues towards the pervasive integration of information security into the Computer Science (CS), Information Systems (IS), and Information Technology (IT) fields as this could ensure that these qualifications produce graduates who are capable of pro-active response to information security threats (NIST 2003). The Association for Computing Machinery (ACM), the Association for Information Systems (AIS), and the IEEE Computer Society (IEEE-CS) play an important role in education and curricula development. They state that computing graduates are required to possess information security skills, knowledge, and understanding as they typically will be working with the technological systems of an organisation. Important organisational information is contained in these various systems (ACM/AIS/IEEE - CS, 2005).

Security breaches can occur where different components of a system interface, whether in the interface between different computers in a networked application, or across the interface between the user and the other components of the system. An awareness and understanding of the possible security breaches would give computing graduates the ability to identify and design high-level solutions that are less likely to put the organisation's information assets at risk and that will protect the organisation from various security threats (ACM/IEEE - CS, 2008; ACM/AIS, 2010).

During the deliberations of the Special Interest Group for Information Technology Education (SIGITE) Curriculum Committee, several topics emerged that were considered essential. These essential topics did not seem to belong in a single specific knowledge area or unit and were referred to as pervasive themes. One of these pervasive themes is Information Assurance and Security (IAS) (SIGITE Curriculum Committee, 2005). IAS is intended to protect and defend information and the associated information systems from threats (ACM/IEEE - CS 2013). IAS as a knowledge area should be addressed multiple times in multiple classes (ACM/IEEE - CS, 2008).

One of the ways in which a topic can be integrated as a pervasive theme into multiple knowledge areas or units is with the thread approach. Through the thread approach, pervasive themes can be integrated into the curriculum without changing the essence of the curriculum. Furthermore, individual educators could develop material at their own pace and change the syllabus gradually. This approach would require material on information security to be embedded into the current curricula. By integrating information security as a pervasive theme in multiple knowledge areas or units, students could learn to appreciate the importance of information security as an underlying theme across the curriculum which can help avoid the isolation of knowledge units. Furthermore, the thread approach provides exposure to smaller units of knowledge over a longer period of time allowing students to reflect and better assimilate the basic concepts of information security (Perrone et al. 2005).

Although the ACM defines IAS both as a knowledge area and as a pervasive theme, there is inadequate guidance provided with respect to assisting computing educators in pervasively integrating information security into their various modules (Futcher & Van Niekerk, 2011).

2. Purpose of the study

The main purpose of this study was to determine South African educators' perspectives on pervasively integrating information security into undergraduate computing curricula. This was achieved through addressing four key research objectives. Table 1 depicts the objectives of this research and defines the aim of each.

Research Objective	
Research Objective 1	To determine computing educators' perspectives on the pervasive integration of information security into undergraduate computing curricula
Research Objective 2	To determine the current integration of information security into curricula
Research Objective 3	To determine which fundamental information security concepts should be integrated into undergraduate computing curricula as a pervasive theme
Research Objective 4	To identify possible approaches for integrating an information security concept into computing curricula and the related challenges

Table 1: Research Objectives

The interview process aimed at achieving the objectives as stated in Table 1. This was supported by semi-structured questions to ensure these objectives were met.

3. Research Process

3.1. Participants

The study included ten participants who were all educators in either CS, IS or IT. These participants were from three universities in the Eastern Cape region of South Africa. Three of the participants were Professors, six were Senior Lecturers, and one participant was a Junior Lecturer. Participation in the study was voluntary.

3.2. Interview Process

A semi-structured interview was conducted with each of the ten participants of this study. The semi-structured interview was supported by a questionnaire. This questionnaire was structured according to the four research objectives as shown in Table 1. At the end of the interview, each of the participants was asked to complete an information security concepts checklist.

The purpose of the checklist was to determine the fundamental information security concepts which should be pervasively integrated into undergraduate computing curricula. When completing the checklist, the participants were encouraged to provide a brief comment as to why they thought the specific concept should or should not be regarded as a fundamental information security concept.

4. Results and Findings

This section presents the results and findings of this study according to the specified research objectives.

4.1. Research Objective 1

The first research objective was achieved through the questions depicted in Table 2.

Question 1	What is your perspective on the importance of information security education to undergraduate computing learners?
Question 2	What is your perspective on the pervasive integration of information security into computing curricula?
Question 3	What is the department/colleagues perspective on the pervasive integration of information security into computing curricula?
Question 4	Has your department ever had a formal discussion regarding information security?

