TOWARDS A FRAMEWORK FOR THE INTEGRATION OF INFORMATION SECURITY INTO UNDERGRADUATE COMPUTING CURRICULA

K-L. Thomson*
School of Information and Communication Technology
Cisco Networking Academy
e-mail: kerry-lynn.thomson@mandela.ac.za

L. A. Futcher*
email: lynn.futcher@mandela.ac.za

L. Gomana*
email: lindokuhle.gomana@mandela.ac.za

*School of Information and Communication Technology,
Nelson Mandela University
Port Elizabeth, South Africa

ABSTRACT

With the rapid rise of the world's reliance on technology, organisations are facing an increased demand for a security savvy workforce. It is, therefore, important that computing graduates possess the necessary information security skills, knowledge and understanding that can enable them to perform their organisational roles and responsibilities in a secure manner. The information security skills, knowledge and understanding can be acquired through a computing qualification that is offered at a higher education institution. The ACM/IEEE, as a key role player that provides educational guidelines for the development of computing curricula, recommends that information security should be pervasively integrated into the curriculum. However, its guidelines and recommendations do not provide sufficient guidance on *"how"* this can be done. This study therefore, proposes a framework to address the pervasive integration of information security into computing curricula. Various research methods were used in this study. Firstly, a literature review was undertaken to inform the various phases and elements of the proposed framework. The literature reviewed included relevant information security education standards and best practices, including key computing curricular guidelines. Secondly, a survey in the form of semi-structured interviews supported by a questionnaire were used to elicit computing educators' perspectives on information security education in a South African context, including the perceived challenges and ideas on how to integrate information security into the curricula. Finally, elite interviews were conducted to validate the proposed framework. It is envisaged that the proposed framework can assist computing departments and undergraduate computing educators in the integration of

South African Journal of Higher Education http://dx.doi.org/10.20853/33-3-3011
Volume 33 | Number 3 | 2019 | pages 155–175 eISSN 1753-5913

information security into the curricula thereby helping to 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.

Keywords: information security concepts, undergraduate computing curricula, pervasive theme, information security education framework

INTRODUCTION

For many years, the human factor has been referred to as the "weakest link" in securing an organisation's information assets. According to Hinson (2005), when it comes to the protection of information assets, the human factor is an immediate, close and dangerous threat agent that can cause vulnerabilities to exploit information systems and related information assets. Amankwa, Loock and Kritzinger (2014) as well as 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. Amankwa et al. (2014) support this view when they argue that, "... 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".

Computing graduates, who in the context of this study are defined as graduates in the Computer Science (CS), Information Systems (IS) and Information Technology (IT) disciplines, upon graduating, typically become organisational employees. It can be argued, therefore, that the computing graduates should be required to possess adequate information security knowledge to perform their organisational roles and responsibilities in a secure manner. Further, it is important that computing students are taught information security to enable them to build secure information systems (Conti et al. 2003).

According to Futcher, Schroder and Von Solms (2010), as well as Talib, Khelifi and Ugurlu (2012), higher education institutions are responsible for producing computing graduates who possess adequate information security understanding that can enable them to manage organisational information assets securely. Furthermore, the computing students' information security education should result in graduates who are prepared for the challenges they will encounter in their organisational roles and responsibilities (Irvine, Chin and 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. These guidelines refer to the knowledge areas, units and learning outcomes when developing curricula. The ACM/IEEE curricula body of knowledge is structured in a three-tiered hierarchy, which is illustrated in Figure 1.

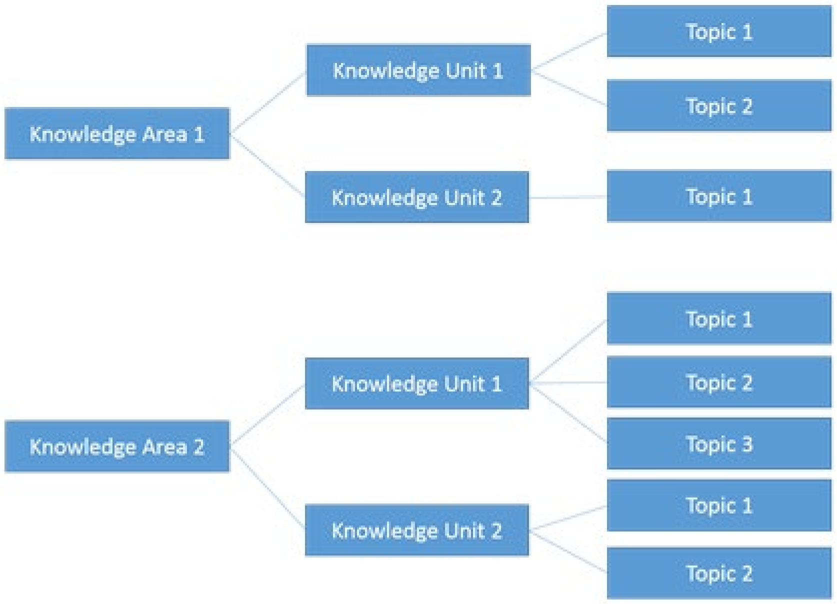

Figure 1: Body of Knowledge Structure (Dodge 2013)

As shown in Figure 1, the highest hierarchy level 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 to define the topics. These topics are at the lowest tier of the hierarchy (ACM/IEEE – IT 2008; ACM/IEEE – CS 2013).

