Topic Map for representing Network Security Competencies

by

Odwa Yekela

Topic Map for representing Network Security Competencies

by

Odwa Yekela

Dissertation

submitted in fulfilment
of the requirements
for the degree

Master of Information Technology

in the

Faculty of Engineering, the Built Environment and Information Technology

of the

Nelson Mandela Metropolitan University

Supervisor: Prof. Kerry-Lynn Thomson

Co-supervisor: Prof. Johan van Niekerk

December 2017

Declaration

I, Odwa Yekela, hereby declare that:

- The work in this dissertation is my own work.
- All sources used or referred to have been documented and recognised.
- This dissertation has not previously been submitted in full or partial fulfilment of the requirements for an equivalent or higher qualification at any other recognised educational institute.

Odwa Yekela

Abstract

Competencies represent the knowledge, skills and attitudes required for job roles. Organisations need to understand and grow competencies within their workforce in order to be more competitive and to maximise new market opportunities.

Competency Management is the process of introducing, managing and enforcing competencies in organisations. Through this process, occupational competencies can be assessed to see if candidates match the required job role expectations. The assessment of competencies can be conceptualised from two perspectives. The first is 'competency frameworks', which describe competencies from a high-level overview. As such, they are regarded as the "What" element of competency. The second perspective is 'competency-based learning', which focuses on addressing competencies from a more detailed, task-oriented perspective. Competency-based learning is regarded as the "How" element of competency. Currently, there is no available tool that can map the "What" with the "How" element of competency. Such a mapping would provide a more holistic approach to representing competencies.

This dissertation adopts the topic map standard in order to demonstrate a holistic approach to mapping competencies, specifically in network security. This is accomplished through the design and evaluation of a Design Science artefact. In this research process a topic map data model was constructed from mapping the 'What' and 'How' elements together. To demonstrate the applicability of the model, it was implemented in a Computer Security Incident Response Team (CSIRT) recruitment scenario. The aim of this demonstration was to prove that the topic map could be implemented in an organisational context.

Acknowledgements

I would like to express my sincere gratitude to my supervisor Prof. Kerry-Lynn Thomson and co-supervisor Prof. Johan van Niekerk for their continuous support and guidance during my Master's study. Their immense knowledge assisted me throughout the research and writing of this dissertation.

I would also like to thank the South African National Research Network (SANReN) department and the Nelson Mandela Metropolitan University's Post Graduate Research Scholarship (PGRS) for their financial assistance.

To Sandile Nqwenya, Ntombifuthi Dladla and Zandile Manjezi for peer-reviewing and recommending suggestions for improving the documents readability.

To Yasmine Kilian, for the proofreading and the language editing of this dissertation; your input was greatly appreciated.

Finally, I must express my very profound gratitude to my mother, Nopiliso Yekela for providing me with unfailing support and continuous encouragement throughout the process of researching and writing this dissertation.

Abbreviations

CSIRT	Computer Security Incident Response Team
CM	Competency Management
CBL	Competency-based learning
CIPD	Chartered Institute of Personnel and Development
ICT	Information Communication Technology
IT	Information Technology
HRM	Human Resource Management
KSA	Knowledge, Skill and Attitude
SFIA	Skills Framework of the Information Age
e-CF	European Competency Framework
ISACA	Information Systems Audit and Control Association
ENISA	European Union Agency for Network and Information Security
NICE	National Initiative for Cybersecurity Education
ITIL	Information Technology Infrastructure Library
ISO	International Organization for Standardization
IS	Information Systems
EFGs	Exploratory Focus Groups
CFGs	Confirmatory Focus Groups
HR	Human Resource
U.S. OPM	United States Office of Personnel Management
CCENT	Cisco Certified Entry Networking Technician
CCT	Cisco Certified Technician
TAO	Topics, Associations, and Occurrences
IFS	Identity, Facet and Scope

URI	Uniform Resource Identifier
URL	Uniform Resource Locator
CEO	Chief Executive Officer
TMQL	Topic Map Query Language
XML	Extensible Markup Language
GTM	Graphic Topic Map
TMDM	Topic Map Data Model
GIAC	Global Information Assurance Certification
IITPSA	Institute of Information Technology Professionals South Africa
SIMOS	Cisco Secure Mobility Solutions
RDF	Resource Description Framework
CCNP	Cisco Certified Network Professional
CCIE	Cisco Certified Internetwork Expert
CAr	Cisco Architect
CIS	Communications Information Systems
CND	Computer Network Defence
IPS	Intrusion Prevention Systems
VPN	Virtual Private Network
NICE	National Initiative for Cybersecurity Education
SIEM	Security Information and Event Management
IPsec	Internet Protocol security
AES	Advanced Encryption Standard
DES	Data Encryption Standard
MD5	Message Digest 5
IP	Internet Protocol
ISO/ICE	International Organization for Standardization and International Electrotechnical Commission
OSI	Open Systems Interconnection
CIS	Centre for Internet Security
NERC-CIP	North American Electric Reliability Corporation Critical Infrastructure Protection
NIST	National Institute of Standards and Technology
COBIT	Control Objectives for Information and Related Technologies

Contents

List of Tables

List of Figures

Chapter 1

Introduction

> *"the biggest commodity in the world today is knowledge, and the ability to generate, access, and distribute knowledge have become key determinants for a higher developmental trajectory for any nation."* Deputy Vice-President Kgalema Motlanthe (SouthAfrica.info, 2016)

1.1 Background

Today's modern world demands that organisations realise the value that is provided by employees' skills and capabilities. This realisation allows them to remain competitive and also allows them to move into new market opportunities. The introduction of competencies is one of the changes that organisations are making, with the aim of selecting the most competent individuals for job positions. Surveys conducted by the Chartered Institute of Personnel and Development (CIPD) found that there was an increase in the use of competency-based processes in many organisations (CIPD, 2004). In the Information Communication Technology (ICT) industry, organisations have voiced their concern that specialised competencies are required for job positions. This concern stems from the skills shortage faced by the entire ICT sector, which includes a shortage of cybersecurity and network security skills. In South Africa, the increasing shortage of security-related competencies has led to security breaches.

Statistics conducted by Intel Security and Center for Strategic and International Studies (CSIS) revealed that 82 percent of Information Technology (IT) professionals believe that there is a shortage in the cybersecurity workforce (Coertze, 2013). Further studies by Cisco Systems indicate that as many as a million jobs will be left unfilled internationally due to this lack of competencies (Schofield, 2014).

Although there are efforts in the form of competency frameworks, which seek to bridge the gap between supply and demand with regard to ICT skills, most of these competency frameworks offer only a one-sided perspective of competency and are unable to represent competencies holistically. As such, a more holistic approach to representing competencies is needed. Research into the integration of competency frameworks with other competency mediums, such as Competency-Based Learning (CBL) frameworks, may provide a more comprehensive way of modelling competency holistically.

The next section defines and delineates competency and its relation to Competency Management (CM) and network security. This is followed by an explanation of the problem that centres around the holistic representation of competencies.

1.1.1 Defining Competency

The concept of competency is central to both strategy and Human Resource Management (HRM). From a strategic perspective, competencies can be functions, processes and routines performed by people in an organisation and are described as core competencies (L. Cardy & Selvarajan, 2006). Personnel competencies, which are the focus in HRM, are personal characteristics related to effective job performance (L. Cardy & Selvarajan, 2006). The term competency is often associated with the definition provided by Boyatzis in the 'The Competent Manager' (Boyatzis, 2008). Boyatzis differentiates competencies from job functions by pointing out that competencies are the characteristics people bring with them to perform the job. Competency is regarded as an individual's ability to do a job properly.

Competency is often used interchangeably with the term ‘competence’, but they have different meanings. ‘Competence’ broadly describes what a person is required to do and under what conditions, while ‘competency’ is an individual’s ability to draw on the required knowledge, skill and attitude (KSA) to perform activities to a specified standard. It is important to define and measure characteristics associated with effective competency because the expected pattern of behaviour should be explicitly stated (L. Cardy & Selvarajan, 2006). When competencies are defined, employees know what they should do and how they should do it in order to be productive. CM is a process that can be used to evaluate and determine if an individual is competent for a job role.

The increased demand for specialised competencies has led organisations to use CM in the process of assessing people’s competencies for job roles (Rodriguez, Patel, Bright, Gregory, & Gowing, 2002). Certain job roles require a specialised set of competencies. These competencies are sometimes viewed as critical by management, because they cultivate organisational functions, processes and routines (Wahba, 2012). Competency models can help an organisation to embody these competencies for strategic decision making and also to assist in CM (L. Cardy & Selvarajan, 2006). The management of competencies is the act of ensuring that the right competencies are available, in the right quantity and at the right time to facilitate the achievement of organisational goals. Competency models are, therefore, invaluable tools used in the process of CM.

1.1.2 Competency Frameworks

Another aspect of CM is the use of competency frameworks. Competency frameworks share many similarities with competency models, such as describing which characteristics are required to perform a job task effectively. The main difference between the two, however, is that competency frameworks focus on describing and cataloguing competencies, whereas competency models describe competencies within the context of a specific organisation’s job role (Wahba, 2012). Further, competency models are used within the boundaries of an organisation, while competency frameworks are widely used within the industry to provide a common understanding of what a competency entails.

However, competency frameworks do not attempt to address all the competencies that may be held by an individual, nor do they comprehensively describe every competency (European Committee for Standardization, 2014). Instead, competency frameworks can be regarded as high-level overviews of the essential competencies within the ICT industry (SFIA Foundation, 2015). Within the ICT industry, there are two prominent competency frameworks, namely the Skills Framework of the Information Age (SFIA) and the European Competency Framework (e-CF). SFIA is currently the most widely used of the frameworks and is utilised by thousands of organisations for managing their ICT competency resources (SFIA Foundation, 2015). The SFIA Foundation describes their framework as *"[a] common language for skills in the digital world"*. SFIA version 6 characterises competency within the context of a job role as a mix of KSA that is justified by experience or qualification.

Competency frameworks seek to encompass the KSA characteristics for a competency, but this KSA should be based on widely accepted, reputable standards as specified by the industry. These standards are referred to as competency standards and they play a major role in determining the level of expectation for a set of competencies that is used in competency frameworks. Competency standards can be described as an industry-determined specification of performance, which sets out the KSA characteristics required for an individual to operate effectively in a job role (Wahba, 2012). These industry-determined specifications are the result of functional analysis of a sector or particular industry (Schofield, 2014). As such, competency standards provide the tools for transforming the sector and they cover the whole sector area. In network security, competency standards are used to encompass industry "know-hows".

1.1.3 Competency within Network Security

Organisations seek to protect their network systems by employing people who are competent in network security (Cisco Systems, 2010b). Competency standards within network security are validated by professional bodies such as Cisco System and Information Systems Audit and Control Association (ISACA). These professional bodies rely on competency standards to certify individuals as competent with respect to a set of competencies.

Many sources state that certifications are a good way of establishing competency standards within a specific field (Montante & Khan, 2001; Feisel, D. Peterson, & Emeritus, 2002; H. Randall & Zirkle, 2005). Certifications assist organisations in determining whether an individual is equipped with the most relevant industry approved competencies for a job role. Thus, according to Wahba (2012), certification can be thought of as the proof of verified competency, based on evaluated competency standards.

Many occupations within network security have dedicated competency standards that are synchronous with CBL. CBL refers to educational programmes that develop and evaluate the KSA characteristics required to achieve a competency standard (Wahba, 2012). Furthermore, competency is developed from on-the-job training, based on a range of tasks, that tests an individual's capacity to cope with a variety of different situations and ultimately improves an individual's ability to handle new problems. CBL within network security is based on industry certification. Cisco's network security CBL is centred around their hierarchical certification examinations which seek to evaluate competency from entry-level up to a mastery-level (Cisco Systems, 2010b).

The cybersecurity field consists of many subfields, many of which overlap with other ICT fields such as communication networks. Network security is a product of this overlap between cybersecurity and communication networks. Cybersecurity initiatives such as CSIRTs, rely on effective network security competencies for the protection of network system resources. A CSIRT must have personnel who are competent and trustworthy in order to communicate effectively with its constituents (ENISA, 2006). Killcrece et al (2003b) state that,

> *"[h]aving well-defined job descriptions that include a list of the roles and responsibilities for each of the CSIRT positions along with the necessary skills, experience, educational background and/or certifications and clearances required can be a helpful tool in identifying and hiring the right staff."*

To this end, competency frameworks and CBL can help with the formulation of well-defined job descriptions. ENISA (2006) further elaborates that the hiring and training of CSIRT personnel is a challenging process.

Currently, there is a lack of consistency within the cybersecurity industry with regard to the definition and description of cybersecurity work. For example, there is significant variation in occupation descriptions, job titles and positions. This could lead to certain occupations, jobs and positions being perceived as either superior or inferior when, in fact, they entail the same competencies. This has led to a miscorrelation regarding the competencies that are needed within the context of various areas of expertise, network security included (Fallis, 2013). This absence of a common language to describe and understand the cybersecurity and network security workforce has resulted in the development of competency frameworks such as the National Cybersecurity Workforce Framework. This framework was specifically created by the National Initiative for Cybersecurity Education (NICE) to describe cybersecurity-related competencies (National Institute of Science and Technology, 2013). The NICE Framework establishes a common taxonomy that can be used to reference network security related competencies. The NICE Framework follows a 'Describe, Explain and Predict' approach to the classification of competencies. The framework is assembled in four sections namely 'Collect and Analyse Data', 'Recruit and Retain', 'Educate, Train and Develop' and 'Engage'. Each competency identified in the Framework consists of an identification number and a classification statement.

1.2 Problem Area

The main challenge faced by CM with regard to competency, is identifying and developing competencies in a way that leads to the most efficient operations of the organisation. Competency frameworks are usually high-level overviews of the KSA characteristics required for a specific competency, and are commonly used by management to describe and measure the level of expectation for job roles. A possible shortcoming of competency frameworks is that they only cover high-level description of competencies, they do not address the lower-level, task-oriented competencies that may be held by ICT professionals, nor does it describe how competencies can be developed. Although CBL does provide a detailed insight into the deeper context of a competency and how to systematically learn and evaluate that competency, it may fail to cover all aspects of the competency.

Further, many industry certifications focus too much on the knowledge aspect of competency, while paying little attention to skills and attitudes. Another concern is that certifications are often linked to specific vendor products or are technology-specific.

Based on the foregoing discussion, competency can be understood to have two spheres of focus: competency frameworks and CBL.

- **Competency frameworks:** focus on “what” competencies are required in industry, as identified by competency frameworks such as the SFIA and NICE Framework.
- **CBL:** deals with “how” to develop competencies based on well-defined competency standards. CBL is a systemic approach to the effective learning and evaluation of competencies, which is accomplished through the use of certification programmes. CBL focuses more on nurturing an individual’s competency within a specific area.

The integration of these two perspectives of competency has the potential to increase efficiency in how competency is handled in the CM process. Thus, it would be advantageous for organisations to balance both competency frameworks and CBL initiatives to ensure that appropriate competencies exist in the organisation and that employees are given opportunities to further their competency development.

1.2.1 Mapping the “what” and the “how”

Although competency frameworks and CBL can be described as different perspectives to representing competency, their difference presents an opportunity to map competency frameworks and CBL together. Such a mapping has the potential to provide CM with greater utility. The mapping of competency frameworks with CBL is not an entirely new concept. Documentation from SFIA, NICE, SANS and e-CF have suggested the integration of their frameworks with CBL initiatives. For example, frameworks such as SFIA directly address the benefits of using competency frameworks with other CBL platforms, such as certifications or qualifications. Some organisations, such as ISACA and ITIL, have taken advantage of this opportunity to map certifications directly with SFIA competency levels.

Existing documentation indicate that it is possible to integrate competency frameworks and CBL. However, there is currently no scientific method that explains how to map competency frameworks with CBL, or what utility will be gained from the integration. Furthermore, there is no direct mapping of competency frameworks and CBL for competencies within the network security domain.

Another important consideration that needs to be addressed when it comes to mapping is how the competency frameworks should be mapped with the CBL frameworks, as organisations each have their own method of doing this. In addition, the mapping process gives rise to a number of challenges that could affect the mapping. For instance, the mapping must be short and concise so that it can easily be used for the evaluation of competencies, but it must also be extensive enough so that it can be used to refer to task-oriented competencies. Grant (2005) conceptualised a method of mapping information, very similar to competencies, by using a topic map.

Topic maps are an ISO standard for representing knowledge structures and they are used as a way to flexibly model Information System concepts. Furthermore, topic maps can be used to map information together with other information (Ahmed & Moore, 2005). This dissertation will adopt topic maps as a means of mapping competencies holistically. Topic maps will be discussed in detail in Chapter 5.

1.3 Problem Statement

Currently, there is no competency framework or CBL programme that provides a holistic representation of network security competencies.

1.4 Thesis Statement

It is possible to represent network security competencies holistically by using a topic map.

1.5 Research Objectives

Primary Objective Design a topic map that can represent network security competencies holistically.

Secondary Objectives

1. Identify suitable competency frameworks and CBL for the topic map.
2. Determine a suitable methodology for the construction of the topic map.
3. Verify the proposed topic map through a demonstration of its application.