Table 2: Research Objective 1 Questions

From the study conducted, there was general consensus that information security education is important to computing learners and that it should be part of the computing curriculum. In support of this, it was mentioned that information security education is critical from the first to the final year of study. In so doing, it could assist with preparing learners, and most importantly graduates with skills to protect themselves, their personal information, as well as organisational information. Learners need to understand the various threats that exist pertaining to information security in order for them to be able to combat those threats within organisations.

However, despite the general consensus, some participants were not sure as to whether information security should be pervasively integrated into the curriculum. A comment was made that a module should focus on teaching the content of that particular module. In order to be successfully integrated, it needs to be done in a manner that complements the module rather than taking away from the main focus and content of that module. Some participants also felt that it could be difficult for information security to be integrated into certain modules.

Pervasive integration implies that fundamental information security concepts should be taught in multiple modules to ensure that relevant skills, knowledge, and understanding are transferred to the learners across these modules. This, however, was deemed to be unnecessary duplication by some participants. It was suggested that fundamental information security concepts be gradually introduced into the first year to final year modules so that learners understand them better to prevent them from being taught all the concepts at once.

With regards to their colleagues, it was generally agreed that they would consider integrating information security concepts into their modules. However, it was mentioned that in many cases the curriculum was already overloaded and therefore time would not allow for such integration. In some cases, it was thought that information security is addressed in another module within the curriculum.

Some of the participants indicated that many educators may not be aware of the importance of information security in computing education and would, therefore, need to be convinced. However, educators are often resistant to change and would perceive the integration of another topic such as information security into their modules as additional work.

Responses regarding formal information security discussions highlighted that the extent to which this is done varies extensively across the various departments and higher education institutions.

4.2. Research Objective 2

The second research objective was to determine the current integration of information security into computing curricula. Table 3 depicts the three questions related to this research objective as well as the corresponding responses.

Detailed Question		Yes	No
Question 5	Does the department have a security-related module that is taught to all undergraduate computing learners?	1	9
Question 6	Do you integrate information security into your module?	7	3
Question 6b	If Yes, do you assess information security within your module?	2	5

Table 3: Research Objective 2 Questions

From Table 3 it is clear that most departments do not currently have a specific security-related module that is taught to all undergraduate computing learners. In most cases, this is only done at fourth-year level. One participant mentioned that such a module did exist in their department but that the module was discontinued when the curriculum was changed.

Seven of the participants indicated that they do integrate information security into their module. However, it is only assessed by two participants. It was mentioned that they did not integrate information security because they do not perceive it to be relevant to their module. In certain instances, the educators have already been forced to integrate Human Immunodeficiency Virus (HIV) and Acquired Immune Deficiency Syndrome (AIDS) education into their modules. Some educators understandably would prefer to retain the core focus of their modules.

4.3. Research Objective 3

The third research objective comprised of one question, which was in the form of a checklist of twenty-three information security concepts.

The list of the fundamental information security concepts that should be pervasively integrated into undergraduate computing curricula was derived from the security services and security aspects adapted from the ISO/IEC 7498-2 (1989) standard, Whitman & Mattord (2010), from an analysis of the IAS knowledge area and the related units within the ACM/IEEE-CS in their ‘Information Technology 2008, Curriculum Guidelines for Undergraduate Degree Programs in Information Technology’ document (ACM/IEEE - CS, 2008) and in the ‘Computer Science Curriculum 2013’ document (ACM/IEEE - CS 2013). The information security concepts identified include, but are not limited to authentication; confidentiality, integrity and availability; cryptography; digital forensics, disaster recovery, accountability, and privacy.

Nine of the participants completed this checklist.

Question 7	What fundamental information security concepts do you think should be pervasively integrated into undergraduate computing curricula?

Table 4: Research Objective 3 Question

For the purposes of this research, any concept where six or more participants indicated that the information security concept should be pervasively integrated will be regarded as a fundamental information security concept.

In addition, the participants were encouraged to provide a brief comment as to why they think the specific concept should or should not be pervasively integrated into undergraduate computing curricula.

Figure 1 shows the results of Question 7. All participants indicated that authentication, secure principles, secure SDLC and security awareness should be considered as fundamental information security concepts.

However, the concepts of non-repudiation/non-denial, cryptography, intrusion detection, and forensics are considered as non-fundamental concepts. Participants indicated that these concepts should not be pervasively integrated and should rather be taught in more advanced modules, for example, in the fourth year of study. Furthermore, cryptography and digital forensics were seen as specialist areas in industry and, therefore, not required for pervasive integration.