During the Special Interest Group for Information Technology Education (SIGITE) Curriculum Committee's deliberations in 2005, several essential themes emerged. The 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 a knowledge area (ACM/IEEE – CS 2008, 2013; SIGITE Curriculum Committee 2005). According to the committee, a pervasive theme should be addressed multiple times, in multiple modules and from a different perspective in each module.

Although IAS is defined as a pervasive theme and a knowledge area, Futcher and Van Niekerk (2011) as well as 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) argue 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 study's primary aim was 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.

RESEARCH PROCESS

In order to achieve the study's aim, it was important that a systematic research process was followed. According to Rajasekar, Philominathan and Chinnathambi (2006), following an appropriate systematic research process allows the researcher to correctly achieve the specified study objectives. An initial literature review was conducted to determine a relevant problem in information security education. The identified problem was that not enough guidance is provided to computing educators on *"how"* to pervasively integrate information security into computing modules. Additional literature reviews were conducted to understand information security and the need for computing graduates to be educated in information security.

Furthermore, it was important to determine the computing educators' perspectives on information security in a South African context. In order to achieve this, a survey, in the form of semi-structured interviews supported by a questionnaire, was conducted. 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. Convenience sampling was used as these participants were easily accessible to the researcher. Through this survey, computing educator's perspectives on the integration of information security into undergraduate computing curricula and the current level of integration of information security in the curricula were determined. The survey was also used to determine which fundamental information security concepts should be integrated as a pervasive theme and it was also utilised to determine the possible ideas and challenges for integrating information security into undergraduate curricula. It must be noted that not all the survey results are presented in this article as other details can be found in two additional papers by Gomana, Futcher and Thomson (2015) as well as Gomana, Futcher and Thomson (2016). The literature review findings and the survey were used to argue towards the proposed framework. The research process that this study followed is illustrated in Figure 2.

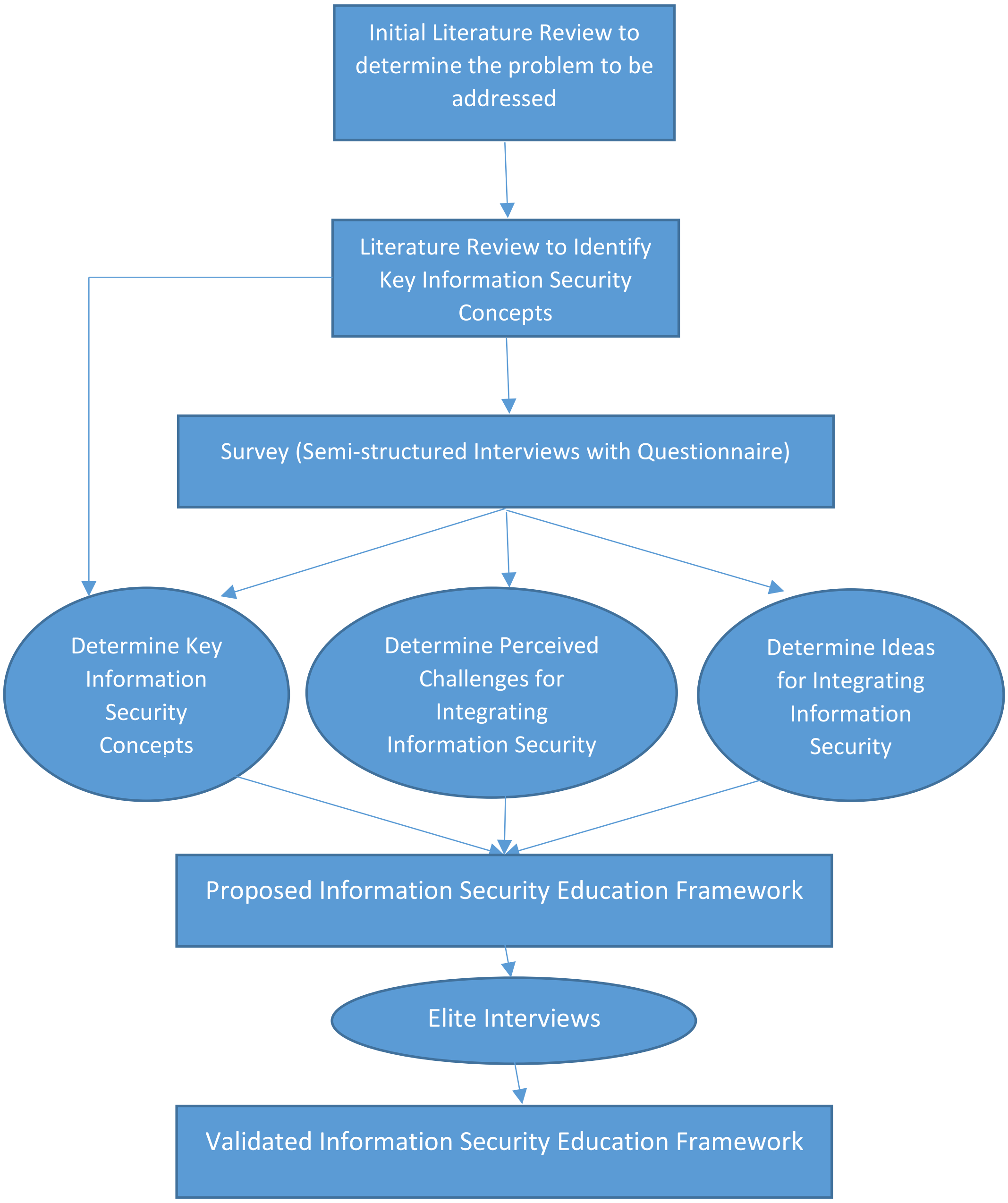
Initial Literature Review to determine the problem to be addressed
Literature Review to Identify Key Information Security Concepts
Survey (Semi-structured Interviews with Questionnaire)
Determine Key Information Security Concepts
Determine Perceived Challenges for Integrating Information Security
Determine Ideas for Integrating Information Security
Proposed Information Security Education Framework
Elite Interviews
Validated Information Security Education Framework