1.6 Research Design

The research methodology that is used in this research is the Design Science paradigm, as described by Hevner and Chatterjee (2012). Design Science seeks to produce an artefact that still adheres to research. In accordance with this description of Design Science, the objective of the research is to design, develop and evaluate a solution in the form of an artefact. The research process is based on the six general steps for developing a Design Science artefact. These six steps, described by Peffers et. al. (2007), are in accordance with Hevner and Chatterjee's view of the Design Science paradigm and are illustrated in Chapter 2, Section 2.4 and Figure 2.5. Other significant research methods used in this dissertation are the following: a Literature Review, Modelling that employs the Topic Map Standard, Proof of Concept and a Focus Group. These research methods are discussed in detail in Chapter 2.

1.7 Delineation

This research focuses only on network security-related competencies identified in competency frameworks and CBL. The network security competencies presented in the topic map will be evaluated through a Focus Group, to prove that it is possible to gain utility from mapping competency frameworks with CBL within the context of CM.

1.8 Layout of Dissertation

This dissertation consists of six chapters. These chapters are briefly described below:

Chapter 1 Introduction: This chapter provides an overview of the dissertation. This overview consists of a brief background to the study and definition of the problem statement. Additionally, it also outlines the research objective and the research design.

Chapter 2 Research Design: This chapter discusses the research design in more detail and also gives a full representation of the research methodology applied to the study.

Chapter 3 Understanding Competency: This chapter discusses literature on competency. It provides a deeper discussion of what competency is defined as, why competency is important and it also distinguishes the two main perspectives on assessing competency.

Chapter 4 Competencies in Network Security: This chapter discusses competencies within the context of network security. As such, it provides a definition of network security and the fields that are related to network security. It also discusses competency standards, competency frameworks and CBL programmes related to network security.

Chapter 5 Topic Map for Network Security: This chapter is the solution part of the dissertation. As such, it describes how the research methodology was used to create and evaluate a topic map for representing network security competencies.

Chapter 6 Conclusion: This chapter summarises the document and the research contribution made through this study. Furthermore, it also discusses the limitations of the research and some future research opportunities for this study

Chapter 2

Research Design

> *"The fundamental principle of Design Science research is that knowledge and understanding of a design problem and its solution are acquired in the building and application of an artefact."*
> (Hevner & Chatterjee, 2012)

2.1 Introduction

This chapter describes the structural approach that was followed in this study to meet the research objectives. As such, the research design provides an outline of the methodological approach that was used to ensure that the research objectives do in fact present a solution to the research problem. The chapter is divided according to the sections which make up the Research Design. The first section introduces the chosen research paradigm which is Design Science, also known as Design Science research. The second and third sections focus on the research methods used within the context of the Design Science paradigm and how the selected research methodology was used in this research.

2.2 Research Design

Research Design In Research, paradigms are defined as universally recognised scientific achievements that for a time provide model problems and solutions to a community of practitioners. They provide a structured set of theories, methods and ways of defining data (Collis and Hussey, 2003, pp 46-47). There are two main research paradigms, which are as Qualitative and Quantitative research. Qualitative research stresses the subjective aspect of human behaviour by focusing on the meaning and implication rather than measurement of a phenomena. While Quantitative research is logical reasoning is applied to the research so that precision and objectivity replace hunches and intuition.

A research paradigm whether it be for qualitative or quantitative research, is generally shaped by the philosophical assumptions of the researcher. The research philosophy can be thought of as a lens through which the researcher can perceive and attempt to understand the phenomenon under study. As such, it is the basic guidelines on how knowledge may be acquired in research, thus guiding data collection and analysis (Hathaway, 1995, Oates, 2006). Due to the nature of the problem and the research objectives, it is clear than design plays a strong role in researching the objective. Design is described by Charles Eames (Hevner, 2012) as A plan for arranging elements in such a way as to best accomplish a particular purpose.

Charles Eames offered the following: A plan for arranging elements in such a way as to best accomplish a particular purpose. Therefore, Design is the instructions, based on knowledge, that turns things into value that people use. This research will apply Design according to the Design Science paradigm.

2.3 Design Science

Design Science in Information Systems is the use of Information Technology to solve human problems through the creation of novel artefacts (Hevner & Chatterjee, 2012). Peffers et al.(2007, p.48) concur by stating that *"Design Science attempts to create things that serve human purpose"*. Furthermore, Design Science is concerned with the creation of an artefact that solve organisational (real-world) problems. Thus, Design Science can be described as the science of obtaining knowledge to solve research problems through the rigorous process of building and evaluating innovative artefacts. One of the most comprehensive ways of depicting Design Science research is the 'Three Cycle View of Design Science research' described by Hevner. The next section discusses the Three Cycle View of Design Science research and it also discusses the applicable guidelines for Design Science research.

2.3.1 Three Cycle View of Design Science

Design Science as a field of research has grown as a result of contributions from multiple authors and has produced multiple views of how to conduct Design Science. Hevner describes a view of Design Science which is referred to as the Three Cycle approach of interpreting and conducting Design Science in IS (Hevner, 2007; Peffers et al., 2007). This view of Design Science in conveyed in his book *'Integrated Series in Information Systems Volume 28'* which is a widely cited Design Science publication. According to the Three Cycle View of Design Science, Design Science can be divided into three corresponding cycles which define the ontology of how Design Science should be conducted in IS (Hevner & Chatterjee, 2012). The three cycles are:

- **The Relevance Cycle** is the link that bridges the environment in which Design Science is applied with Design Science activities.
- **The Rigor Cycle** connects the Design Science activities with the knowledge base (scientific knowledge about the environment in which the artefact is relevant). In order for Design Science to be considered as research it has to be rigorous in how knowledge is obtained and conveyed. This cycle focuses on that element.
- **The central Design Cycle** consists of the core activities, namely the building and evaluation of the design artefacts. This is a repetitive process which ends when a satisfactory artefact is produced.

These three cycles must be present and clearly identifiable in a Design Science research project. Figure 2.1 illustrates the Three Cycle Model from

Hevner's 2004 research paper (Hevner, March, Park, & Ram, 2004). According to Hevner, research draws from relevance and rigour. As such, Design Science draws its relevance (Relevance Cycle) from the opportunities and problems that exist in the organisational environment. The rigour (Rigour Cycle) is drawn from the knowledge base that is required to perform the building and evaluation activities of Design Science. The design aspect (Design Cycle) is the actual building and evaluating which allows an artefact to be refined. This is an iterative process that continues until two contributions are achieved. The first contribution is the ability to implement the artefact in the relevant environment and to evaluate its usefulness in solving the problem. The second contribution is to add knowledge to the knowledge base through the creation of the artefact.

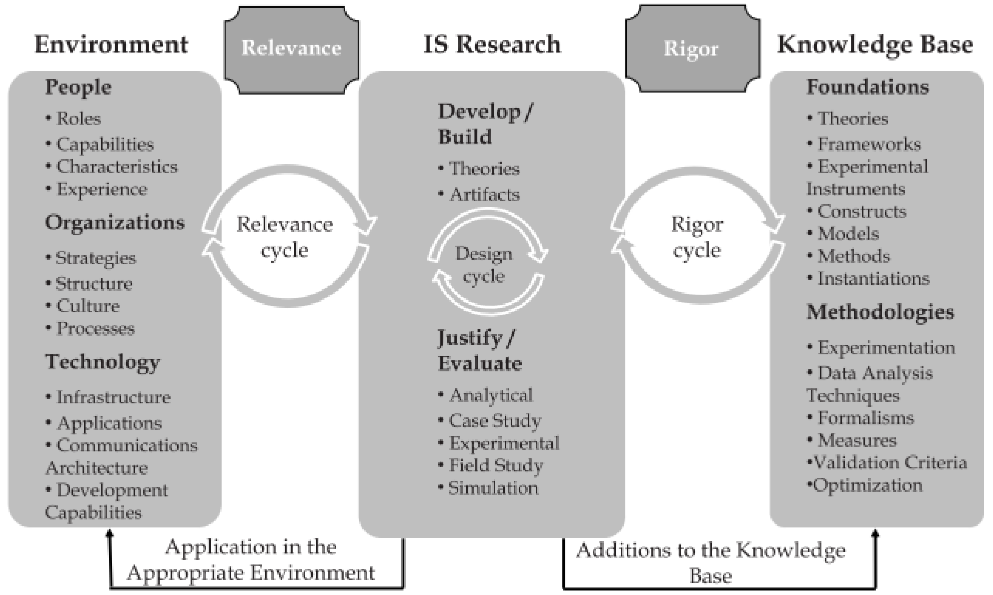


Figure 2.1: Three Cycle View of Design Science (Hevner and Chatterjee, 2012)

From the Three Cycle perspective of Design Science, Hevner and Chatterjee further describe seven guidelines of Design Science research. Peffers et al. (2007, p.49) refer to these as "practice rules" for Design Science. According to Hevner, a research project has to adhere to these guidelines in order to be viewed as Design Science (Hevner & Chatterjee, 2012). These guidelines are presented and described in Table 2.1 below. This research study adheres to these guidelines as shown in Table 2.2 below.

Table 2.1: Design Science research guidelines (Hevner and Chatterjee, 2012)

Guideline	Description
Design as an artefact	Design Science research must produce a feasible artefact in the form of a construct, a model, a method, or an instantiation.
Problem relevance	The objective of Design Science research is to develop technology-based solutions to important and relevant business problems
Design evaluation	It is necessary to demonstrate the utility, quality, and efficacy of a design artefact through rigorous, well-executed evaluation methods.
Research contributions	Effective Design Science research must provide clear and verifiable contributions in the areas of the design artefact, design foundations, and/or design methodologies.
Research rigor	Design Science research relies upon the application of rigorous methods in both the construction and evaluation of the design artefact.
Design as a search process	The search for an effective artefact requires the use of available means to reach desired ends while satisfying laws in the problem environment.
Communication of research	Design Science research must be presented effectively to technology-oriented as well as management-oriented audiences.

2.3.2 Outputs of Design Science

Output in Design Science research is in the form of an artefact. As stated in the previous sections, Design Science is the process of building and evaluating artefacts in order to solve organisational problems. An artefact in Design Science refers to a thing that has, or can be transformed into, a material reality as an artificially created object (Gregor & Hevner, 2013). As such, the way in which an artefact is articulated is of significance. In Section

2.3.1 above, the Design Science Three Cycle Model specified that the Design Science must produce an artefact that is both applicable in the relevant environment and contributes additional knowledge to the knowledge base. However, knowledge contribution can come in different level of abstraction and the type of artefact that should be applied depends on the maturity of the organisational problem being solved.

Types of Artefacts

March and Smith (1995) propose four general deliverables for Design Science, namely constructs, models, methods, and instantiations. Furthermore, Hevner and Chatterjee's (2012, p.12)) first guideline 'Design as an artefact' states that an artefact must come in the form of constructs, models, methods, and instantiations, which are defined below:

- **Constructs** are the conceptual vocabulary of a domain
- **Models** are a set of propositions or statements expressing relationships between constructs
- **Methods** are a set of steps used to perform a task's how-to knowledge
- **Instantiations** are the operationalisation of constructs, models, and methods.

It is also important to understand that the output of Design Science is more than just the material artefact (Gregor & Hevner, 2013). In reality, there are two kinds of outputs in the Design Science paradigm. The first is the actual artefact that is produced and evaluated in the Relevance Cycle, while the second output is the knowledge that is gained and contributed to the knowledge base as a result of designing the artefact (Purao, 2002; Gregor & Hevner, 2013). Hevner et al (2004) state that,

> *"In addition to a knowledge contribution, effective Design Science should make clear contributions to the real-world application environment from which the research problem or opportunity is drawn."*

In the statement above Hevner et al. (2004) emphasis the importance of both the contributions made in the form of artefacts and the knowledge contributions. Knowledge contribution from the different types of artefacts (discussed above) is not equal. In fact, Purao (2002) and Gregor and Hevner (2013) describe different levels of knowledge contribution that an artefact can produce, which they refer to as 'levels of abstraction'. These levels relate to the kinds of contribution an artefact makes, because an artefact can possess characteristics from one or more of these levels. These levels of abstraction are discussed in the next section:

Knowledge contribution: levels of abstraction

The levels of abstraction refer to the depth of 'prescriptive knowledge' (knowledge about how to do something) that is contributed by the artefact. There are three levels of abstraction with which an artefact can be associated. The higher the level of abstraction, the more abstract, mature and complete the knowledge contribution is, while the lower the level, the more specific, limited and less mature the knowledge contribution tends to be (Purao, 2002). Furthermore, the differentiation of the levels of abstraction are not only in terms of a transition from less abstract to more abstract, but also in terms of the knowledge's maturity level (that is, how far the knowledge has advanced in terms of the characteristics of a well-developed body of knowledge).The levels of abstraction are the following:

- **Level 1 Situated Implementation** this level describes the contribution to the knowledge base of new knowledge that nobody has thought of before. This type of knowledge contribution is situational, because the new knowledge is being applied only to specific instances. An example of an artefact on this level is Instantiations.

- **Level 2 Nascent Design Theory** this level is also referred to as 'Knowledge as Operational Principles/Architecture'. Knowledge contribution at this level is abstract, because it can be applied and generalised to a number of situations and a number of different contexts. As a result, knowledge has moved from being situational to being more general in how it can be applied. Examples of artefacts on this level are Contracts, Models and Methods.

- **Level 3 Emergent Theory about Embedded Phenomena** this level describes well-developed design theories about why the design works the way it does.

Essentially, there are different levels of knowledge contribution according to which an artefact can be characterised, as described above. Where an artefact falls in the knowledge contribution sphere depends on the maturity of the organisational problem being solved. Maturity within this context is judged according to two dimensions, namely the maturity of the problem at hand and the maturity of current solutions to the problem. From this interpretation of knowledge contribution, Gregor and Hevner (2013) have proposed a knowledge contribution framework for Design Science that is illustrated in Figure 2.2. In this framework, knowledge contribution is segmented into four broad categories. These categories are then assessed according to the two dimensions of maturity discussed above. The horizontal axis in Figure 2.2 expresses the maturity of the problem. This axis ranges from 'low', where little is known about the problem, to 'high', when a lot is known about the problem. The vertical axis of the diagram expresses the maturity of existing solutions to the problem. In this context, 'low' indicates that there are little or no effective solutions to the problem, while 'high' indicates that there are effective solutions in place for the problem. As such, four quadrants can be drawn from this interpretation. These quadrants are discussed below:

- **Improvement**, this quadrant deals with new solutions for known problems.

- **Invention**, this quadrant deals with new solutions for new problems that have never been addressed before.

- **Exaptation**, this quadrant deals with the adoption of effective solutions from other disciplines to solve new problems.
- **Routine Design**, this quadrant symbolises research that has already been addressed. As such, it is not considered to be a research contribution.

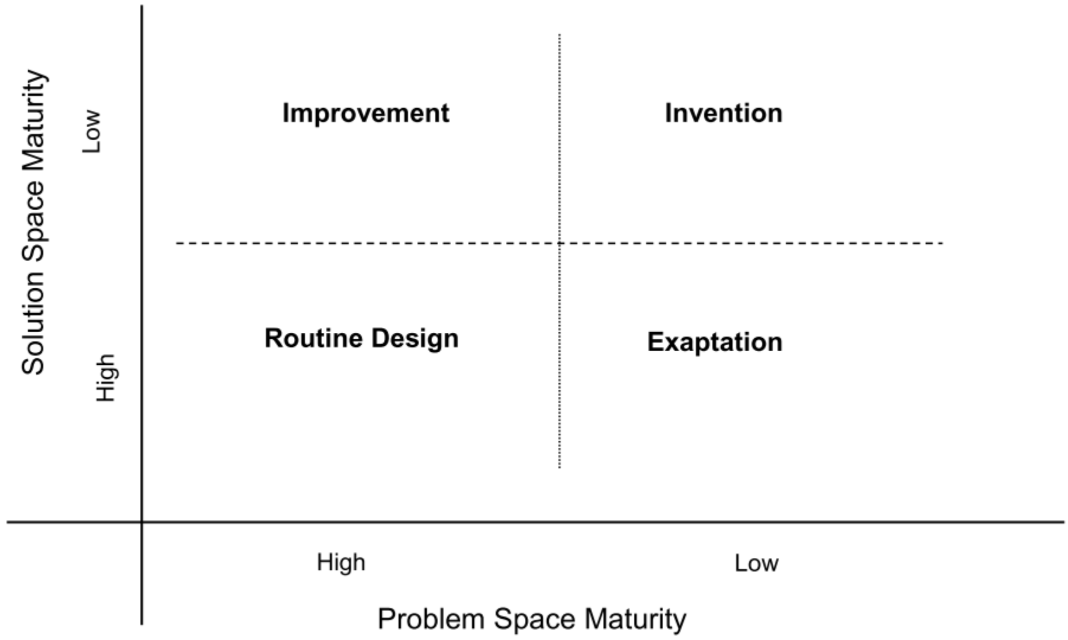


Figure 2.2: Knowledge contribution framework (Hevner and Chatterjee, 2012)

It should also be noted that Design Science follows a specific research process where key steps dictate a researcher's actions (Hevner et al., 2004; Peffers et al., 2007). What differentiates Design Science from other paradigms, are the key steps in the research process. These steps revolve around the design and evaluation of the artefact. The research process is explained in the following section.

2.4 Design Science Process

The need for a consistent process in the act of performing Design Science has long been recognised by researchers in the field.