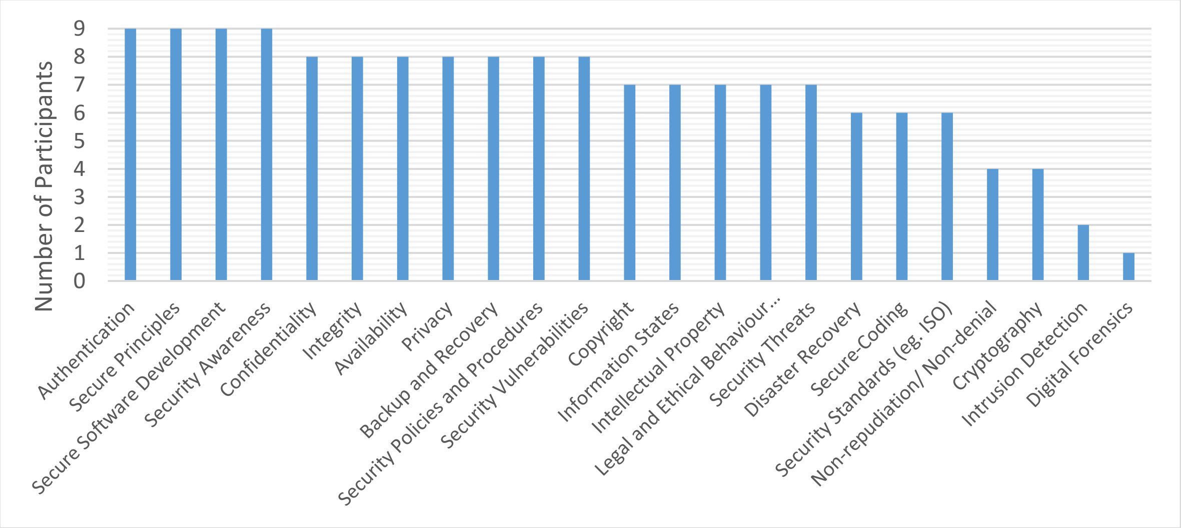

Figure 1: The fundamental information security concepts

As seen in Figure 1, many of the information security concepts were seen by the participants as being important to integrate pervasively into the undergraduate computing curricula.

4.4. Research Objective 4

Table 5 depicts the questions that were asked to achieve the final research objective for this study.

Question 8	Do you have any ideas on how to pervasively integrate information security concepts into various undergraduate computing modules?
Question 9	What challenges do you foresee in the pervasive integration of information security concepts into undergraduate computing curricula?
Question 10	Do you think computing educators would be able to pervasively integrate these fundamental information security concepts into their various modules?

Table 5: Research Objective 3 Questions

Many participants indicated that a good way to integrate information security concepts into particular modules would be to relate or contextualise these concepts to make them as relevant as possible for those particular modules. For example, when teaching Networks, confidentiality, integrity, and availability could be discussed within the context of firewalls and intrusion prevention systems. It is also important to integrate relevant information security concepts that the learners will find interesting. Furthermore, it was suggested that social or interactive discussions related to the students' experience with regard to information security may be beneficial, thereby integrating the concepts through discussion as well as into the theory of the modules. A few of the participants proposed that information security concepts should be pervasively integrated from the first to the final year of study and should be assessed through a capstone-type project towards their final year.

It was also suggested that social media and smartphones, as well as the benefits of security and risks associated with a lack of security, be used as frames of reference to convey certain information security concepts, thereby engaging students through platforms they are familiar with. A further suggestion was that each fundamental information security concept should be covered in at least one of the undergraduate modules. Table 6 below depicts an example of how an information security concept can be pervasively integrated into one or more modules.

Fundamental Concepts	Databases	Programming	Operating Systems	Networks
Privacy	X		X	X
Backup and Recovery	X			X
Security Threats	X	X	X	X
Security Vulnerabilities	X	X	X	X
Legal and Ethical Behaviour	X			X
Confidentiality		X	X	
Integrity		X	X	
Availability		X	X	
Secure coding		X		

Table 6: Mapping of Fundamental Information Security Concepts to Modules

It would be ideal for a single fundamental information security concept to be integrated repeatedly into various modules so that they are taught to learners in multiple classes and multiple times. This could assist the learners in gaining the skills, knowledge, and understanding of these fundamental information security concepts from a different perspective in each module. Many of the fundamental concepts are repeated in other modules as shown in Table 6. In the Database module, for example, the fundamental concepts of privacy, backup and recovery, security threats, security vulnerabilities, and legal and ethical behaviour can be integrated and taught from a database perspective. This could ensure that the concepts complement the module rather than take away the focus and the purpose of that specific module. Similarly, the fundamental concepts that could be integrated and taught from a Programming, Operating Systems, and Network perspective are shown in Table 6. It was also highlighted by many participants that for any of these ideas or strategies to work, educators must be motivated and willing to integrate these information security concepts into their particular module.