Figure 2: Research Process

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

The proposed Information Security Education Framework was validated through the use of elite interviews, supported by a questionnaire. Six elites were chosen from an IT department at a single higher education institution and included a Director of School, Head of Department and various IT 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.

Both the semi-structured interviews and the elite interviews were conducted by the researcher. No ethical clearance was required as the study posed no risk to the participants nor their associated higher education institutions.

KEY FINDINGS FROM SURVEY

As mentioned, the survey was conducted as semi-structured interviews supported by a questionnaire. It must be noted that the survey results and findings are based on the surveyed higher education institutions and cannot be generalised to all higher education institutions in South Africa. The purpose of the survey was to conduct a situational analysis on information security and related concepts, through the current perspectives of computing educators in higher education institutions in South Africa.

Survey participants indicated that in their higher education institutions, there is currently no security-related module taught to undergraduate computing students and 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 can 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 can 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.

Key information security concepts

One of the objectives of the survey was to determine the fundamental information security concepts that should be pervasively integrated into undergraduate computing curricula. The participants were given a separate questionnaire with a list of 23 information security concepts derived from the "Information Technology 2008, Curriculum Guidelines for Undergraduate Degree Programmes in Information Technology" document (ACM/IEEE – IT 2008), the "Computer Science Curriculum 2013" document (ACM/IEEE – CS, 2013), ISO Standards (ISO/IEC 7498-2 1989) and the "Management of Information Security" book (Whitman and Mattord 2014). It must be noted that the Information Technology Curricula 2017 (IT2017) had not been published at the time of the study. Even though 21 participants took part in the semi-structured interviews, only 19 completed the information security concept questionnaire. In terms of this study, any information security concept where 17 (89%) or more participants indicate that a concept should be pervasively integrated would be considered as a fundamental information security concept. The *authentication*, *secure principles*, *security awareness*, *confidentiality*, *integrity*, a*vailability*, *privacy*, *secure software development*, *backup and recovery*, *legal and ethical behaviour issues*, *security threats* and *security vulnerabilities concepts* were determined to be fundamental by the participants.

Integrating information security concepts into computing curricula

Another survey objective was to determine possible ideas and perceived challenges for integrating information security concepts into computing curricula. Participants indicated that in order for information security to be successfully integrated, it needs to be done in a manner that complements the module and information security should be contextualised for each module in which it is integrated. 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 as 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* could 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 it from its focus and purpose.

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, in order to prevent them from being taught all the fundamental information security concepts 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 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 to the final year of the qualification.

To further assist with the pervasive integration of fundamental information security concepts into computing curricula, it was suggested that information security concepts can be grouped and taught together to show students how the concepts relate. 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. In addition, the participants indicated that examples of how computing educators could integrate the fundamental information security concepts into their modules and how they could make these examples relevant to their specific module and context would benefit educators, particularly those whose modules are not security focused.

The perceived challenges for integrating information security into undergraduate computing curricula included that educators do not have enough time to work through the current curriculum and they could become overloaded by the inclusion of information security. Participants indicated that educators are often resistant to change and would have to be motivated to integrate these information security concepts into their particular modules. It was, therefore, suggested that the proposed integration of information security into undergraduate computing curricula be included as part of the departmental plan, for the department to show support for the integration and to provide directives to educators within the department. Participants also indicated that computing educators may lack the necessary information security "know-how" to enable them to integrate information security concepts. It would, therefore, be ideal to ensure that all computing educators within a department are aware of information security and the importance thereof. Computing educators should be convinced that information security concepts can be integrated into their modules without changing the core content. 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 in ensuring that it is not considered as an afterthought or abstract concept after designing, developing or implementing information systems.

PHASES OF THE INFORMATION SECURITY EDUCATION FRAMEWORK

The proposed framework is structured in three phases, namely: Guideline Development, Planning and Implementation. These phases were based on typical curriculum development cycles, which include situation and job analysis, planning, implementation, evaluation and stakeholder participation (Institute of Progressive Education and Learning 2018).