Although several publications can be found that outline the process of conducting Design Science research, no consensus has been reached. However, Peffers et al. (2007) established a methodology and conceptual model for the Design Science paradigm. The research process for Design Science produced by Peffers et al. (2007) takes into account design approaches from various other relevant research paradigms and fields of study to provide a defined middle ground for IS research and design in general. Furthermore, Peffers et al.'s (2007) view on the Design Science process takes into account the views of other authors and is later recognised by Hevner (2012), who is another key researcher in Design Science. The steps in the Design Science process are presented as follows (Hevner & Chatterjee, 2012):

Problem identification and motivation seeks to define the specific research problem and justify the value of a solution. The problem definition is used to subsequently develop an artefact that can effectively provide a solution. This step requires knowledge of the maturity of the problem, the maturity of existing solutions and the significance of a new solution.

Define the objectives for a solution uses the problem description to infer a set of objectives regarding what is expected from the solution. The objectives can be expressed according to the knowledge contribution framework discussed in Section 2.3.2. As such, the solution may be a new solution to a new problem, a new solution to an existing and well-understood problem or a solution adopted from another discipline and applied in a new context to solve a problem.

Design and Development creates an artefact that serves as the solution. As previously discussed in Section 2.3.2, an artefact can be any designed object in which a research contribution is rooted in the design. During this step the researcher must articulate the artefact's functionality and structural design. This is then followed by the creation of the actual artefact. To move from 'Definition of the objectives for a solution' to 'Design and Development' requires knowledge from the knowledge base (portrayed in Figure 2.1) that can be used to create a solution.

Demonstration involves using the created artefact from the previous step to solve one or more instances of the problem. This may include using the artefact in experimentation, simulation, case study, proof or other appropriate activity. This step can also be traced to the 'Three Cycle View of Design Science' discussed previously in Section 2.3.1. Demonstration requires effective knowledge of how to use the artefact to solve the problem.

Evaluation: is the observation and measurement of the extent to which the artefact supports a solution for the problem. This is accomplished by comparing the objectives of a solution to the actual results obtained from the use of the artefact in the 'Demonstration' step. At the end of this step the researcher can decide to refine the artefact's design (reverting to 'Design and Development' to improve the effectiveness of the artefact) or may choose to continue on to the last step. This would then mark the end of the 'Design Cycle' as set out in the Three Cycle View of Design Science.

Communication: involves the researcher communicating the artefact and the knowledge contribution from designing the artefact (its utility, novelty and the rigour of its design). This must be communicated in a manner that will suit both technical and non-technical audiences.

2.5 Research Methods

This section discusses the various research methods that were used in conjunction with the Design Science process.

Literature Review: A literature review can be described as a thorough examination, summary and report of the relevant available research and non-research literature on the topic under study (Cronin, Ryan, & Coughlan, 2008). The goal of a literature review is to help the researcher establish the status quo with regard to the subject area and to form the foundation for the research. Additionally, it can be used to point out gaps in previous research (Cronin et al., 2008; Oates, 2006).

Modelling: Models are another common method of research. In Section 2.3.2 models were defined as *'set of propositions or statements expressing relationships between constructs'*. Models can be representations of real-world constructs that capture the essential aspects of a system or process . Furthermore, they can serve as a blueprint for a new system or can be used to evaluate existing systems or processes (Olivier, 2013). To design a model involves identifying the major components of the system to be modelled, using a data modelling technique to then identify major events, understanding and formulating interactions and links between components and, finally, using these to then construct the model. A model is usually expressed through some form of modelling language or graphical representation.

Proof of Concept: Proof of concept is a demonstration in principle that a certain concept is feasible and has practical potential. It thus establishes that an idea, invention, process or model is feasible. A Proof of Concept should state clearly what is to be proven, how it will be proven and to what degree it will be proven. It can be differentiated from a prototype in that a Proof of Concept demonstrates that a concept can be accomplished, while a prototype further demonstrates how it will be accomplished. Proof of Concept works well with models, because a model can be created and then demonstrated through a Proof of Concept or prototype. The results of a Proof of Concept need to be measurable so that they can be used to assess if the concept has been thoroughly demonstrated (Olivier, 2013).

Focus Group A Focus Group is a qualitative research technique that is used for data collection (Stewart & Shamdasani, 1990). It is defined as an organised, focused discussion among a small group of people of between six and twelve in number. The group is brought together under the guidance of a moderator, whose role is to promote interaction and keep the discussion focused on the topic of interest (Stewart & Shamdasani, 1990; Hevner & Chatterjee, 2012). As such, Focus Groups provide a setting for a group to reflect constructively on a topic of interest. In Design Science, Focus Groups have been adopted to meet specific goals of design research (Hevner & Chatterjee, 2012). There are two kinds of Focus Groups in Design Science, namely Exploratory Focus Groups (EFGs) and Confirmatory Focus Groups

(CFGs). Both of these Focus Groups focus on the evaluation of the design artefact (Hevner & Chatterjee, 2012).

2.6 Research Methodology

This study attempts to solve an organisational problem. The problem is *"the lack of a competency frameworks or competency-based learning programme that can represent network security competencies holistically"*. The objective is to solve this organisational problem by designing and evaluating a model in the form of a topic map as a solution. The topic map represents an IS tool. As such, the nature of this study lends itself to the Design Science paradigm. This section of the chapter will focus on how Design Science, in conjunction with the previously stated research methods, has been applied to this research study in order to create the appropriate Research Methodology. This Research Methodology is portrayed in Figure 2.3. This image shows how all the previously discussed concepts and processes were integrated and the extent to which they were used in this research.

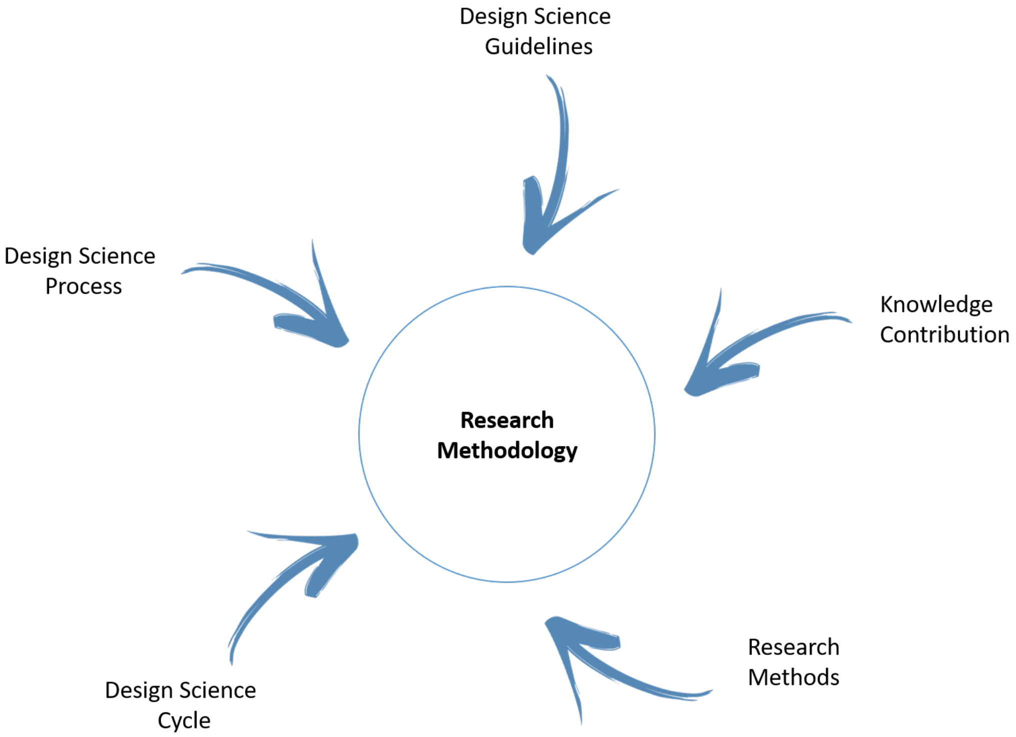


Figure 2.3: Components of the Research Methodology

This next section will describe how the topic map is created and evaluated using the Design Science cycles approach. It will then discuss how the Design Science guidelines were applied in this research. This is followed by an explanation of the expected research artefact and the knowledge contribution it will make. This section will then conclude with a discussion of the research process that was followed.

2.6.1 Three Cycle Model in Research study

Hevner's view of Design Science consists of a repetitive process of designing and evaluating an artefact across three cycles that represent the reality of Design Science research. As such, a range of research methods that correlate with Design Science research have been applied in this research study. This section will discuss how the Three-Cycle approach to Design Science has been applied in the context of this research. As such, it will discuss how the research methods introduced in Section 2.5 have been integrated into the Design Science research. This is best expressed in Figure 2.4.

Literature Review: In accordance with the Design Science *'Rigor Cycle'* discussed in Section 2.3.1, this research will draw rigour from a prescribed Design Science Process that was obtained from literature. Furthermore, literature represents a rigorous way of gathering and assessing relevant knowledge from the *'Knowledge Base'*. A literature review is rigorous by nature, which is why it is ideal to incorporate it into the *'Rigor Cycle'*. This knowledge, drawn from the literature review, is then used in the *'Design Cycle'* as the background information needed to build the topic map.

Modelling: In this research study modelling is conducted through the creation of a topic map. Topic maps are an ISO standard for modelling knowledge structures. The result of the modelling process will produce a topic map data model. The topic map is built and evaluated through the Design Science *'Design Cycle'*. During this process, the topic map's utility is demonstrated through a Proof of Concept, which is then evaluated by a Focus Group.

Proof of Concept: As discussed earlier in Section 2.5, Proof of Concept works well with modelling in the research process. This is because modelling concepts can be demonstrated through proofs of concepts. As such, this research will produce a topic map data model through the modelling process. This topic map will then be demonstrated through a Proof of Concept. In order to adhere to the Design Science *'Relevance Cycle'*, the topic map will be demonstrated specifically in relation to network security competencies for CSIRT job roles.

Focus Group Focus Groups are traditionally widely accepted in Design Science. There are two kinds of Focus Groups in Design Science. This research will evaluate the topic map through a Confirmatory Focus Group (CFG). CFGs are used to establish the utility of the artefact in field use. As such, the topic map is evaluated through a CFG. As part of the evaluation, the performance of the topic map is monitored closely. If changes are required, the topic map will be refined and evaluated again. When the topic map is of a satisfactory standard, it can contribute to both the *'Knowledge Base'* and the relevant environment.

The topic map and the way in which the topic map is designed will serve as the knowledge contribution of the research study that is communicated through this dissertation.

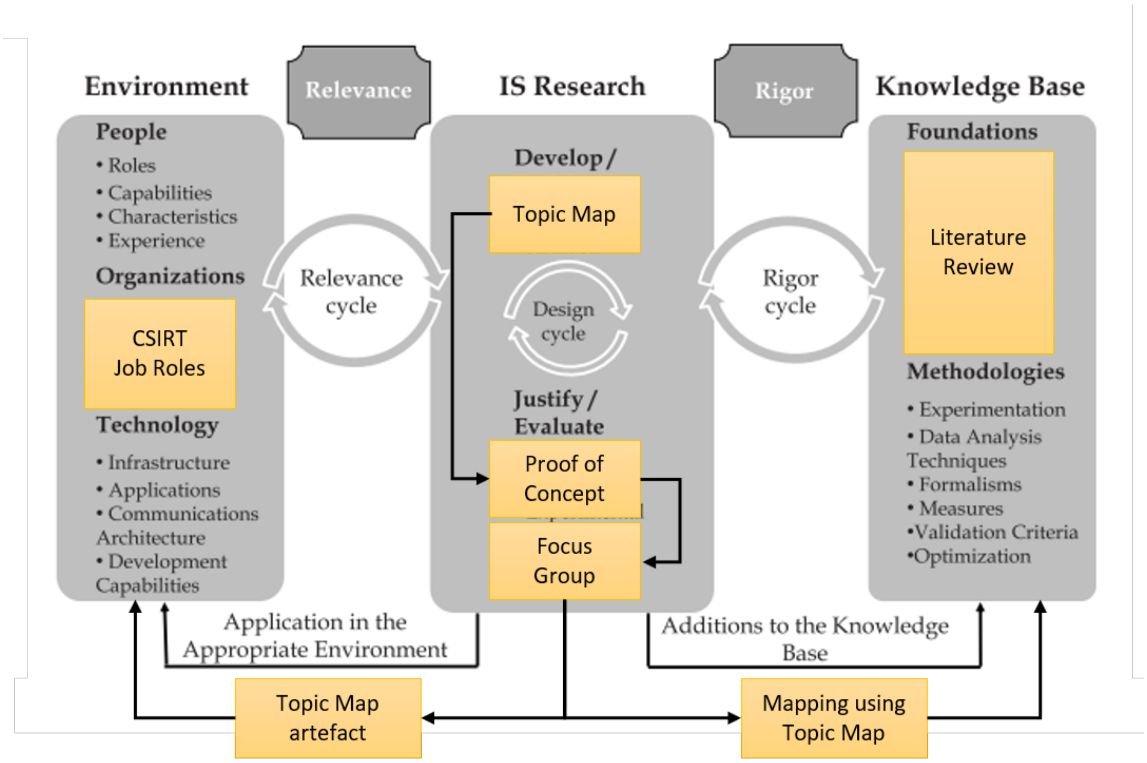


Figure 2.4: Research methods as applied in the Design Science three cycle model

2.6.2 Design Science Guidelines

The seven Design Science guidelines have been consistently referred to as critical to a Design Science research project. Peffers (who is well-known for designing the 'Design Science Process' used in this study) goes as far as stating that these guidelines are the "practice rules" for Design Science research. As such, these rules of practice have been applied in this study in the manner stated in the table below. The left column of the table lists the guideline as expressed in Table 2.1 and the right column describes how each of the guidelines was used in this research study.

Table 2.2: Design Science Guidelines as applied in the research study

Guideline	Research relevance
Design Science research must produce a feasible artefact in the form of a construct, a model, a method, or an instantiation.	The artefact that will be produced by this research is a model in the form of a topic map. Topic maps provide a practical way of mapping IS concepts.
The objective of Design Science research is to develop technology-based solutions to important and relevant business problems.	This research focuses on attempting to solve an organisational problem as discussed in Chapter 1 Section 1.3, by using an IS tool which is the topic map. As such, the research adheres to this guideline.
It is necessary to demonstrate the utility, quality, and efficacy of a design artefact through rigorous well-executed evaluation methods.	The topic map is rigorously evaluated through a well-defined research method in the form of a Focus Group. The context of the Focus Group is discussed in Section 5.10.1.
Effective Design Science research must provide clear and verifiable contributions in the areas of the design artefact, design foundations, and/or design methodologies.	The knowledge contribution of this research study is the topic map and the method in which the topic map is developed. The topic map itself contributes knowledge on how to holistically represent network security competencies, while the method is on how to map high-level frameworks (competency frameworks) with low-level frameworks (CBL).
Design Science research relies upon the application of rigorous methods in both the construction and evaluation of the design artefact.	Research rigour is obtained through following the prescribed Design Science research process introduced in Section 2.4 and applying sound research methods as discussed in Section 2.5.
The search for an effective artefact requires utilizing available means to reach desired ends while satisfying laws in the problem environment.	This research study followed the Research Methodology described in this section of the dissertation. The Research Methodology describes the methods used to construct a solution for the problem described in the problem statement.
Design Science research must be presented effectively both to technology-oriented as well as management-oriented audiences.	The communication is done through this dissertation.

2.6.3 Output of Research Study

A topic map is the artefact of choice, as it matches the relevance of the problem being solved through this research study. In Section 2.3.2 it was established that an artefact should be chosen based on the maturity of the problem and the maturity of existing solutions to the problem. The application of this line of reasoning to the Problem Area, reveals that the problem is well-known, yet there are opportunities for improvement through the development of a better solution. This would result in an artefact in the 'Improvement' quadrant (discussed in Section 2.3.2). Artefacts in the 'Improvement' quadrant must at least be at level 2 or level 3 (level of abstraction discussed in Section 2.3.2) as this would further justify the creation of a model as an ideal artefact for this research study. According to Gregor and Hevner (2012), artefacts in the Improvement quadrant should be judged in terms of:

- Clear grounding, representation and communication of the artefact's design. This is expressed in the presentation of the topic map in Chapter 5.
- Convincing evaluation that provides evidence of improvement over existing solutions. This evaluation is also expressed in Chapter 5, through reporting the result of the Focus Group.

2.6.4 Research Process

In Section 2.4 the Design Science process described by Peffers at al. (2007) was introduced and described as being the most comprehensive process followed in Design Science research to create a substantial artefact. This research study will thus use the Design Science process as described by Peffers et al. (2007). This entails a 6-step approach to Design Science, which is implemented in this dissertation and illustrated in Figure 2.5.