The challenge that all participants highlighted was that there is often not enough time to work through current module content and if additional content, for example, information security concepts, needed to be included, this would prove very challenging. It was suggested that the planning of how and where these concepts would be integrated should be done at the beginning of each year to ensure that each concept is addressed multiple times in multiple modules. Furthermore, a few of the participants indicated that a challenge to pervasively integrating information security concepts into various modules may be resistance from educators as they are reluctant to change, and their 'buy in' would be necessary for the pervasive integration to be successful. It was also suggested that educators may be unaware, or lack knowledge, regarding information security concepts, or may not be confident in teaching these concepts. Therefore, it was suggested that, in order to facilitate their integration, the fundamental information security concepts should be provided to educators in a format that would make it easy for them to understand and convey to learners.

Most participants indicated that there would, most likely, be resistance to the added workload required to integrate the information security concepts into modules and that educators are, for the most part, resistant to change. One participant indicated that he did not think that educators would be able to integrate these fundamental security concepts into their modules and it would depend on what the educators would have to do. To assist with this, it was suggested that examples of how educators could integrate these concepts into their modules and how to make these examples relevant to their specific module and context would benefit educators, particularly those whose modules are not security focused. However, the participants also indicated that educators would need to be convinced that the integration of information security concepts is necessary and it would be important to show educators the value of information security education, to increase their willingness to integrate these concepts into their modules.

5. Conclusion

Information security is a fundamental and common topic that can fit into any computing module. However, the appropriate information security concepts should be identified for each specific module to ensure the effective integration of these information security concepts into the various computing modules. This will ensure that computing graduates are equipped with the required information security skills, knowledge, and understanding. The primary aim of this study was to determine South African computing educators' perspectives on the pervasive integration of information security into computing curricula. This was achieved through the four research objectives specified in Section 2. The results and findings from this study indicated that these computing educators are aware of the importance and generally support the pervasive integration of information security into undergraduate computing curricula. However, they do not currently integrate information security effectively into their various modules. Many computing educators still need to be made aware of the importance of information security education to computing learners and they require assistance to ensure the effective integration of these information security concepts into the various modules. Thus, further research is required to determine how these fundamental information security concepts can be seamlessly integrated into the various computing modules. The limitations of this study are that this study was an exploratory study conducted in South Africa. Generalization of the study's findings to other countries cannot be ensured.

6. Acknowledgements

The financial assistance of the National Research Foundation (NRF) towards this research is hereby acknowledged. Opinions expressed and conclusions arrived at, are those of the authors, and are not necessarily to be attributed to the NRF.

7. References

ACM/AIS, 2010. IS 2010: Curriculum guidelines for undergraduate degree programs in information systems. Communications of the Association for Information Systems, 26, pp.359– 428.

ACM/AIS/IEEE - Computer Society, 2005. Computing Curricula 2005. ACM Journal of Educational Resources in Computing, 1(3), pp.1–240.

ACM/IEEE - Computer Society, 2008. Information Technology 2008 Curriculum Guidelines for Undergraduate Degree Programs in Information Technology. Current Practice, pp.1–139.

ACM/IEEE - CS, 2013. Computer Science Curricula 2013. Practice, pp.1–172.

Futcher, L. & Van Niekerk, J., 2011. Towards a Pervasive Information Assurance Security Educational Model for Information Technology Curricula. In F. Ronald C, Dodge Jr & Lynn, ed. Proceedings of the 7th World Information Security Education Conference. Lucerne, Switzerland: Springer Berlin Heidelberg, pp. 47–54.

ISO/IEC 27002:2013, 2013. ISO / IEC 27002 Information technology — Security techniques

— Code of practice for information security controls 2nd ed., Switzerland: ISO.

ISO/IEC 7498-2, 1989. Information Processing Systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture, Switzerland: ISO/IEC.

NIST, 2003. Building an Information Technology Security Awareness and Training Program. NIST SP 800-50, (October), pp.1–38. Available at: http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf.