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 phase helps to determine the fundamental information security concepts which can be pervasively integrated 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 curricula. The Implementation Phase aims to ensure that the identified fundamental information security concepts are pervasively integrated into various modules.

Phase 1: Guideline Development

Figure 3 depicts an illustration of the first phase of the proposed framework. This section will discuss each of the elements in the figure.

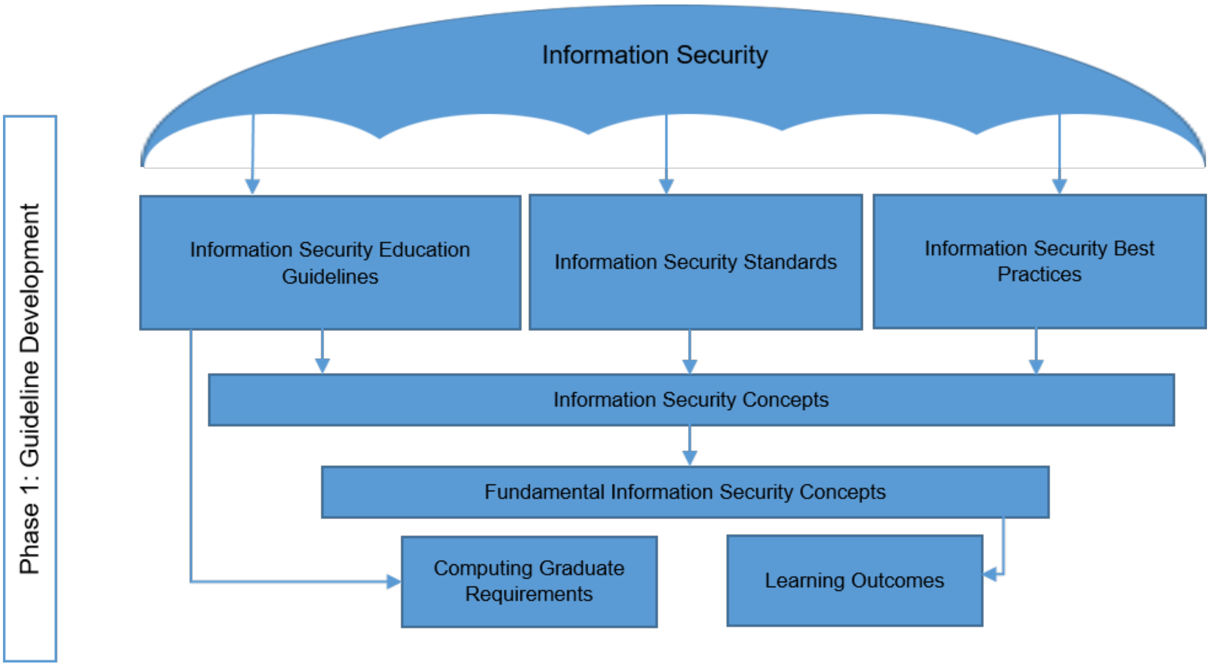
Information Security
Phase 1: Guideline Development
Information Security Education Guidelines
Information Security Standards
Information Security Best Practices
Information Security Concepts
Fundamental Information Security Concepts
Computing Graduate Requirements
Learning Outcomes

Figure 3: Phase 1 – Guideline Development Elements

Information security

Information Security can be considered as the “umbrella” concept that includes information systems and information assets. Information Security should be taught to all CS, IS and IT computing disciplines. It is, therefore, considered as the overarching discipline for the framework and as such should inform all phases of the proposed framework.

Information security education guidelines, standards, best practices

To identify the Information Security Concepts that should be pervasively integrated into a computing curriculum, a literature review should be conducted by the key stakeholders in the computing departments. Relevant literature that can be used to derive these 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 documents would include those published by the ACM/AIS/IEEE;
- *Information Security Standards* – These can include documents that provide information security standards, such as those provided by the International Organization for Standardization (ISO);
- *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);
- *Information Security Textbooks* – These can include authoritative textbooks on information security, such as those from Whitman and Mattord;
- *Information Security Education Working Groups* – These can include international working groups specialising in information security education, such as the International Federation for Information Processing (IFIP) Working Group 11.8.

From reviewing the literature regarding Information Security Education Guidelines, Standards and Best Practices, computing departments can identify Information Security Concepts that are important to their undergraduate computing students.

Information security concepts

A few of the challenges identified through the survey that computing educators are facing regarding the integration of information security into computing curricula are that the existing undergraduate computing curricula are over-extended and that information security is a broad area of study. Therefore, it is 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 of information security would allow 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. However, in order to pervasively integrate information security into undergraduate computing curricula, the Information Security Concepts need to be identified. Pervasively integrating all the 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 identified concepts as it may already be over-extended. It would, therefore, be important for each computing department to identify the Fundamental Information Security Concepts that are the most relevant to their qualification.

Fundamental information security concepts

This study proposes that the identified Information Security Concepts must be narrowed down to a manageable number by indicating which 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 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, they could review their integration of information security after a period of time, for example, a year later, during which they could add or remove concepts as deemed necessary.