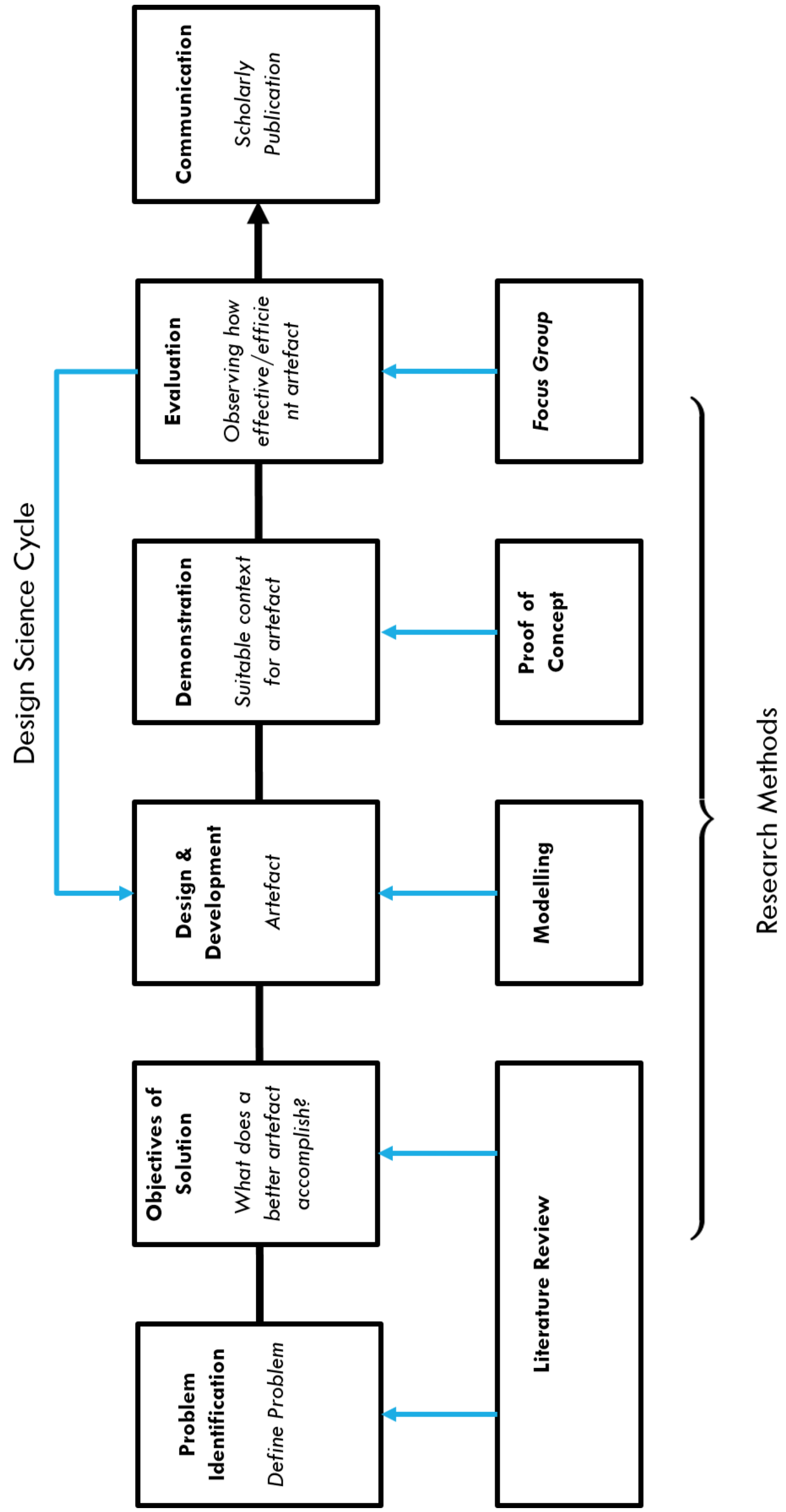


Figure 2.5: Design Science Process as applicable in this research study

Problem identification and motivation: Competency is described as the KSA required to perform a task to a required competency standard. Competency frameworks and CBL programmes are two perspectives to addressing competency. The existence of these two perspectives create the need for an artefact that can represent both perspectives holistically, in order to better manage and develop competencies in network security. Thus, the creation of such an artefact has the potential to improve decision-making for both competency management and CBL, which is a particularly important need in a network security environment. Chapter 1 provides additional information on the research problem and motivates the creation of this artefact. This step in the research process was validated through a literature review that consisted of rigorous research into the application of competency frameworks and CBL programmes, and how they relate to each other. Problem identification and motivation are discussed in greater detail in Chapter 3.

Define the objectives for a solution: In conjunction with the previous step, the objective of this research study is to create an artefact that can represent both perspectives of competency holistically. This artefact should be able to align both perspectives in such a way that it will result in accurate mapping. Furthermore, the artefact should present sufficient utility in both competency management and CBL environments. Finding the most suitable and compatible competency framework and CBL programme is one of the challenges that could be faced. Section 1.5 (research objectives) discusses the research objectives and the sub-objectives that are required to develop the artefact.

Design and Development: As discussed in Section 2.6.3, the artefact that will be designed and developed is a topic map. The road to developing the topic map can be summed up in four phases:

1. Deciding what competency framework and CBL programme to use for the topic map

2. Deciding how to align and map the selected competency framework and CBL programme

3. Developing a data model in the form of a topic map and implementing it through various topic map applications

4. Analysing and examining the relationships within the topic map to interpret useful data that can be leveraged for decision making

These four steps are discussed in greater detail and implemented in Part 2 of Chapter 5. The development of the topic map will require familiarity with topic map tools and best practices, as explained in Chapter 5 Part 1.

Demonstration: Given the objective and context of this research study, as set out in Chapter 1, it is necessary only to demonstrate the feasibility of the solution. This means that the demonstration will serve as a Proof of Concept that a topic map can be used to represent network security competencies holistically and in such a way that useful information can be abstracted from the topic map. Although there are many different applications for this topic map in both competency management and CBL, this study will demonstrate only the applicability of the topic map in a network security environment as the Proof of Concept. The demonstration step is discussed in further detail in Part 3 of Chapter 5.

Evaluation: During this step, the topic map is evaluated by a Focus Group to determine the quality of its utility. The evaluation consists of the researcher determining how the artefact competes against existing solutions in solving the problem. This evaluation is based on criteria set out in Chapter 5. If the topic map meets the necessary utility standard based on a set of criteria, it will be judged as satisfactory. If it is not satisfactory, it will have to be refined again through the 'Design Cycle' described in Section 2.3.1.

Communication: This research study is communicated through this dissertation, thus the knowledge contribution from designing and evaluating the artefact is also disseminated through this dissertation.

2.7 Conclusion

Based on the context of the problem and the information collected, it was decided that Design Science was the appropriate paradigm for following. As such, the paradigm requires that two contributions be achieved. The first contribution is in the form of the artefact and the second contribution is in the form of knowledge on how to design the artefact. This research methodology has identified and discussed how these contributions will be achieved. Furthermore, this chapter covered the research methods that were followed throughout this research in order to achieve the research objective. These included the artefact type, how the artefact will be demonstrated and the evaluation of the artefact according to Design Science principles.

Chapter 3

Understanding Competency

> *"The concept of competency is closely linked to human resources management. It is immediately related to the key strategic goal of HRM winning and developing highly competent people who will achieve their goals quickly and thus will maximally increase their input into achieving the goals of the company."* (Armstrong, 2001, p. 248)

3.1 Introduction

Throughout the years, employee competencies have played a critical part in assisting organisations to achieve their strategic vision. Through the identification and continual development of employee competencies, organisations can gain a competitive advantage. Furthermore, an effective competency strategy can lead to lower error occurrence rates and increased organisational effectiveness. Currently, competencies are commonly used in many facets of HRM to align recruitment and performance management with organisational strategic planning (Selmer & Chiu, 2004).

The concept of competency is central to both strategic management and HRM, but is treated differently by the two. In strategic management, core competencies distinguish an organisation from competitors (Reza & Javadein, 2013). According to Cardy and Selvarajan (2006), an organisation's core competencies are its strategic strength. In HRM, personnel competencies are related to employee behavioural capabilities. Personnel competencies support core competencies (L. Cardy & Selvarajan, 2006).

Lastly, occupational competencies focus on specific skills and knowledge (know-how) thata re required to perform tasks effectively (Konsky & Miller, 2013). This research focuses only on describing and understanding occupational competencies. Figure 3.1 illustrates how occupational competencies relate to core competencies and personnel competencies. Competencies are identified at the top of an organisation. This is represented by the arrow labelled *'A'*. Personnel competencies derive from an organisation's core competencies (arrow *'B'*), but focus especially on promoting and moulding specific behaviours in an organisation's workforce. This is usually accomplished through the development and implementation of tools such as competency models. Competency frameworks and CBL are also aspects of competency, but they are prescribed at an operational level (arrow *'C'*).This is because they are related to specific job competencies or tasks, but they can also describe tasks and job competencies at higher levels in the organisation. This is depicted by the arrow labelled *'D'*.

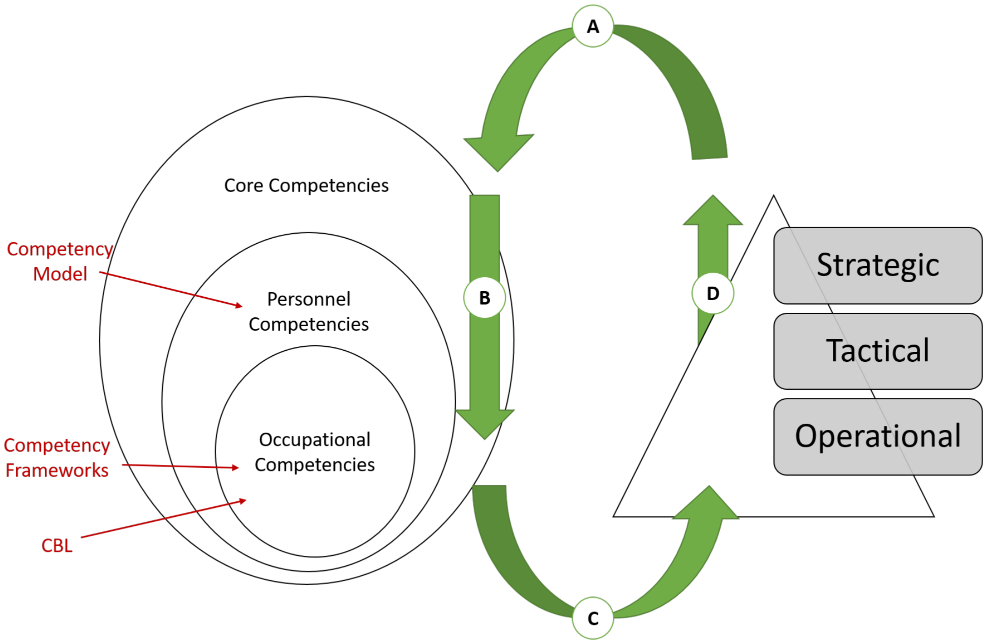


Figure 3.1: Competency types in organisations

This chapter begins by defining what competencies are within the context of this research, discussing why they are important to organisations and describing the two main aspects of competency.

Furthermore the chapter will discuss the main tools used to assess competencies in an organisation, namely competency frameworks and CBL programmes. The final sections of the chapter will then focus on a comparative analysis between competency frameworks and CBL programmes. Figure 3.2 expresses the flow of this chapter.

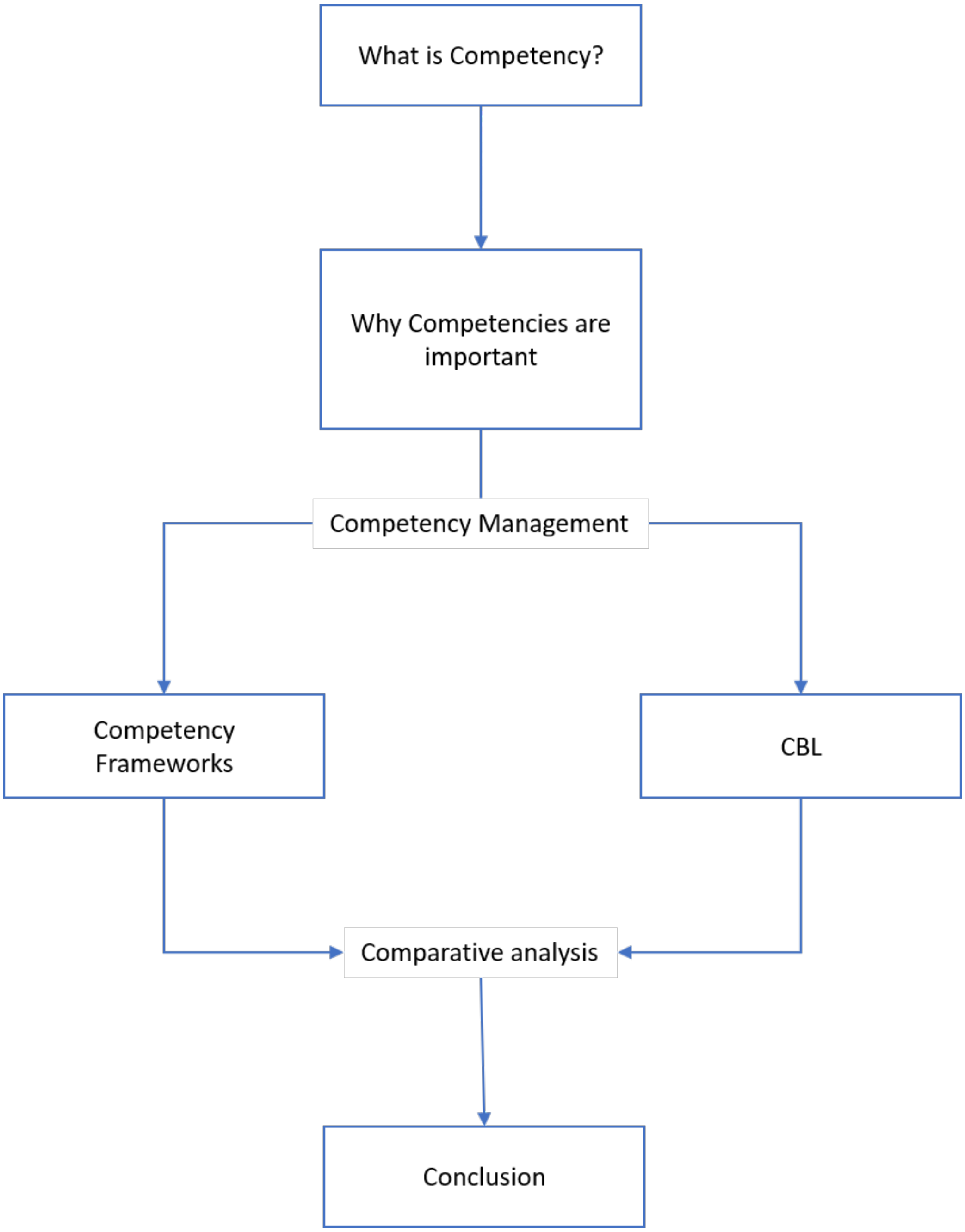


Figure 3.2: Chapter: 3 Layout

3.2 Defining Competency

A common criticism surrounding competency, is that the term *'competency'* suffers from contextual ambiguity (Iles, 2001). This is because it can have different meanings depending on the context in which it is used. Collin (1989) states that competency remains one of the most diffuse terms in organisational and occupational literature. Furthermore, Meyer (1996) cautions that the nature of defining competency normally relates to the context for which it is used. As such, competency within the context of this research relates to occupational competencies. This section examines a series of different descriptions of competencies in relation to occupational work and will then come to a decisive definition of competency for the purposes of this research.

KSA Characteristics: Competency is usually described as characteristics of behaviour related to effective task performance. Many researchers agree that competency is an individual's ability to demonstrate knowledge, skills and attitude or abilities for achieving observable results and this is often referred to as the KSA component of competency (Dubois, 1993; HR-XML, 2004; Jackson & Schuler, 2003; Plessius & Ravesteyn, 2016). Some of the researchers define KSA as Knowledge, Skill and Attitude, while others describe it as Knowledge, Skill and Abilities (Jackson & Schuler, 2003; Plessius & Ravesteyn, 2016). The latest interpretation of KSA, used by most competency frameworks and CBL in ICT, regard competency as the application of Knowledge, Skill and Attitude to a specified standard (SFIA Foundation, 2015; European Committee for Standardization, 2014; National Institute of Science and Technology, 2013).

Competency Standard: The KSA characteristics described above usually relate to some form of output that the competency is associated with. This output is the context in which the competency is applied. Boyatzis (2008) states that competencies are what people bring with them in order to perform jobs. Thus, the output (context) of competency is related to a job-role or tasks for which the KSA is required and this is what is referred to as the competency standard.

According to Dubois (1993, p.9), competency produces job output at an expected level of quality (competency standard). As such, competency relates to job-task performance that can be measured or assessed according to a standard.

Effective Performance: Competency is usually associated with effective performance. Many researchers state that competency results in effective or successful performance. Jackson and Schuler (2003) state that competencies are characteristics that someone needs in order to perform a job effectively. Competencies are seen as that which differentiates ineffective from effective performance. Some researchers go as far as stating that competencies distinguish high performers from average or low performers.

Behavioural Patterns: For competencies to be effective, they must be repeatable. The U.S Office of Personnel Management (2017b) states that competency is a pattern of knowledge, skills, abilities and behaviours that result in successful performance. Woodruffe (l992) states that competencies are behavioural patterns, while Cardy and Selvarajan (2006) elaborate on this view by stating that competencies are observable behavioural patterns that make a positive difference.

Measurable and Observable: Competencies need to be measurable and observable. According to Marrelli (1998) competencies are measurable human capabilities, while the HR-XML website states that competencies are a measurable pattern of KSA (HR-XML, 2004). This measurable view of competency is shared by other sources (U.S. OPM, 2017b).

> Based on these characteristics, the definition of competency used specifically for this research is as follows: *"Competency is the measurable demonstration of knowledge, skill and attitude required to perform job-related tasks to specified standards"*

It is important to note that competencies are not synonymous with job tasks. Instead, they are the characteristics that make an individual more effective in performing job tasks. As such, competencies are supplementary attributes used to aid and enhance job roles (SFIA Foundation, 2015).