Perrone, L.F., Aburdene, M. & Meng, X., 2005. Approaches to undergraduate instruction in computer security. 2005 ASEE Annual Conference and Exposition: The Changing Landscape of Engineering and Technology Education in a Global World, pp.651–663.

Special Interest Group on Information Technology Education Curriculum Committee, 2005.

Computing Curriculum Information Technology Volume,

Whitman, M.E. & Mattord, H.J., 2010. Management of Information security 3rd ed., Course Technology, Cengage Learning.

Appendix B1

Survey Questionnaire

Pervasively integrating information security concepts into computing curricula

Name:	**Date of Interview:**	**Module Code:**	**Level:**	**Qualification:**	**Involved in Research:**
		Module Name:	**1st year** **2nd year** **3rd year** **4th year**	CS /IS/ IT	**Yes** **No**
	Role at University:			**Class Size:**	

Survey Objective 1: To determine computing educators' perspectives on the integration of information security into undergraduate computing curricula.

1. What is your perspective on the importance of information security education to undergraduate computing students?

2. What is your perspective on the pervasive integration of information security into undergraduate computing curricula?

3. What is the department/colleagues perspective on the pervasive integration of information security into undergraduate computing curricula?

4. Has your department ever had a formal discussion regarding information security?

Survey Objective 2: To determine computing educators' perspectives on the current integration of information security into their curricula.

5. Does the department have a security-related module that is taught to all undergraduate computing students?

6. Do you integrate information security into your module?
    a. If yes, do you assess it?
    b. If no, why not?

Survey Objective 3: To determine which fundamental information security concepts should be integrated into undergraduate computing curricula as a pervasive theme

7. What fundamental information security concepts do you think should be pervasively integrated into undergraduate computing curricula?

Survey Objective 4: To identify possible ideas and challenges for integrating information security concepts into computing curricula

8. Do you have any ideas on how to pervasively integrate information security concepts into various undergraduate computing modules?

9. What challenges do you foresee in the pervasive integration of information security concepts into undergraduate computing curricula?

10. Do you think computing educators would be able to pervasively integrate these fundamental information security concepts into their various modules?

Appendix B2

Survey Questionnaire – Checklist

Lecturer name:

Question 7: What fundamental information security concepts do you think should be pervasively integrated into undergraduate computing curricula?

Information security concept	Yes	No	Comment: Why, or why not?
Authentication			
Confidentiality			
Integrity			
Availability			
Non-repudiation/Non-denial			
Cryptography			
Digital Forensics			
Disaster Recovery			
Privacy			
Copyright			
Backup and Recovery			
Information States			
Intellectual Property			
Intrusion Detection			
Legal and Ethical Behaviour Issues in Computing			
Secure Principles			
Secure Software Development			
Secure-Coding			
Security Awareness			
Security Policies and Procedures			
Security Standards (eg. ISO)			
Security Threats			
Security Vulnerabilities			

Appendix C1

Validation Questionnaire – Director of School, Head of Department and Educators

Towards a Framework for Integrating Information Security Concepts into Undergraduate Computing Curricula – Framework Validation (Director of School, Head of Department and Educators)

Name:	**Date of Interview:**	**Qualification**: CS /IS/ IT	**Involved in Research:** **Yes** **No**
	Role at University:		

Section 1: Perspectives on Information Security - To elicit the elites' opinions regarding information security

Question 1.1: Do you regard information security as important?

Question 1.2: Is information security important to undergraduate students in your department? Please provide a reason for your response.

Question 1.3: Should information security be taught as a single module or should it be pervasively integrated into various modules in the IT qualification? Please provide a reason for your response.

Question 1.4: Would the pervasive integration of information security into undergraduate curricula within the department benefit students?

Section 2: Perceived Challenges - To determine the perceived challenges regarding the pervasive integration of information security
Question 2.1: What challenges within your department would make the pervasive integration of information security difficult?
Question 2.2: Do you foresee any challenges with pervasively integrating fundamental information security concepts into your module(s)? Please provide a reason for your answer.
Question 2.3: What measures can be put in place to overcome the challenges stated in *Question 2.2*, if you answered yes?
Section 3: Proposed Framework - To verify the feasibility of the proposed information security education framework
Question 3.1: Has the department had a formal or informal discussion about information security?
Question 3.2: Do the educators within your department have information security knowledge that will enable them to pervasively integrate the fundamental information security concepts into their various modules?
Question 3.3: Do you (Director of the School or Head of Department) support the integration of information security into various modules within your department?
Question 3.4: Would the proposed framework be feasible within your **department**?
Question 3.7: In your opinion, does this framework need improvements?
Question 3.8: If you answered yes to *Question 3.7*, please state how the framework can be improved.