This study proposes for departments to elicit the perspectives of their computing educators to narrow down the list of the identified Fundamental Information Security Concepts. This could be done through an investigation such as a discussion or a survey carried out amongst the computing educators. After conducting such an investigation, a list of the identified concepts that should be pervasively integrated into the various modules within their computing department could be derived.

Computing graduate requirements

During the Guideline Development Phase, it is important for computing departments to identify Computing Graduate Requirements from various literature sources, including, but not limited to those documents published by the ACM/IEEE. For example, in the ACM/IEEE – IT (2017) document, part of the profile of an IT graduate includes "IT graduates have extensive practice with properly *securing* IT networks, applications, data centres and online services. They seek *secure* technology solutions without unduly adversely affecting the ability of users to accomplish their goals." Further, the report requires, "that all computing programs include information assurance and security principles and practices in their curricula". Therefore, it is important that information security is taught to all CS, IS and IT undergraduate students in the computing discipline, as these students are required to possess information security skills, knowledge and understanding.

Learning outcomes

Each of the IAS knowledge units that come from the ACM/IEEE-CS contains a collection of Information Security Concepts (topics) and each concept has Learning Outcomes that are associated 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). For example, the CIA foundational concepts are linked to analysing the trade-offs of balancing key security properties' outcomes (Confidentiality, Integrity and Availability). Further, familiarity and usage are the desired levels of comprehension of each of the Learning Outcomes. For example, relating to usage, after learning about CIA, an undergraduate computing student should be able to use or apply the CIA's Fundamental Information Security Concepts. A further example relating to familiarity is one where students should know and should be able to understand the authentication, authorisation and access concepts (ACM/IEEE – CS 2013).

As seen in Figure 3, the elements of Computing Graduate Requirements and Learning Outcomes should be 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 could include the Director of School, Head of Department and computing educators. Furthermore, Computing Graduate Requirements, Fundamental Information Security Concepts and Learning Outcomes feed into the next phase of the proposed framework, the Planning Phase, by providing the basis for the “buy-in” or support of all stakeholders.

Phase 2: Planning

Figure 4 depicts an illustration of the second phase of the proposed framework. This section discusses each of the elements in the figure.

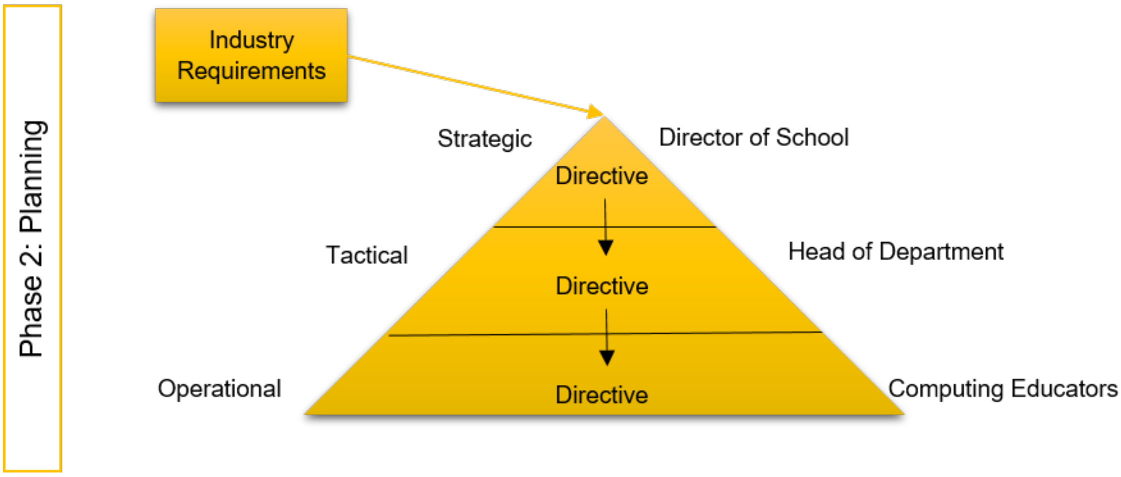

Figure 4: Phase 2 – Planning Elements

Industry requirements

The key computing curricular role players, for example, the ACM, provide fully reviewed, revised and enhanced guidelines as well as recommendations for the development of the undergraduate computing curricula every ten years, with a minor interim assessment at the fifth year mark. During the development process, the role players should consider the industry’s changing needs in terms of the necessary information security knowledge, skills and the understanding that the computing graduates are required to possess. According to Smith et al. (2005), it is necessary that computing departments incorporate the industry’s needs and requirements when teaching information security. However, findings from their study indicated that many higher education institutions were less focused on educating computing students on issues relevant to the industry. Therefore, there is a need for incorporating the industry’s requirements into computing education. Furthermore, information security education at higher education institutions should keep up with the industry’s information security requirements.

With guidelines and recommendations only being revised every five to ten years, it could be argued that there could be a gap as threats to information security and technology advance rapidly within that period. Therefore, in addition to Computing Graduate Requirements, Fundamental Information Security Concepts and Learning Outcomes, the industry’s computing students' requirements could also be used to get the "buy-in" of all stakeholders. These requirements to determine what industry requires of computing graduates could be obtained from a meeting held with an Industry Advisory Board. As computing graduates and organisational employees are required to possess information security skills, knowledge and understanding, it is important for higher education institutions to stay abreast of the industry's needs and they should adapt their curricula accordingly.