3.2.1 Competency and Learning

The previous section has established that competency is drawn from three domains, namely knowledge, skill and attitude. Plessius and Ravesteyn (2016) describe these domains as elements of competency. Spencer and Spencer (1993) describe these domains as follows:

- **Knowledge:** relates to the cognitive knowledge an individual has in a content area.
- **Skill:** relates to an individual's ability to perform physical or mental tasks.
- **Self-Concept (Attitude):** relates to an individual's attitudes, values, or self-image.

It is believed that these domains are related to the Bloom's Taxonomy domains. According to Rudzajs et. al. (2010), competency is based on the Bloom's Taxonomy Model. This is evident in how the description of KSA correlates with the Bloom's Taxonomy domains. Bloom's Taxonomy is a learning taxonomy that is used to assess learning. The model describes three domains of learning, which are the Cognitive, Affective and Psychomotor Domains. The *'Cognitive Domain'* describes different stages of knowledge, the *'Affective Domain'*describes different stages of attitude and, lastly, the *'Psychomotor Domain'*, reflects the different stages of a skill during the learning process (Clark, 2015a). These domains are described in greater detail below:

Cognitive Domain: This domain provides a conventional way of describing the degrees in which knowledge can be expressed. This domain consists of six levels of knowledge representation as expressed in Figure 3.3. *'Remember'* is at the lowest level of the domain because it is believed that remembering represents the lowest form of cognitive knowledge, while *'Create'* is at the top of the domain, because it requires higher order thinking.

Affective Domain: This domain relates to the way in which values, feelings, motivation and attitudes are measured. There are five levels to this domain as expressed in Figure 3.3. These levels also range from the simplest behaviour traits to the most complex.

However, Meyer (1996, p.33) cautions that it is difficult to measure competencies related to attitudes, because they are hard to validate.

Psychomotor Domain: This domain relates to the development of skills, which are measured in terms of precision, speed or techniques in execution. Unlike the previous two domains, the Psychomotor Domain was not fully prescribed by the original authors. As such, there are several representations of the domain from various other authors. The classification used in Figure 3.3 is based on Dave's (1975) Psychomotor Domain Model (Clark, 2015b). This model consists of five levels. The lowest being *' Imitation'* which is described as observing and copying the behaviour of someone else. As such, performance may be of low quality. *'Naturalization'* refers to mastery at a high level that does not require thinking much about the task. This view of skill correlates strongly with the categorisation of skills in the *'Four-Stages of Competency Model'* (Howell & Fleishman, 1982).

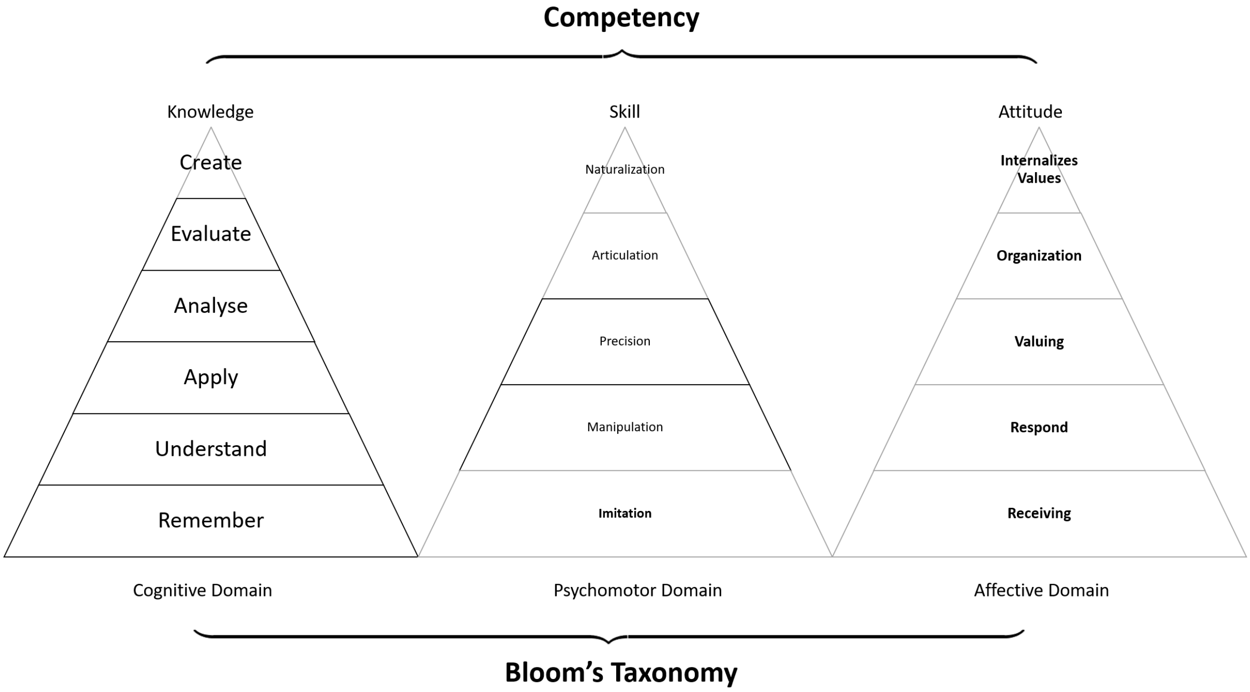


Figure 3.3: Bloom's Taxonomy Domains as described by Clark (2015)

3.3 Importance of Competencies

The use of competencies in an organisation serves to enhance its human resource capabilities, thus yielding a competitive advantage (Lawler, 1994). In various business cases, it was demonstrated that competency yielded benefits such as increased employee productivity, reduced training costs and reduced staff turnover (Homer, 2001).In addition, a sound competency model can help with performance management, succession planning and career development. The ways in which organisations can apply competency are described below.

Selection Process: Competency can help an organisation in the job screening process by providing a more comprehensive description of the job requirements. The application of competency in the screening process increases the likelihood of selecting, interviewing and appointing the best candidates for job-roles. Furthermore, it minimises the risk of investing in people who do not align with the organisation's expectation and ultimately delivers a more systematic and valid interview and selection process.

Training and Development: Competency administration in an organisation can also help to bridge gaps between job competencies by focusing on the training and development of missing competencies or by raising the level of proficiency. This ensures that training and development opportunities align with organisational needs.

Performance Management: This practice ensures the regular assessment of targeted behaviours and performance outcomes linked to a job competency profile. Competency aids this process by providing a shared understanding of what will be monitored, measured and rewarded. Furthermore, competency facilitates effective goal-setting around required development efforts and performance outcomes.

Career Paths: Competency provides the stepping stones necessary for promoting long-term career growth. It clarifies the KSA required for job roles and for future jobs. Furthermore, it assists with identifying necessary levels of proficiency for future jobs.

Competency, therefore, facilitates the identification of clear, valid, legally defensible and achievable benchmarks for employees to progress in the job-roles. Lastly, it helps remove ambiguity in discussions about career progression.

Qualification: Qualification and experience do not guarantee effective job performance. Being qualified does not necessarily mean that the employee is competent, but being competent at executing a task, implies that an individual has the right qualification and also the right competencies. As such, competencies are better indicators of effectiveness. Furthermore, a competent individual knows when to apply technical knowledge and skills.

Finally, the administration of competencies can produce many benefits for an organisation. Competencies provide organisations with the basis for building HR systems that use a structured method of recruitment, selection, performance management, training, and career development. Many organisations and governments, likewise, have used competency tools such as competency frameworks, competency models and CBL programmes to describe and enhance their workforce capabilities (U.S. OPM, 2017b).

3.4 Competency Management (CM)

Competency Management, also known as ‘Skill Management’ or ‘Talent Management’, is the process of managing how competencies are introduced, integrated and maintained in the organisation (Telha, Rodrigues, Páscoa, & Tribolet, 2016; SFIA Foundation, 2015; CPP, 2017). CM ensures that the right competencies are available in the right quantities and at the right time so that organisations can achieve their goals (Draganidis & Mentzas, 2006). Various authors use a cycle approach to describe activities within CM. Although there are variations to the CM cycle, engagement and retention are seen as critical characteristics of the cycle approach (Warren, n.d.).

The goal of the CM cycle is to create a workforce that is engaged and motivated, where employees grow and contribute their knowledge to the organisation. Figure 3.4 is a model that describes the CM cycle. In this model six steps are fleshed out (CPP, 2017);

- **Recruitment** involves recruitment strategies that seek to create and maintain a talent pipeline of skilled employees.
- **Employment Selection** includes assessment methods used to evaluate candidates for job roles.
- **On-Boarding:** involves the provision of a formal on-boarding process for new recruits, which includes the supervision and support needed to successfully transition to job roles.
- **Training and Development** ensures that employees obtain the knowledge and skills required to perform job roles, it also provides opportunities for employees to learn new skills.
- **Performance Management** includes providing feedback and recognition for employee work performance.
- **Succession Planning** involves the provision of mentoring programmes, formal staff development programmes and cross-training opportunities to support strategic planning.

According to Warren (n.d.) the increased rate of technology change has impacted all the steps in the CM cycle. As a result, modern interpretations of the cycle differ from previous career path models.

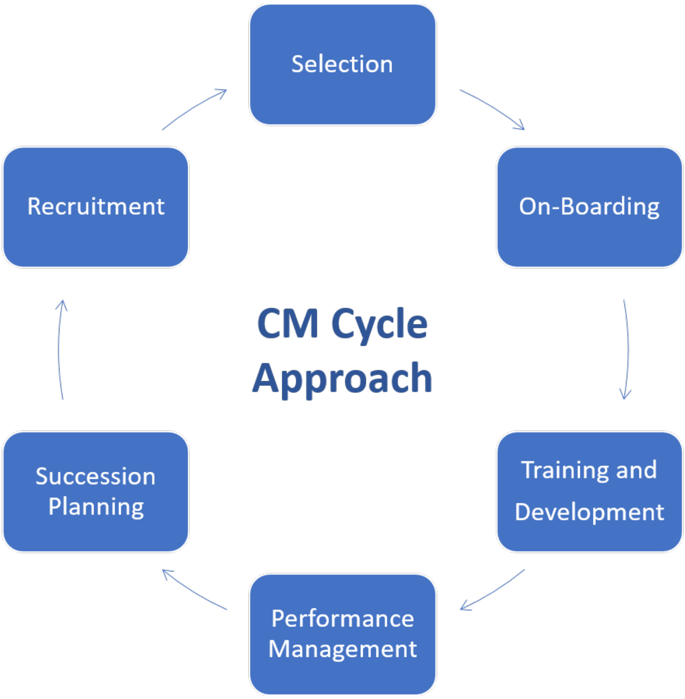


Figure 3.4: CM Cycle adopted from Talent Management Cycle (CPP, 2017)

The increased demand for specialised skills has led organisations to use competency models and competency frameworks in the CM process (Rodriguez et al., 2002). The next section focuses on describing competency models and competency frameworks as components of CM.

3.4.1 Competency Models and Competency Frameworks

Competency models and competency frameworks are both tools that are used within CM, but they are used differently and are meant to achieve different objectives.

Competency Models: A competency model is a descriptive list of the competencies required for employees to be effective in a job role (Draganidis & Mentzas, 2006). Competency models derive from observable and measurable behaviours and embody an organisation's strategic intent (L. Cardy & Selvarajan, 2006). These models enable the identification of competencies that employees need to develop in order to improve job performance or to prepare them for new job roles (Draganidis & Mentzas, 2006).

As such, competency models do align with the CM cycle described in the previous section. Furthermore, competency models are useful in skills gap analysis, which is the process of comparing available competencies with required competencies for occupational job tasks (Draganidis & Mentzas, 2006; L. Cardy & Selvarajan, 2006).

Competency Frameworks: A competency framework is a classification of the competencies required for particular job roles (Markowitsch & Plaimauer, 2009). Competencies included in a competency framework are usually sorted along one or more axes or dimensions (Markowitsch & Plaimauer, 2009). Competency frameworks share many similarities with competency models, such as describing which characteristics are required to perform a job task effectively (SFIA Foundation, 2015).

However, the first difference between competency frameworks and competency models, is that competency frameworks focus on describing and cataloguing competencies for the use of different organisations, whereas competency models focus on describing competencies within the context of a particular organisation (Wahba, 2012).

Secondly, competency models may encompass qualities broader than just the occupational competencies expressed in Figure 3.1. They represent a mix of organisational qualities and occupational competencies (Le Deist & Winterton, 2005). Competency frameworks, on the other hand, are taxonomies and are used to reference industry expectations of competencies in an occupation (Plessius & Ravesteyn, 2016). Both the SFIA Foundation and the National Institution of Cybersecurity consider their respective frameworks to be a language for describing ICT work (SFIA Foundation, 2015; National Institute of Science and Technology, 2013). As such, competency frameworks are aimed at providing a common language that all organisations can reference for occupational description, while competency models are aimed at enabling an organisation to be more competitive.

Thirdly, competency models update on the basis of organisational change that result from new tasks, procedures and positions (Telha et al., 2016). Competency frameworks change according to industry change that emanates from changes in technology, standards or expectations (Plessius & Ravesteyn, 2016). As such, competency frameworks can be regarded as high-level overviews of the essential competencies of ICT skills (SFIA Foundation, 2015). The basic components of a competency framework include the following (Plessius & Ravesteyn, 2016);

- **Category:** A grouping scheme to which similar competencies belong.
- **Competency:** A descriptive name for each competency.
- **Definition:** Statements that explains the basic concept of the competency.
- **Demonstrated Behaviour:** Behaviour indicators that an individual should demonstrate in order to meet the competency requirements

Within the context of this research, there are two prominent competency frameworks, namely the Skills Framework of the Information Age (SFIA) and the NICE framework. The SFIA framework is currently the most widely used ICT competency framework and is also recognised by ICT bodies such as Public-Private Partnerships (IP3) and Institute of IT Professionals South Africa (SFIA Foundation, 2015; IITPSA, 2017). The NICE Framework is the most applicable taxonomy for describing network security competencies. As such, it is discussed further in Chapter 4 Section 4.4.

The next section focuses on discussing the SFIA framework as an effective tool for describing and assessing competencies.

3.4.2 SFIA Framework

SFIA is a skills competency framework that defines a collection of competencies in ICT. It is described by the SFIA Foundation as *"[a] common language for skills in the digital world"*. The framework is utilised by thousands of organisations around the world to define ICT occupational competencies. SFIA version 6 characterises KSA within the context of a job role as a mix of

Knowledge, Behavioural skills and Business skills which is justified by experience or qualification. The framework itself is a multi-dimensional framework consisting of two dimensions known as axes (SFIA Foundation, 2015). These axes represent competency and competence respectively.

Competency The first axis fuses Knowledge, Professional Skills and Behavioural Skills and labels them as *'Competency'*. Each of the competencies within the context of this framework consists of *'Autonomy'*, *'Influence'*, *'Complexity'* and *'Business Skill'* (SFIA Foundation, 2015).

Competence The second axis describes the level of responsibility that should be allocated to specific skill sets at specific levels of depth. This part of the framework describes the *'Competence'* component, which is expressed through seven levels of responsibility (SFIA Foundation, 2015).

Figure 3.5 is an illustration of the two axes. The horizontal axis represents *'Competency'*, while the vertical axis represents *'Competence'*.

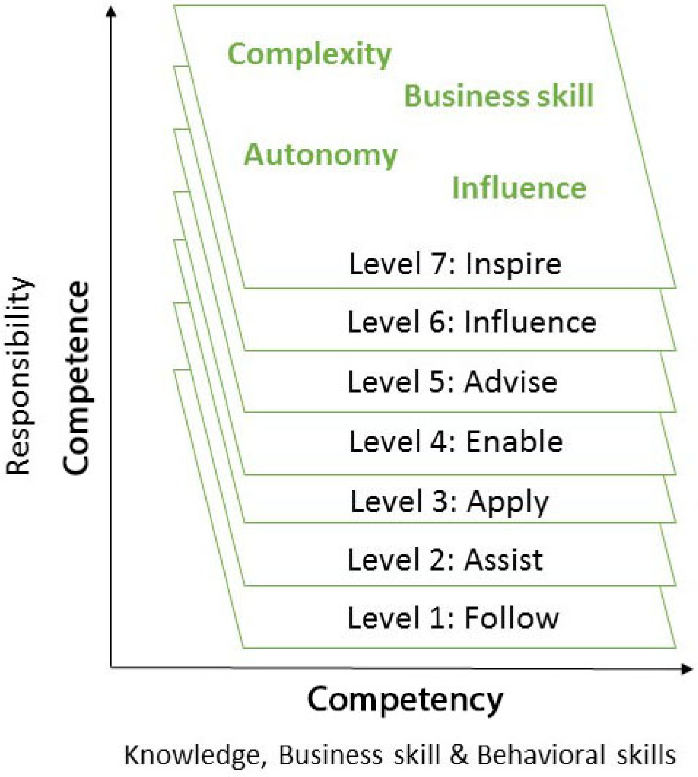


Figure 3.5: SFIA Dimensions adapted from SFIA Foundation (2015)

Competency and Competence Although competency and competence are often used interchangeably, they represent different concepts within the context of SFIA. Competence describes what a person is required to do and under what conditions. In contrast, competency is an individual's ability to draw on the KSA required to perform activities to a specified standard (SFIA Foundation, 2015).

3.4.3 Application of SFIA

The SFIA framework can be used by organisations to improve their ICT capabilities. SFIA provides a comprehensive way of understanding the capabilities of ICT professionals, thus reducing the risk and possible costs of incorrect placements. The framework itself serves as a competency referencing tool that can be used within many of the stages of the CM cycle. The framework can be started at any point of the CM cycle to acquire, deploy, assess, develop and reward employees (SFIA Foundation, 2015), as discussed below.