Section 4: Implementation of Proposed Framework - To determine how the computing educator elites would implement the fundamental information security concepts into their modules
Question 4.1: In which subject area do you teach?
Question 4.2: Please select all fundamental information security concepts that could be pervasively integrated into module(s) within your subject area.
Question 4.3: Please provide an example of how one of the concepts that you selected in Question 4.2 can be pervasively integrated into one of your modules.

Appendix C2

Validation Brief

Towards a Framework for Pervasively Integrating Information Security into Undergraduate Computing curricula

Dear Elite Interviewee,

Thank you for being willing to act as an elite interviewee for the validation of this framework. Please see below a brief background of an elite interview. The process of validating this framework will begin with a brief presentation by me to introduce the framework, this will be followed by a semi-structured interview supported by a questionnaire to elicit information from you regarding the proposed framework. As stated in the previous email, this should take no longer than 30 minutes.

Elite Interviews:

The term “elite” is applied to a person or group of people that are generally considered to be important. Furthermore, the idea of elite involves the formation of identities in relation to concepts of professionals and professionalism and points at the power they have and that is associated with them. The “elite” can typically be seen to have knowledge, influence, control and power in a given setting or situation (Moore & Stokes, 2012). An elite interview, therefore, is interviewing an expert or an individual who can be considered an elite person in their field. The aim of this elite interview is thus to gain feedback from you, as an elite that is knowledgeable in you subject area, on how feasible the proposed framework is and to suggest changes and improvements to the proposed framework.

Background – Research Project:

The problem identified for this research is: **“*Currently, no generally used framework exists to aid the pervasive integration of information security into undergraduate computing curricula.*”**

Various research methods were used to solve the identified problem. A literature review relating to information security and information security within higher education was conducted. In the reviewed literature, it was stated that information is an important organisational asset which needs to be protected from potential threats that can arise against it. It was further stated that the roles and responsibilities computing graduates acquire as organisational employees require them to possess information security skills, knowledge and understanding to ensure the protection of the organisational information housed in the information systems that they design, develop, implement and maintain.

Results and findings from a survey that was conducted for this research indicated that in most departments there was no security-related module that was taught to all undergraduate computing learners. Further findings indicated that a security-related module is only offered to computing learners at fourth-year level. However, this module is often offered as an elective. This means that not all learners who proceed to fourth-year will take this module. They would have to elect the relevant security-related module in order to develop the necessary information security knowledge, skills and understanding required upon graduating from the particular higher education institution. Some learners simply do not proceed to this level and they exit higher education institutions and go into organisations without ever having been exposed to information security education.

Due to the importance of information to organisations and the lack of information security education of all undergraduate computing learners, it was clear and evident that an approach to integrate information security education into computing curricula needed to be identified. Key role players that provide guidance relating to computing curricula have developed computing curricula guidelines and recommendations for higher education institutions for decades. These key role players provided guidelines stating that information security should be pervasively integrated into computing curricula. The pervasive integration of information security means that information security is added into an existing module and is taught from that module's perspective.

Framework:

A framework was, therefore, developed to assist higher education institutions, computing departments and computing educators to pervasively integrate information security into multiple modules within their department. The successful integration of information security could ensure that undergraduate computing learners are taught information security from various perspectives in each module. Furthermore, this could also ensure that higher education institutions produce computing graduates from undergraduate qualifications that possess information security skills, knowledge and understanding to protect organisational information systems and related information assets.

Appendix D1

Editor’s Letter

LoveToEdit

You Write. We Edit. You Love it.

20 March 2017

TO WHOM IT MAY CONCERN

REF: CONFIRMATION OF LANGUAGE EDITING SERVICES: LINDOKUHLE GCINA GOMANA.

I confirm that I have done Language Editing for Lindokuhle Gcina Gomana’s Dissertation titled:

Towards a Framework for the Integration of Information Security into Undergraduate Computing Curricula.

The Dissertation now conforms to Nelson Mandela Metropolitan University’s language editing standards. Yours sincerely

Sibanda

Lynn N Sibanda

Tel: 011 050 0376

Mobile: 071 989 0983

Email: lynn@lovetoedit.co.za

Member of the Professional Editors Guild

Professional EDITORS Guild