Direct/Control cycle

The board of directors and executive management are responsible for the overall well-being of an organisation (King 2009; Von Solms and 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 and Mattord 2014). 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 and Von Solms 2009). The Direct/Control Cycle divides organisational employees into three levels, namely (Von Solms and Von Solms 2006):

- The board of directors and executive management at the Strategic level;
- Senior and middle management at the Tactical level;
- Lower management and administration at the Operational level.

In a higher educational institution context, the Director of School would typically be at the Strategic level within their institution. The Strategic level provides directives to the Tactical level, mandating what should be carried out. 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. 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.

Through the survey, computing educators suggested that information security be included in the departmental plan. This 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. Furthermore, the directive for pervasively integrating information security should come from top management. As discussed, one of the challenges with pervasively integrating information security into undergraduate computing curricula is that some computing educators are resistant to change and 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 a 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. The outcome of the Planning Phase, through a course curriculum planning meeting, would be the identification of fundamental information security concepts that are relevant to the computing qualification. In addition, this would ensure the buy-in and a shared understanding of and commitment to the pervasive integration of these identified concepts into the relevant modules.

Phase 3: Implementation

Whitman and Mattord (2004) identify five academic approaches for integrating information security into computing curricula. The most used and preferred approach is the, "add information security concepts to existing modules" approach, as it is more effective to include information security throughout various modules rather than to add it as a single module. For example, programming could include the information security concept "*secure software development*", and "*backup and recovery*". Similarly, Perrone et al. (2005) describe three approaches for integrating computer security into the curriculum, one of which is the "thread approach". Through the "thread approach," information security can be integrated into the curriculum without drastically changing the module's core content. This approach does not require computing educators in the department to attend information security training, or similar, 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 it does not require additional isolated information security modules. The "thread approach" provides exposure to smaller units of knowledge over a longer period of time thereby 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. Figure 5 depicts an illustration of the third phase of the proposed framework.

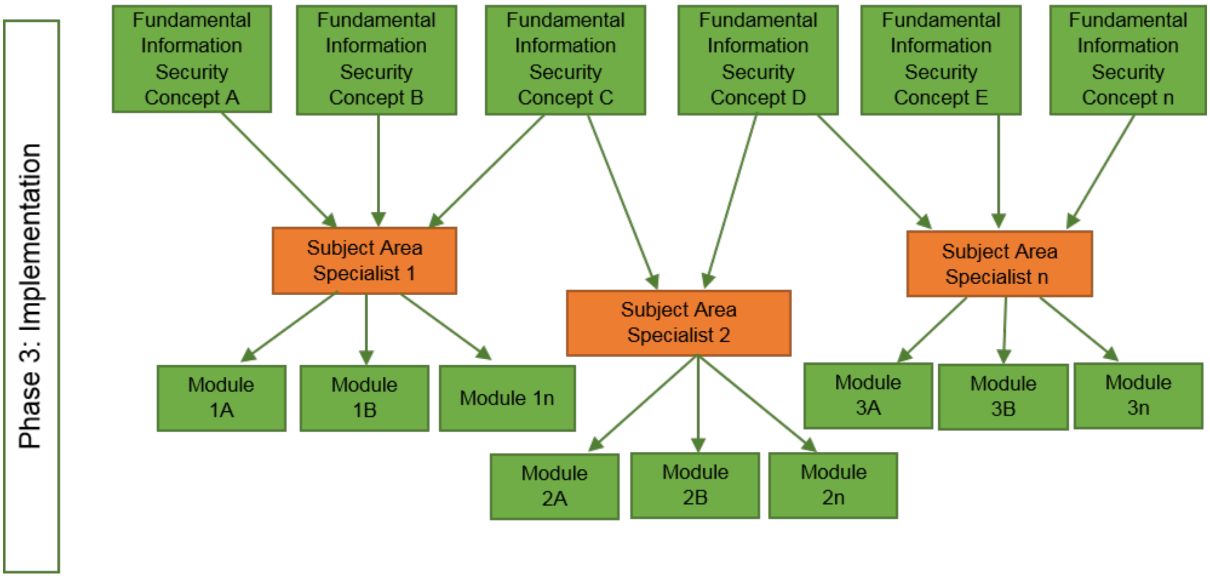
Phase 3: Implementation
Fundamental Information Security Concept A
Fundamental Information Security Concept B
Fundamental Information Security Concept C
Fundamental Information Security Concept D
Fundamental Information Security Concept E
Fundamental Information Security Concept n
Subject Area Specialist 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 5: Phase 3 – Implementation Elements

Due to the scope and depth of information security, it cannot be addressed by a single module. Figure 5, therefore, depicts how information security can be integrated as a pervasive theme which would allow for the scope and depth of information security to be addressed by multiple modules from a different perspective in each module. As mentioned, in addition to IAS being defined as a knowledge area, it 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. For example the Fundamental Information Security Concept C is relevant to Subject Area 1 and Subject Area 2.