Acquire: SFIA can be used during the recruitment and acquisition of skills process. Its application may be crucial when new positions open during mergers or during engagements with suppliers and service providers. SFIA helps set criteria for recruitment to ensure that the right candidates are attracted, selected and evaluated through criteria-based assessment.

Deploy: SFIA can also be used to assign the right people for specific project endeavours. The effective deployment of competencies can reduce project and operational risk because of the more effective use of human resources. SFIA can also ensure that outsourced capabilities lead to desired outcomes and value for money.

Assess: SFIA can be used to analyse performance and capabilities. The use of SFIA allows organisations to translate their business objectives into the performance management process. Individuals can map their skills and experience and identify their goals with the aid of the SFIA framework. By referencing SFIA descriptions, employee performance can be analysed to reveal employee strengths and development needs.

Develop: SFIA can also be used to help with the planning and execution of CBL activities. The development of capabilities must align with organisational needs. This can be accomplished through the implementation of SFIA's statements of competence (Competence axis) along with CBL programmes. In this context, SFIA's statements of competence can be used to define development objectives and identify the major skills that need to be developed. This information can then be used to set education and training objectives during development interventions such as CBL.

Reward: SFIA can also be used to help in the recognition and remuneration processes. This is accomplished in the framework by ensuring that remuneration relates coherently to the individual's competence and contribution. The competency levels prescribed by SFIA are a key strength in the job description and professional profiling process. As such, the levels provide clarity about how job descriptions fit into the organisation's hierarchy structure.

Through the continual use of SFIA across the CM life cyle, organisations can achieve greater performance capabilities from their ICT workforce. The applicability of SFIA in CM can actually be linked directly to the CM Cycle phases described in Figure 3.4. This is illustrated in Table 3.1, which illustrates the application of SFIA as it relates to the CM Cycle phases. The first column shows how SFIA is applied in CM, while the second column, shows the phases of CM. In this analogy, *'Acquire'* relates to *'Recruitment'* and *'Succession Planning'*, while *'Deploy'* relates to the *'Employment Selection'* phase, *'Assess'* relates to *'Performance Management'*, and lastly *'Develop'* relates to *'Training and Development'*.

Table 3.1: SFIA application in CM

SFIA in CM	**CM Cycle**
Acquire	Recruitment Succession Planning
Deploy	Employment Selection
Assess	Performance Management
Develop	Training and Development
Reward	

3.4.4 SFIA Sphere of Focus

This last section seeks to describe what aspects of competency SFIA specifically focuses on. Although SFIA can be used across the CM Cycle, it does not holistically represent all aspects of competency. This is because SFIA is a competency framework. Competency frameworks focus on describing competencies and on the application of these high-level descriptions. As such, SFIA does not necessarily address the lower-level, task-oriented competencies that may be held by ICT professionals, nor does it describe how competencies can be developed. Instead, the framework can be regarded as a high-level overview of the core competencies of ICT skills (SFIA Foundation, 2015).

Futhermore, SFIA competency levels are not equivalent to a job role, but rather serve as components of a job role. For example, the SFIA skill *'Incident Management'* does not represent the complete context of an Incident Manager's job role. Instead, it represents the core competencies that an Incident Manager should have. It does not describe task-oriented competencies that may be included in an Incident Manager's job role, such as, *'prioritizing incident reports, defining accountability, roles and responsibility and creating security policies and procedures'*.

SFIA and Job Roles: Through the aggregation of multiple competencies job roles can be derived from the SFIA framework. Furthermore, a single competency in the SFIA framework can be assigned to multiple job roles (SFIA Foundation, 2015). SFIA competencies do not try to replace organisational competencies. Instead, they work alongside core organisational competencies as a supplementary resource (SFIA Foundation, 2015). As such, organisations can use SFIA alongside competency models. Through this combination, organisations will be able to capture industry expectations (SFIA) along with organisational values (competency models).

3.5 Competency-Based Learning (CBL)

CBL relates to the assessment and development of competencies. As an outcome-focused paradigm, CBL focuses on assessing and developing competencies based on standards.

These standards are referred to as 'competency standards' (Szasz, Louridas, Harris, & Grantcharov, 2016).

Competency standards consist of three elements, namely 'Domains', 'Standards' and 'Performance Indicators'. *'Domain'* refers to a specific discipline to which the competency is applicable. *'Standard'* refers to the outline of the KSA in that given domain, while the term *'Performance Indicators'* refers to how the standard is measured and demonstrated (Trinder, 2008). Competency standards test the effectiveness of training, improve recruitment and identify competency gaps, thus leading to improved efficiency, productivity and employee retention (Sienkiewicz, 2014).

3.5.1 CBL sphere of focus

CBL programmes are based on competency standards. A unit of competency in CBL is described by its function and purpose in relation to a task. Tasks are normally very specific. They include the required steps to perform the tasks. As such, CBL descriptions include the knowledge and skills that a person should have to perform the task, as well as the means of assessing whether a person can perform the task (Mcclelland, 2007).

CBL is largely task-oriented and is based on mastery-learning. This means that competencies are drawn from specific tasks. These tasks must be demonstrated with a degree of mastery before the learner systematically moves on to other tasks. At any given time, learners have to acquire a relative number of competencies, which are often part of a larger context. Mastery-learning is an integral part of this process. Mastery-learning is described as a method of instruction, which establishes a level of performance that learners must master before advancing to the next unit (Slavin, 1996). Some of the characteristics of mastery-learning are the following:

- Tasks in mastery-learning are divided into smaller units. Learners must master prerequisite skills before proceeding to new units.
- Feedback is an integral part of mastery-learning. Through formative assessment learners can be given corrective feedback.

Learning Outcome: Output from CBL programmes is usually in the form of learning outcomes. Learning outcomes are very specific statements that describe what is expected from a learner who has performed a task to a specified standard. Learning outcomes are measurable. There may be one or more measurable outcomes that is/are defined for a given competency. *"Good learning outcomes are focused on what the learner will know or be able to do by the end of a defined period of time and indicate how that knowledge or skill will be demonstrated."* (Frankl, 2016).

To sum up this section, CBL is a systematic approach to the development and assessment of competencies, based on competency standards. This competency standard is assessed through experience and/or certifications. Furthermore, CBL is task-oriented. As such, it isusually is technology-specific. This indicates that CBL programmes may focus on developing competencies related to specific technologies. CBL also implements KSA through mastery-learning. As such, many CBL programmes follow a hierarchical approach to the development and assessment of competencies. These pre-requisites are expressed through learning outcomes which measure what is required for progression to the next level.

The Cisco Certification Programme is a communication network certification programme offered by Cisco Systems to develop task-oriented competencies in network-related fields. The programme can be regarded as a CBL, because it focuses on developing and assessing competencies based on certification. It is also task-oriented. Organisations can use Cisco certifications to assess individuals based on best-practices. Furthermore, the Cisco Framework offers several certification levels that are based on mastery-learning.

The next section will discuss the Cisco Certification Programme as it relates to CBL. This is discussed further in Chapter 4 Section 4.6.2, which focuses on how the Cisco Certification Programme specifically addresses network security competencies.

3.5.2 The Cisco Certification Approach

Cisco is recognised as a worldwide leader in communication networks. Cisco's deep understanding of industry and emerging technology has enabled them to establish network standards and best-practices which are recommended and practiced on an international scale (Lammle, 2013). Cisco focuses on CBL through certification. Certifications usually establish a standard of competency and job roles in a specific sector (Al-rawi, Lansari, & Bouslama, 2006). Cisco's certification programme is the most widely used CBL programme in the communication network sector.

Cisco Framework Levels: The certification programme provides a wide range of certifications as part of Cisco's CBL framework. The framework spans several interrelated network disciplines. These include network designing, network routing and switching and network security. Cisco certifications consist of a hierarchy of levels for each of the network disciplines. This is what is referred to by authors as the 'Cisco Framework' or the 'Cisco Certification Path'. Furthermore, each of the levels in the framework correlates with competencies of a career path. These levels are described below in ascending order (Cisco Systems, 2017).

- **Entry:** The (Cisco Certified Entry Networking Technician) CCENT and (Cisco Certified Technician) CCT signify the starting point of competencies administered and assessed through the Cisco framework. These competencies are the basic requirements for someone to be competent in a network position.

- **Associate:** The (Cisco Certified Network Associate) CCNA level certifications are considered to be the foundation of all the network disciplines covered by Cisco. They provide organisations with the assurance that employees understand best practices and standards. The CCNA certifications span several network disciplines, including network security (discussed further in Section 4.6.2).

- **Professional:** The (Cisco Certified Network Professional) CCNP level certification offers more advanced and in-depth expertise in networking.

Organisations can use CCNP to help develop or assess network security positions such as ‘Network Security Engineer’.

- **Expert:** The (Cisco Certified Internetwork Expert) CCIE level certifications signify high technical expertise in a network industry. They test individuals on all facets of a specialised network discipline. CCIE certifications are regarded worldwide as the most prestigious network certifications in the industry because they require in-depth knowledge and understanding of best practises and standards.

- **Architect:** The (Cisco Architect) CAr is the highest level of accreditation achievable through the Cisco framework. This certification recognises the mastery of both technical and business contextual expertise in networking. As such, it is often associated with high positions that require high-level understanding of technology, business and organisational requirements.

The certification levels discussed above are hierarchical by design and, as such, they are related to one another. For instance, before an individual can be recognised as a CCNP security professional, they will have to hold a valid CCNA security certificate. Thus, an individual must possess competencies of the previous level before attempting the next level (Cisco Systems, 2017). This is a great benefit to organisations. They usually capitalise on this by mapping their network security requirements against the Cisco framework levels. This helps employees develop and assess competencies at the right level. The way in which competencies are developed and assessed using Cisco’s framework is different from how competencies are assessed by competency frameworks such as SFIA. For this reason, the next section is a comparative assessment of CBL and competency frameworks. The aim of next section is to identify and map the similarities and differences between the two perspectives of assessing competencies.

3.6 Comparing Competency Frameworks and Competency-Based Learning

Competency frameworks and CBL can both be used to accomplish the same goals, which is to help introduce and mature the right competencies at the right levels in an organisation. However, these goals are accomplished differently by the two. Competency frameworks are aimed at describing "what" competencies are required in an organisation based on competency standards (industry knowledge). CBL, on the other hand, is aimed at describing "how" to develop competencies, based on well-defined competency standards (best practices and industry knowledge). As such, CBL is more centred around nurturing an individual's competency within a specific area. Based on this realisation, competency frameworks and CBL can be regarded as two different approaches to competency. Table 3.2 illustrates some of the differences between competency frameworks and CBL.

Table 3.2: Comparison between Competency Frameworks and Competency-Based Learning

Competency frameworks	**Competency-Based Learning**
What	How
Describe competencies	Develops specific competencies
High-level overview	Specific (Task-oriented)
Independent of technology	Technology-specific
Flat-bed levelling scheme	Hierarchical levelling scheme

Competency frameworks are usually high-level overviews of the KSA required for a specific skill and are commonly used by management to describe and measure the level of expectation for the skill. A possible shortcoming of competency frameworks is that they do not describe task-oriented competencies, nor do they comprehensively describe every competency in a skill. Although CBL does provide a detailed insight into the inner workings of a skill and how to systematically learn and evaluate KSA, they do not describe competencies at a high level like competency frameworks do. Further, many industry certifications focus rigorously on the knowledge aspect of KSA, paying little attention to skills and attitude. Another concern is that certifications are often linked to specific vendor products or are technology-specific.

Another difference between competency frameworks and CBL is the levelling scheme used by the frameworks. Figure 3.6 is a side-by-side comparison between the SFIA and Cisco Framework levels. The SFIA framework has seven levels of competence and describes competencies at different hierarchical levels based on the responsibility and complexity of the competencies and expectations. The Cisco Framework describes five levels of complexity with which competencies can be associated. There is also a difference between the two frameworks in how levelling is signified.

Flat-Bed: The SFIA framework follows a 'Flat-bed' structural approach to levelling. This means that although levels are hierarchical, they are also seen as equal by the framework. For example, Incident Management at SFIA level 6 is not seen as superior to Incident Management at SFIA level 5. Instead, they are seen as two different sets of competencies that require different forms of responsibility. Thus, the organisation must decide when to use SFIA level 5 or Level 6 based on their organisational needs and not just upgrade to higher SFIA levels because they seem more attractive.

Hierarchical: The Cisco Framework follows a 'Hierarchical' structural approach to levelling. This means that one Cisco level is seen as superior or inferior to other levels. For example, competencies developed at 'Professional' level are seen as superior to 'Associate' and 'Entry', but inferior to 'Expert'. As such, it is better to develop and assess competencies at higher levels, but this practice is restricted due to the cost of training and of maintaining highly qualified employees. Thus, organisations should still evaluate their needs before selecting Cisco levels.

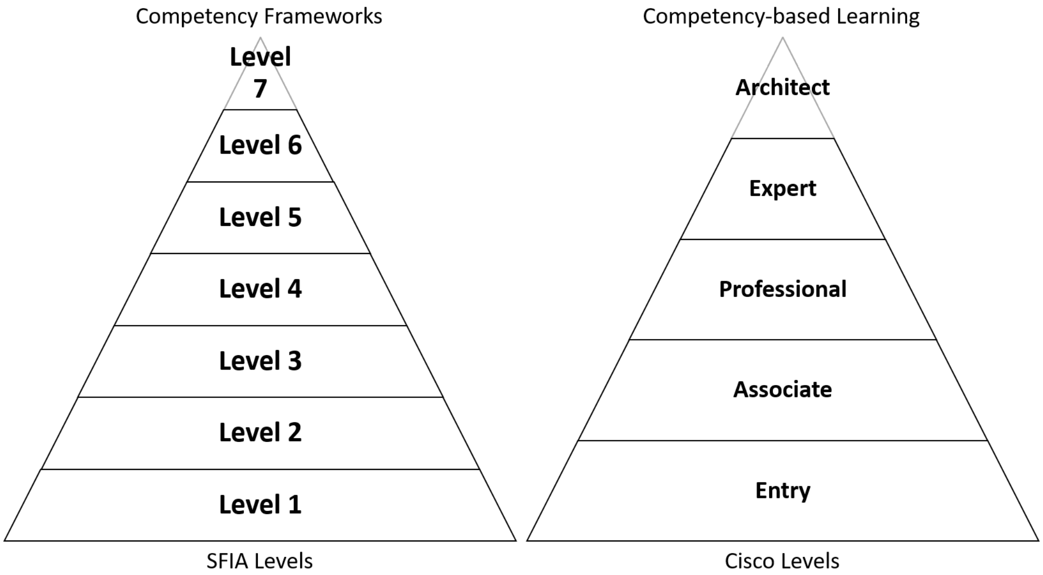


Figure 3.6: SFIA and Cisco side-by-side comparison

3.6.1 Similarities

Although competency frameworks and CBL are approached differently, they do share some similarities.

Bloom's Taxonomy: The first similarity relates to learning taxonomies and how they influence competency. Section 3.2.1 explains how Bloom's Taxonomy represents KSA through its learning domains. Both competency frameworks and CBL can be mapped to Bloom's Taxonomy. In this particular instance, the SFIA and Cisco frameworks are used as analogies. In both SFIA and Cisco the lower levels correlate with lower levels of Bloom's Taxonomy domains, while the higher levels correlate with higher levels of Bloom's Taxonomy. For example, SFIA describes lower levels as being more technical, while the higher levels depict less technical knowledge and require greater understanding of the impact of technology on the organisational mission. This description relates to Bloom's Taxonomy because lower-order thinking activities involves implementing tasks, while higher-order thinking requires higher abstract understanding.

According to the SFIA, *'Business Skills'* at a SFIA level 1,

> *"Uses basic information systems and technology functions, applications, and processes. Demonstrates an organised approach to work. Learns new skills and applies newly acquired knowledge"*

This description maps closely with Bloom's Taxonomy lower-order thinking activities. At SFIA level 7 *'Business Skills'* are described as;

> *"Has a full range of strategic management and leadership skills. Understands, explains and presents complex ideas to audiences at all levels in a persuasive and convincing manner. Has a broad and deep business knowledge..."*

This description maps closely with Bloom's Taxonomy higher-order thinking. In relation to the Cisco Framework, competencies are expressed through certification levels. The lower levels of Cisco certifications focus on basic understanding and implementation of network concepts, while further up the framework the assessment of certification levels is more strict and intensified. At the top, the certification level focus is on strategy setting and business requirements. For example,

- The CCNA certification focuses on the development and assessment of basic understanding and the implementation of network concepts.

- The CCIE certification, which is at a higher level than the CCNA, focuses on in-depth understanding and implementation of network concepts. This involves analysing and evaluating complex technical concepts. In this context, the individual's knowledge and skills are better tested through the certification. According to the Cisco Website, this certification correlates with seven years of experience.

- The CAr certification focuses on evaluating higher understanding of the impact of technology. It involves higher-order activities. In this context individuals are tested on their KSA with regard to translating technology into business requirements.

Criterion Assessment: The second similarity between competency frameworks and CBL relates to the type of assessment used by both perspectives. Both competency frameworks and CBL follow criterion-referenced assessment. In criterion assessment, an individual is seen as either competent or not competent. This is different from norm-referencing, which assesses an individual's performance against other participants. Criterion assessment attempts to provide information about a standard, such as the knowledge and skill which are characteristic of each level of attainment. McClelland supports the use of criterion assessment as a means of assessing competencies (Clark, 2015a). Furthermore, other researchers such as Tate (1995) see criteria as useful for distinguishing levels of performance.