Subject Area Specialist

Using the fundamental information security concepts identified in Phase 1, Subject Area Specialists for each subject area, for example, Development Software or Networks 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). As shown in Figure 5, it is necessary for a subject area specialist to 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.

An example of how information security can be pervasively integrated into a department's curriculum is provided. Subject Areas could include, for example, Development Software, Information Systems and Networks. Using Development Software as an example, the Development Software Specialist could integrate Fundamental Information Security Concepts of *authentication*, *secure principles* and *security awareness* into the relevant modules within Development Software. For example, the Fundamental Information Security Concepts of *authentication* and *secure principles* could be pervasively integrated into Development Software 1A module, while the Development Software 1B module could be pervasively integrated into *authentication* and *security awareness*. In Figure 5, Module 1n, 2n and 3n indicate that a subject area can have any number of modules and within those modules- Fundamental Information Security Concepts can be integrated as deemed relevant. Furthermore in Figure 5, for each of the fundamental information security concepts mapped to a specific subject area, 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.

PROPOSED INFORMATION SECURITY EDUCATION FRAMEWORK

Figure 6 illustrates the complete proposed information security education framework. As shown in Figure 6, 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, fundamental information concepts and their related learning outcomes provide a basis for getting the stakeholders' "buy-in" at all department levels, while at the Planning Phase, industry requirements also contribute to getting the stakeholders' "buy-in". The Planning Phase and the Implementation Phase are connected using arrows. Arrows leading to each fundamental information security concept from the Planning Phase are necessary to show that the departmental course curricula's planning determines the relevant fundamental information security concepts.

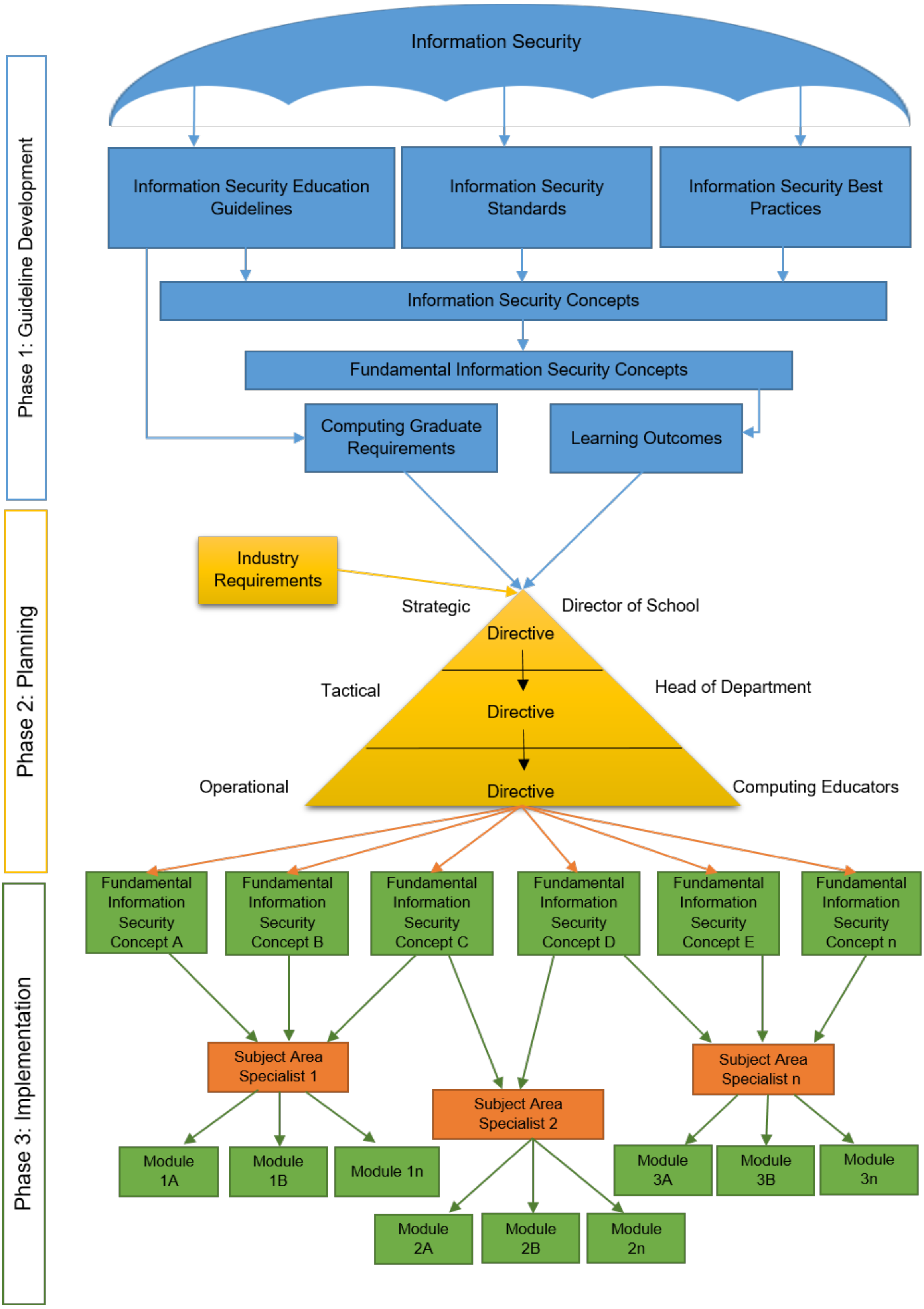
Phase 1: Guideline Development
Phase 2: Planning
Phase 3: Implementation
Information Security
Information Security Education Guidelines
Information Security Standards
Information Security Best Practices
Information Security Concepts
Fundamental Information Security Concepts
Computing Graduate Requirements
Learning Outcomes
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
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 6: Information Security Education Framework

The proposed framework was validated through elite interviews. When asked if the proposed framework would be feasible in their department, all elites indicated that it was feasible both at a departmental level and in terms of the integration of information security into their modules.