3.7 Conclusion

This chapter covered the literature behind competency and distinguished the use of competency within this research from other uses. Hence, the chapter focused specifically on describing occupational competencies. This included describing what competencies are, discussing why competencies are important and introducing Competency Management (CM) as the processes of introducing, managing and enforcing competencies in organisations. From this analysis it was concluded that there are two aspects of assessing competencies, namely competency frameworks and Competency-Based Learning (CBL) frameworks. Competency frameworks are a classification of competencies that describe competencies from a high level. The other aspect of competency, namely CBL, consists of task-oriented programmes that focus on mastery-learning. Unlike competency frameworks, CBL frameworks describe lower-level, task-oriented competencies specifically. As such, competency frameworks and CBL frameworks are emphasised as important aspects to the development of the solution in Chapter 5.

Chapter 4

Competencies in Network Security

> *"The ability of academia and public and private employers to prepare, educate, recruit, train, develop, and retain a highly-qualified cybersecurity workforce is vital to our nation's security and prosperity."* (National Institute of Science and Technology, 2013)

4.1 Introduction

Information systems and networks have assumed a critical role in facilitating socio-economic development in many countries. According to the European Union Agency for Network and Information Security (ENISA), networks and information systems are necessary for economic and social development (ENISA, 2006). They are fast becoming universal utilities, much like water and electricity. Due to the strong reliance on information, the protection of information as it passes through network systems has become of critical importance to many organisations. The protection of information and information assets requires a specialised set of competencies. This increased demand for security job roles has led to the use of competency frameworks and CBL to assess competencies in network security.

This chapter will focus on assessing how competencies are represented in network security. This will include defining and categorising network security competencies, discussing common standards and competency frameworks used in network security, as well as the CBL programmes used for network security.

4.2 Defining Network Security

Network security is the protection of network systems and network accessible resources through the implementation of controls and policies. According to the U.S. Office of Personnel Management, network security can be defined as:

> *"Knowledge of methods, tools, and procedures, to protect the organisation's system boundaries and to prevent information systems vulnerabilities, and provide or restore security of information systems and network services."* (U.S. OPM, 2017a)

This definition of network security places emphasis on the technical competencies required to protect and restore a network system. Other definitions of network security, such as the ISO/IEC 27033, include some managerial competence, as expressed in the definition below:

> *"Network security applies to the security of devices, security of management activities related to the devices, applications/services, and end-users, in addition to security of the information being transferred across the communication links."* (ISO, 2010)

4.2.1 Network Security Related Disciplines

Since network security has both technical and managerial elements, it requires competencies that overlap with several other disciplines, which include the following (Klimburg, 2012);

- **Networking** is concerned with the design construction and use of network systems. This includes the establishment of policies and procedures related to network systems.

- **ICT Security** is concerned with the protection of computer systems on which information is stored or through which it is transmitted.
- **Information Security:** is concerned with the protection of the information itself and its critical components. This includes the systems that use, store and transmit information.
- **Cybersecurity** is concerned with the monitoring and protection of the cyber landscape and its users. This protection may require the collective use of tools, policies, security safeguards, best practices and other concepts related to cybersecurity.
- **Internet Security** is concerned with protecting information that is transmitted over the internet. This encompasses browser security and the safeguarding of information sent via internet protocols.

Although these disciplines may be defined differently from network security, network security practitioners may possess competencies from these other fields too. Figure 4.1, which has been adopted from ISO/IEC 27032:2012, is an illustration of the overlap between these disciplines. As described in this context, network security *"is concerned with the design, implementation, and operation of networks for achieving the purposes of information security"* (Klimburg, 2012, p. 10). Furthermore, internet security is described as an extension of network security, while cybersecurity overlaps with information security and network security (Klimburg, 2012, p. 11).

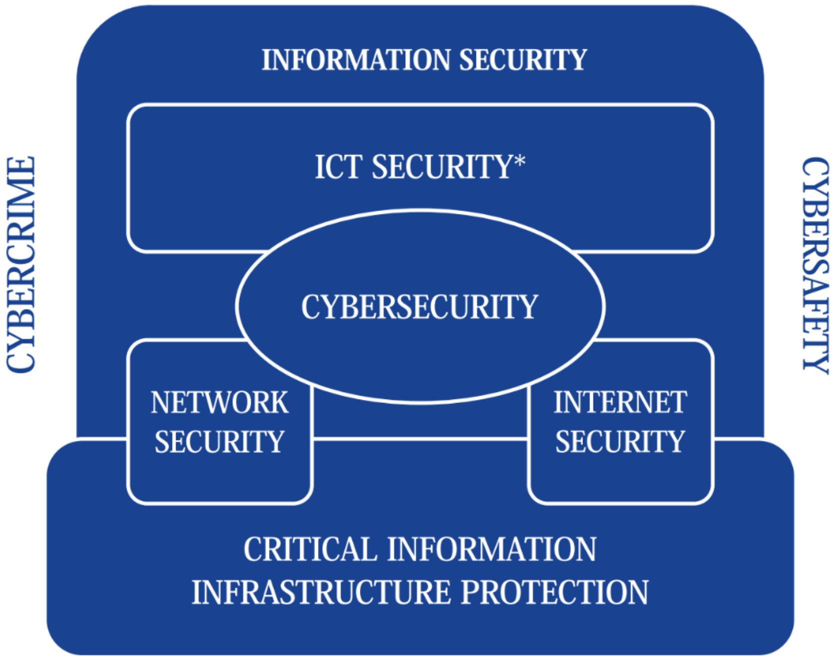


Figure 4.1: network security related disciplines

(Klimburg, 2012, p. 10)

According to Klimburg (2012, p.12), other commonly used terms that relate to network security include.

- **Communications Information Systems (CIS)**, which is the protection of the confidentiality, integrity and availability of communication information systems, as well as the information processed, stored and transmitted in/through them.

- **Computer Network Defence (CNS)**, which is the protection, monitoring, analysis and the response to unauthorised activities in information systems and computer networks.

4.3 Network Security-related Work

In the previous section, network security was described as an inter-disciplinary field. In reality, the network security industry is much more complex.

However, Cisco does provide a sample of common topics addressed specifically through network security (Cisco Systems, 2010b). These topics shed light as to what to expect from network security work. These topics are described as:

Access Control limit the access of users to specific network resources. Thus, they are an important security measure to keep out potential attackers. Access controls can be enforced through security policies, which specify the requirements for the access controls.

Antivirus and Antimalware Software which is malicious software that can infect computer systems through access to the network system. Furthermore, malicious software can reside on a network and lie dormant for days or even weeks. According to Cisco (2017), , *"[t]he best antimalware programs not only scan for malware upon entry, but also continuously track files afterward to find anomalies, remove malware, and fix damage"*. As such, network security practitioners need to ensure that malicious software and risks are handled appropriately.

Application Security ensures the protection of business applications that use the network need to be protected. Any security holes are vulnerabilities that attackers can exploit through network access. Application security encompasses hardware, software and processes used to handle security holes and vulnerabilities.

Behavioural Analytics involves the detection of abnormal network behaviour. Behavioural analytic tools can automatically detect activities that deviate from the norm. Network security practitioners should be able to identify indicators of compromise that pose potential threats and quickly remediate them.

Data Loss Prevention is the prevention of the loss or the damage of sensitive information. Such losses can significantly damage an organisation. Thus, organisations must ensure that employees do not send sensitive information outside the network.

The use of data loss prevention technologies can prevent users from uploading, forwarding or even printing sensitive information in an unsafe manner.

Email security is required because email gateways are the most common vector for security breaches. Attackers use personalised information and social engineering strategies to launch phishing attacks. Email security is the protection of email applications and protocols. This involves blocking incoming attacks and controlling outbound messages to prevent the loss of sensitive data.

Firewalls are used to build barriers between trusted areas and untrusted areas on the network surface. Firewall rules can be used to allow or block specific network traffic. A firewall can be hardware, software or both. Firewalls are among the most common network security controls used by practitioners.

Intrusion Prevention Systems (IPS) are used to scan network traffic in order to actively block attacks. They can accomplish this by correlating huge amounts of global threat intelligence to both block malicious activities and track the advancement of suspected files. IPS are able to prevent the spread of outbreaks and reinfection in the network.

Mobile Device Security is necessary because mobile devices are increasingly vulnerable to cyber-attacks. According to Cisco (2016), the next three years could see 90% of IT organisations supporting corporate applications on personal mobile devices. Mobile device security is the regulation of mobile devices on the network.

Network Segmentation is software-defined segmentation, which classifies network traffic, and which makes the enforcement of security policies much easier. These classifications can be based on user information. Access rights can be assigned based on role, location and other parameters.

Security Information and Event Management (SIEM) is a holistic approach to viewing and securing an organisation's network. SIEM can aggregate network information and allow it to be managed and viewed from specific locations. This allows security staff to respond to threats more effectively.

Virtual Private Networks (VPNs) encrypt the communication between endpoints and the network, often over the internet. The design and implementation of VPN networks is important for the protection of organisational information during communication.

Web Security can control user web usage, block web-based threats and deny access to malicious websites. Web security can protect web gateways on websites or in a cloud environment.

Wireless security is the use of controls and policies to prevent unauthorised access or damage to an organisation's wireless network. Typically, wireless networks are less secure then wired networks. As such, wireless networks need to be effectively monitored and controlled to prevent exploits.

Although the topics listed above are typical in network security, studies have shown that even ICT professions that do not have the word "security" in their job titles, also spend a considerable amount of time performing security-related activities daily (Adnan et al., 2015). The absence of a common language that can be used to define cybersecurity and network security competencies at high levels, has resulted in the development of cybersecurity competency frameworks.

4.4 Network Security-related Competency Frameworks

One of the most descriptive cybersecurity competency frameworks is the National Cybersecurity Workforce Framework established by the National Initiative for Cybersecurity Education (NICE).

The NICE Framework was specifically created for describing cybersecurity-related competencies (National Institute of Science and Technology, 2013). Furthermore, the NICE Framework is spearheaded by the National Institute of Standards and Technology (NIST). The Framework itself establishes a common taxonomy that can be used to reference competencies. This includes several competencies that relate to network security. These competencies are listed below (National Institute of Science and Technology, 2013).

- **Network Security:** Consists of skills in implementing, maintaining and improving network security practices.
- **Computer Network Defence:** Knowledge of computer network defence (CND) and vulnerability assessment tools, including open source tools, and their capabilities.
- **Infrastructure Design:** Knowledge of network protocols and networking fundamentals.
- **Operating Systems:** Knowledge of the protection of client and server operating systems (e.g. Windows and Linux).
- **Technology Awareness:** Knowledge and research into new and emerging IT and information security technologies.
- **Security:** Knowledge and implementation of data security standards.
- **Configuration Management:** Knowledge and skill in the configuration and utilisation of protection components (e.g. firewalls, routers and servers).
- **Identity Management:** Consists of skills in developing and applying security access controls, as well as knowledge of authentication methods and network access management.
- **Incident Management:** Consists of the knowledge and application of incident response and handling methodologies.
- **Infrastructure Design:** Knowledge of network protocols and networking fundamentals.

- **Cryptography:** Knowledge of cryptology and encryption algorithms (e.g. IPsec, AES, DES, and MD5).
- **Telecommunications:** Knowledge and implementation of telecommunications concepts.
- **Hardware:** Knowledge of hardware devices (e.g. computer systems, access control devices and network components).
- **Encryption:** : Consists of knowledge and skills in using VPN devices and encryption.
- **Project Management :** Knowledge and application of resource management principles and techniques, which include information security programme management.

Because network security is a discipline that overlaps with cybersecurity (Klimburg, 2012), the NICE Framework is useful in determining and understanding network security competencies. Furthermore, industry standards are also seen as useful in understanding and determining network security work. The next section will discuss standards that relate the to definition of network security processes, procedures, tools and functions.

4.5 Network Security-related Standard

In Section 3.2 competencies were described as the KSA required to perform a task to a specified standard. As such, standards play a critical role in laying the foundation on which network security competencies are established. Within the context of this research, standards are defined as well-documented practices that are generally accepted and followed by members of an industry. In network security, standards (Stallings, 2006):

- Define the scope of security function,
- Provide a basis for designing policies that securely manage information and network resources,
- Serve as criteria for evaluating the effectiveness of security measures,
- Define techniques for assessing security and monitoring security breaches,

- Provide procedures for dealing with security failures.

By addressing network security matters, standards are able to increase the effectiveness and productivity of security practices, thus enhancing the professionalism of the network security industry (ASIS, 2017).There are several standards related to network security. Among these, the International Organization for Standardization (ISO) provides the best-rounded set of standards for interpreting network security work. The following section will discuss several of the standards related to network security, starting with the ISO/IEC 27033, which is the official standard for network security (ISO, 2010).

4.5.1 ISO/IEC 27033

The purpose of the ISO/IEC 27033 is to be used as a security guide for various network security aspects, such as the secure management of network systems and the operational use of network systems. It was designed specifically to be used by network security practitioners (ISO, 2010). The standard consists of a five-part series that is being actively expanded to seven documents.

ISO 27033-1: The first documentation of the series provides an overview of the standard. It also defines and describes various concepts related to network security and the management of network security. The aim of this part of the standard is to give an overview of network security and then to provide guidelines on how to achieve good quality network security architecture. It also describes risks, designs and controls associated with network systems (ISO, 2010).

ISO 27033-2: The second part of the standard covers the design and implementation of network systems. It defines how organisations can achieve quality network security architecture and implementation by using a consistent approach to the planning, design and implementation of network security best practices. This part of the standard is useful for defining network security requirements (ISO, 2010).

ISO 27033-3: The third documentation in the series discusses risks, design techniques and control issues commonly associated with network scenarios. The objective of this issue is to highlight threats, design techniques and controls for various types of networks. This part of the standard is geared towards personnel involved in the planning, design and implementation of network systems related to network security (ISO, 2010).

ISO 27033-4: The fourth documentation of the series focuses on securing communication between network systems that use security gateways. Thus, it defines the specific risks, design techniques and control issues associated with securing information flow between devices that use security gateways. These security gateways include different types of firewalls and other gateway devices such as routers and IPSs. This part of the standard is geared towards individuals involved in the planning, design and implementation of security gateways (ISO, 2010).

ISO 27033-5: The fifth documentation of the series provides technical guidance with regard to risks, design techniques and control issues associated with VPNs. As such, it defines specific risks, design techniques and control issues for network connections that have been established over VPN technology. This part of the standard is for individuals who plan, design and implement VPN networks (ISO, 2010).

ISO 27033-6: The next proposed realisation of the series will provide technical guidance on IP convergence. Thus, it will define specific risks, design techniques and control issues associated with securing IP convergence networks. This part of the standard will be for individuals involved in the planning, design and implementation of secure IP converged networks (ISO, 2010).

ISO 27033-7: The last proposed realisation of the series will provide technical guidance on securing wireless technologies. It will define specific risks, design techniques and control issues for securing wireless and radio networks. This part of the standard will be for individuals who plan, design and implement security for wireless and radio networks (ISO, 2010).

4.5.2 Other ISO Standards

Although the ISO/IEC 27033 standard provides good technical guidance on aspects related to network security, it is actually an extension of the ISO/IEC 27002 standard. The ISO 27002 standard discusses controls related to network security at a basic standardised level. Other standards that are seen as indispensable to the application of the ISO 27033 standard, include the ISO/IEC 7498 on Open Systems Interconnection (OSI) Basic Reference Model, ISO/IEC 27000 and 27001 for information security management systems and, lastly, the ISO/IEC 27005 for information security risk management (ISO, 2010, p. 12).

4.5.3 Centre for Internet Security (CIS)

CIS provides a set of best practice controls and benchmarks for securing IT systems against internet attacks. CIS controls and benchmarks are seen as a de facto standard for internet security. The controls specify actions for defence against dangerous cyber-attacks (CIS, 2017). According to SANS Institution of Technology, a major benefit of the controls is that they prioritise and focus on a smaller number of actions with high pay-off results. The CIS provides over 100 configuration guidelines for various network-based technologies (SANS, 2015).

4.5.4 NERC-Critical Infrastructure Protection (CIP)

NERC-CIP is a set of network security requirements designed to secure electric grid systems against cyber-attacks (NERC, 2016). NERC-CIP consists of nine standards and forty-five requirements. Version 5 of the standards requires the use of firewalls, IPS and deep pocket inspection and the implementation of cyberattack monitoring tools (Cisco Systems, 2010a). Although NERC-CIP is a North American standard, it has also been adopted in other countries such as Canada and Mexico (Beyond Security, 2016).

4.5.5 National Institute of Standards and Technology (NIST)

The NIST provides a variety of standard families related to network security, among which is the NIST SP 800 family for cybersecurity. The NIST SP 800 family consists of the SP 800-41 standard, which provides a practical guide to understanding the capabilities of firewall technologies and firewall policies. The SP 800-46 standard provides recommendations for securing remote access to both clients and servers. The standard is a guide for creating telework-related policies and for security controls related to remote access (NIST, 2017).

4.5.6 Other Standards

Other standards and best practices that may not traditionally be used specifically for network security or cybersecurity practices do also have elements of network security. These include COBIT and ITIL, which both have high-level processes that relate to information security and network security (ISACA, 2017), while the Standard of Good Practice provides controls and guidance on information security and related topics.