Feedback from the elites interviewed included the fact “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”. Another elite stated that, “the proposed framework is feasible as it includes principles that touch on relevant information security concepts” and a further elite 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”.

The Information Security Education Framework is dynamic and it is, therefore, recommended that it should be reviewed periodically 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.

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

CONCLUSION

Typically, when computing students graduate they become employees of organisations. As such, it is vital that these graduates have the necessary information security knowledge to perform their organisational roles and responsibilities in a secure manner. 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. The implementation of this Information Security Education Framework could assist computing departments in the revision of current computing curricula in order to pervasively integrate information security throughout the qualification. This could ensure that a higher education institution's computing department produces graduates who possess the required information security skills, knowledge and understanding to design, develop, implement and maintain secure organisational information systems. This could enable computing graduates to become the "strongest link" in securing organisational information systems and related information assets.

It is envisaged that the study's proposed framework could add value to the South African undergraduate computing department and the body of knowledge within information security education.

REFERENCES

ACM/IEEE – CS. 2008. 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. https://www.acm.org/binaries/content/assets/education/curricula-recommendations/computerscience2008.pdf

ACM/IEEE – CS. 2013. Computer Science Curricula 2013. *Current Practice*, 1–172. https://www.acm.org/binaries/content/assets/education/cs2013_web_final.pdf

ACM/IEEE – IT. 2008. Information Technology 2008 Curriculum Guidelines for Undergraduate Degree Programs in Information Technology. *Current Practice*, 1–139. https://www.acm.org/binaries/content/assets/education/curricula-recommendations/it2008-curriculum.pdf

ACM/IEEE – IT. 2017. Information Technology Curricula 2017. https://www.acm.org/binaries/content/assets/education/curricula-recommendations/it2017.pdf

Amankwa, E., M. Loock and E. Kritzinger. 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), 248–252. https://doi.org/10.1109/ICITST.2014.7038814

Conti, G., J. Hill, S. Lathrop, K. Alford and D. Ragsdale. 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

Dodge, R. C. 2013. Information assurance and security in the ACM/IEEE CS2013. In *IFIP World Conference on Information Security Education*, ed. D. J. Ronald, C. and L. A. Futcher, 48–57. Berlin, Heidelberg: Springer.

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

Futcher, L. and J. van Niekerk. 2011. Towards a Pervasive Information Assurance Security Educational Model for Information Technology Curricula. In *Proceedings of the 8th World Information Security Education Conference*, ed. D. J. Ronald and C. and L. A. Futcher, 164–171. Springer Berlin Heidelberg.

Gomana, L., L. Futcher and K. Thomson. 2015. Integrating information security into the IT undergraduate curriculum: A case study. In *The 44th Annual Southern African Computer Lecturers Association 2015 (SACLA 2015)*, ed. E. Coleman, 19–26. Johannesburg, South Africa.

Gomana, L., L. Futcher and K. Thomson. 2016. An educators' perspective of integrating information security into undergraduate computing curricula. In *Proceedings of the Tenth International Symposium on Human Aspects of Information Security and Assurance (HAISA 2016)*, ed. N.

Clarke and S. Furnell, 179–188. Frankfurt, Germany.

Hinson, G. 2005. The value of information security awareness. Noticebored-creative help for your information security awareness program, (June), 1–20. http://www.noticebored.com/The_value_of_security_awareness.pdf

Institute of Progressive Education and Learning. 2018. Curriculum development cycle. http://institute-of-progressive-education-and-learning.org/k-12-education-part-ii/k-12-curriculum/curriculum-development-cycle/

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

ISO/IEC 7498-2. 1989. *Information processing systems – Open systems interconnection – Basic reference model – Part 2: Security Architecture*. 1st Edition. Switzerland: ISO/IEC.

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

McCumber, J. 2005. *Assessing and managing security risk in IT systems: A structured methodology*. Auerbach Publications.

Perrone, L. F., M. Aburdene and X. Meng. 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.

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

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

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

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

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

Von Solms R. and B. von Solms. 2006. Information security governance: A model based on the Direct-Control cycle. *Computers & Security* 25(6): 408–412.

Von Solms, S. and R. von Solms. 2009. *Information security governance*. 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. and H. J. Mattord. 2004. A draft model curriculum for programs of study in information security and assurance. *Information Systems Security Education* 30114(770). http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1015&context=sais2004

Whitman, M. E. and H. J. Mattord. 2014. *Management of information security.* 4th Edition. Course Technology, Cengage Learning.