4.6 Network Security CBL Programmes

Although standards are good at describing network security work, they do not assess the application of these best practices. This is because standards are not centred on competencies. CBL programmes are centred on competencies because they assess competencies in relation to standards and best practices.

The increased demand for network security, demands practical hands-on skills (Cisco Systems, 2015; SANS, 2015). CBL programmes understand how to access good network security practices. Unlike competency frameworks, CBL focuses particularly on assessing how competencies are learned. Therefore, CBL programmes prove to be another way in which network security competencies can be assessed. In network security two CBL programmes are significant to network security work. These CBL programmes are discussed below.

4.6.1 SANS GIAC Programme

SANS provides a series of CBL programmes for developing and evaluating cybersecurity competencies. This includes information security controls and network security practices. The GIAC Certification Programme consists of more than thirty cybersecurity certifications along with SANS CBL training. GIAC certification examinations are developed through a rigorous process and are reviewed by industry experts in each technical area (SANS, 2015). The certifications are categorised according to five domains. SANS does not specify any particular order for taking the certifications. However, it does recommend taking the lower order certifications before the higher-order ones. This is expressed in the SANS GIAC certification roadmap poster, which is attached in the appendix C.

4.6.2 Cisco Network Security program

While the SANS GIAC Certification Programme focuses on competencies around cybersecurity, Cisco's CBL programme focuses specifically on competency development within the realm of networking. As such, the Cisco network security path is tightly niched around securing network systems. Cisco describes network security as *"any activity designed to protect the usability and integrity of your network and data"*(Cisco Systems, 2010b). The Cisco certified network security programme provides four certification levels for assessing network security competencies. It also includes an additional fifth level for evaluating network architecture designs at a high level, which includes the understanding of security requirements. Cisco certifications are specific, competency-based and aligned closely with best practices and industry standards. The certification levels are described below (Cisco Systems, 2017).

Entry (CCENT): The entry level certification from Cisco is the CCENT, which is described as the starting point for many networking careers. This certification assesses the individual's knowledge and skill to install, operate and troubleshoot a small enterprise branch network. It also assesses knowledge of basic network security (Cisco Systems, 2015).

Associate (CCNA) in Security: The next certification in the Cisco hierarchy is the CCNA Security, which lays the foundation for job roles such as Network Security Specialist, Security Administrator and Network Security Support Engineer. The CCNA Security programme is intended to provide baseline security knowledge and skills in network security (Cisco Systems, 2015).

Professional (CCNP) in Security: The CCNP Security certification provides proof of competency at a professional network security level. The certification assesses knowledge and skills in choosing, deploying, supporting and troubleshooting Firewalls, VPNs, and IPs controls (Cisco Systems, 2015).

Expert (CCIE) in Security: The CCIE Security certification programme recognises network security practitioners who demonstrate network security competency at an expert level. The certification assesses the individual's knowledge and skills in implementing, maintaining and supporting extensive Cisco network security solutions by using the latest industry best practices and technologies (Cisco Systems, 2015).

Architect (CAr): The CAr is the highest level of competency that can be accessed through Cisco certifications. The CAr is aimed at individuals in senior positions who are responsible for producing technical specifications for the network to support business objectives. The curriculum focuses on understanding the business strategy and translating it into technical infrastructure requirements (Cisco Systems, 2017).

4.7 Conclusion

It was discussed in this chapter that both competency frameworks and CBL programmes are tools that can be used to assess competencies in network security. NICE clearly states that there is a need for defining competencies at a high level, hence the development of the NICE competency framework. Both Cisco and SANS state that there is an increasing demand for skill-specific competencies in network security, hence the introduction of CBL programmes. Although both competency frameworks and CBL programmes are based on best practices and standards, they are often used separately. Thus, the next chapter focuses on bridging this gap by mapping these entities together.

Chapter 5

Topic Map for Network Security

> *"It is our firm conviction that they (Topic Maps) will become as indispensable for tomorrow's information providers as maps for the traveller. And once topic maps have become ubiquitous, they (Topic Maps) will indeed constitute the GPS of the information universe."* - Steve Pepper (Chief Strategy Officer at Ontopia), 2013

5.1 Introduction

This chapter is an implementation of the Design and Development phase as described in the Design Science process. As such, this chapter will focus on the creation of the proposed research solution. Chapter 3 accomplished two things. Firstly, it introduced the notion of competency, which is perceived from two points of view, namely a competency framework and a CBL point of view. Secondly, it described the individual properties of these two perspectives, which distinguish them fundamentally from a structural point of view. Chapter 4 then continued by discussing how competency is addressed in network security. It also showed that there is a gap in how competency frameworks and CBL are approached in network security. The previous chapters established the foundation for this chapter, which proposes how competency frameworks and CBL can be mapped together to close this gap in network security.

The closing of the gap is accomplished through the creation of a Design Science artefact in the form of a topic map. This chapter is split into three parts based on the context in which the solution is developed. The first part, *'Describing Topic Maps'* introduces the concept of a topic map and the requirements for creating a topic map data model. The second part, *'TMDM for Network Security'*, deals with the actual construction and presentation of the network security topic map (Solution). The last part of the chapter deals with the evaluation of the topic map through a Proof of Concept and a Focus Group scenario.

Part 1: Describing Topic Maps

5.2 Defining Topic Maps

A topic maps is a conceptual network of nodes and relationships between nodes that is used to represent the interconnectedness of information. Topic maps share some knowledge representation characteristics of semantic networks and information management characteristics similar to indexes. As such, topic maps can bridge the gap between knowledge representation and the field of information management. This is achieved by allowing users to map knowledge whilst providing an effective means of navigating through those knowledge structures (Pepper, 2013). The ISO standard (ISO/IEC 13250) is the official standard for describing topic maps. It is commonly referred to as the *'Topic Map Standard'*. One major benefit of this standard is that it does not come with a predefined ontology. This means that there are no restrictions on the application of topic maps, and even fewer constraints on how topic maps are supposed to be modelled (Ahmad, Sahib, & Nor'Azuwa, 2014). The topic map can serve as a high-level overview of the knowledge contained in a set of resources, which allows experts to model their knowledge and non-experts to understand the relationships between resources before diving down into more detail about the resources (Ahmad et al., 2014).

Because topic maps provide a good means of handling data from a meta-modelling perspective, they are a good technology for mapping frameworks of different types of structures into a holistic model.

In his paper, Grant (2006) describes a method of mapping what he refers to as common frameworks with specific frameworks by using a topic map. Common frameworks are described as high-level frameworks with generic descriptions of concepts in a particular domain. As such, they are very similar in characteristics to competency frameworks. In contrast, specific *'operationalised'* frameworks are described as being tightly designed to suit the requirements of a particular body, very similar to CBL. Thus, the creation and evaluation of the topic map in this dissertation should provide a holistic way of mapping competency frameworks and CBL together, and also provide an effective way of navigating this knowledge structure.

5.3 Components of a Topic Map

At its core, a topic map consists of a collection of 'Topics', which are related to each other by *'Associations'* and which may also be related to a number of resources by *'Occurrences'*. These fundamental components of a topic map are commonly referred to as the TAO of topic maps. The TAO of topic maps are so dynamic that they are the only source of information that is required to translate a mental model into a topic map (Ahmad et al., 2014).

Topics: At the heart of topic maps are its Topics, which represent the concepts that the topic map is about (Ahmad et al., 2014).Topics are the nodes in the topic map that represent a subject being referenced. Each topic represents a single subject. A subject in this sense can be anything from a person, a concept or an instance of something (Pepper, 2013). Topics can be categorised according to what concept they represent. For instance, *'competency'* and *'job role'* could be the topic type while *'network specialist'*, *'network design'* and *'incident handling'* would be the actual topic. According to the Topic Map Standard, any given topic is an instance of zero or more topic types (Pepper, 2013).

Associations: An association shows the link between two or more Topics. Thus, Associations are the components that represent relationships between Topics in a topic map.

An association can be thought of as a grouping of different types of Topics based on some instance (Pepper, 2013). For instance, *'job-competency'* can be an association that describes the relationship between *'competency'* and *'job role'*. Just like Topics, Associations between Topics can also be assigned types that specify the context of the relationship. Furthermore, each topic that participates in an association is given a role that indicates the way in which that particular topic participates in the association. Roles in an association are described by role type(Ahmad et al., 2014).

Occurrences: A topic may be linked to resources which are relevant to the topic in some capacity. Such resources are referred to as the Occurrences of the topic. Occurrences are a means of storing information about a topic (Pepper, 2013). The data that is stored as an occurrence can be of many data types such as strings (description), images or external documents. Much like Topics and Associations, Occurrences can also be categorised according to a declared type. Furthermore, Occurrences distinguish between occurrence types by using occurrence roles.

Figure 5.1 is an example and an illustration of a musical tour topic map. The topic map links documents about artists and the cities in which they have performed. The topic map has two topic types (City and Artist) that describe the context of the documents (Resources). The Associations thus link an artist and a city. For example, *'Driemanskap'* is an artist that has performed in *'Johannesburg'* with the artist *'Adele'*. This relationship is shown through topic type instances between the Topics.

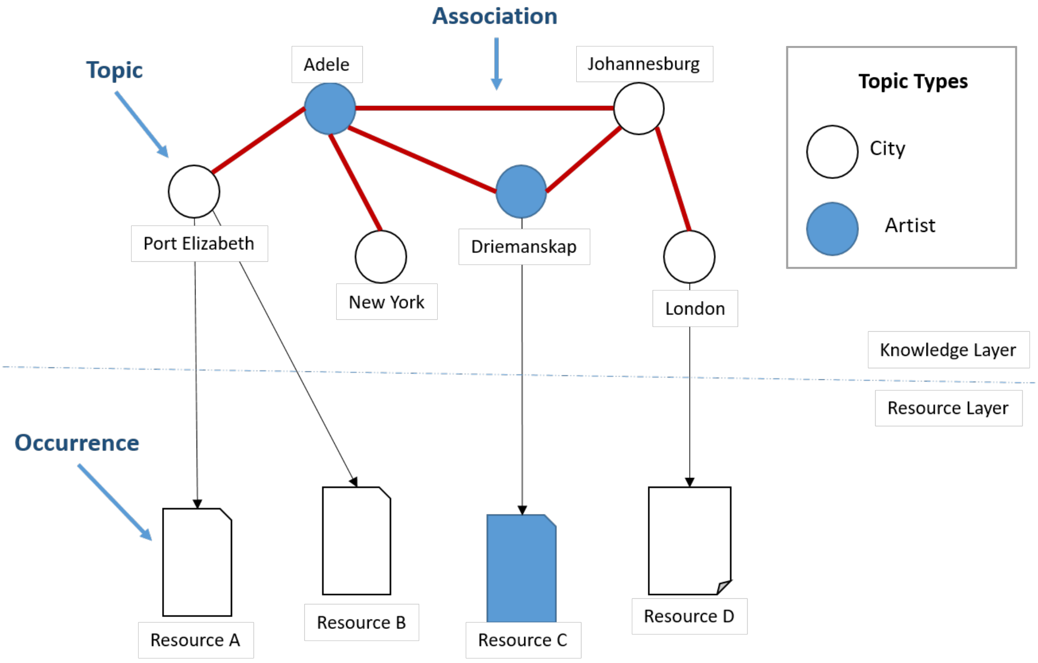


Figure 5.1: Basic topic map structure

5.4 Features of Topic Maps

Although Topics, Associations, and Occurrences (TAO) are the cornerstone of every topic map, the Topic Map Standard also prescribes additional features that enhance topic maps. The most prominent of these additional features are sometimes referred to as the *'IFS of topic maps'*, which is an abbreviation for *'Identity'*, *'Facet'* and *'Scope'*.

Identity: The Topic Map Standard specifies *'subject identifiers'* as a means of uniquely identifying subjects in a topic map. Subject identifiers are expressed as a (Uniform Resource Identifier) URI address and are used for each topic in the topic map (Pepper, 2013). It is important to note that Associations and Occurrences are also regarded as Topics themselves. Thus, they also utilise the identity feature. Subject identifiers allow different topic maps to be merged together. The Topic Map Standard specifies the procedures for merging topic maps.

The concept of merging topic maps can be initiated when two or more Topics sharing the same subject indicator are replaced by a new topic that encompasses the properties (names, Occurrences and Associations) of the original Topics (Ahmad et al., 2014). For instance, if a topic map author is creating a topic map of company resources across several branches, the author can merge the individual branch topic maps together. The topic map will know that *'CEO'* and *'Odwa Yekela'* are names for the same employee and merge the two Topics on that basis.

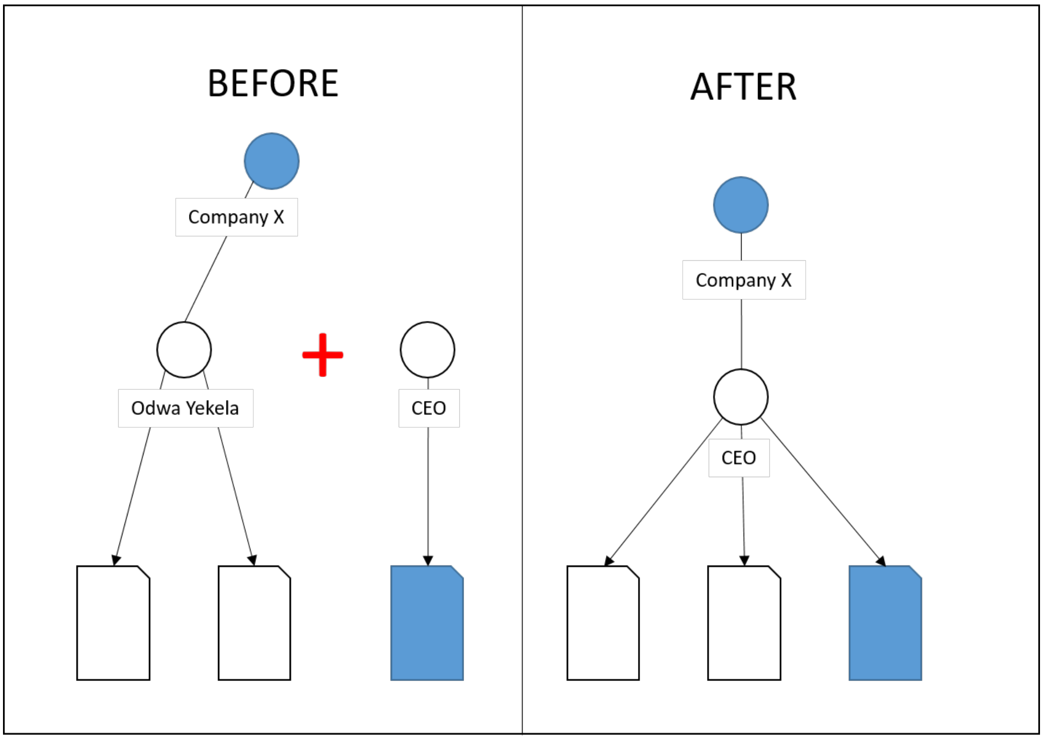


Figure 5.2: Merging two topic maps together

Facets: Facets are a feature that allows users to filter down topic map content based on some criterion specified by the user. Facets can be used to create query filters that interrogate the topic map and return a set of results (Pepper, 2013). For instance, a topic map of competencies and job roles can be queried to return results that display competencies that apply to a specific job role only. Figure 5.3 illustrates the use of a facet filter to only display Topics, Associations and Occurrences that apply to the query statement.

The left image is the topic map before the facet feature is applied and on the right is the topic map after the facet feature is applied. In the 'BEFORE' image all the topic Associations can be seen, but in the 'AFTER' image the topic map has been queried to show only specific relationships

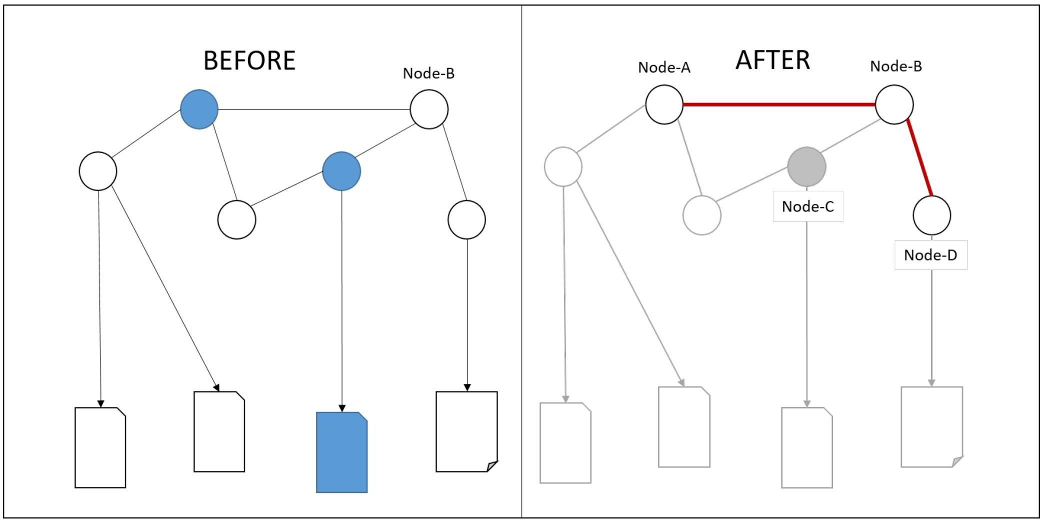


Figure 5.3: Applying facets for filtering

Since topic maps contain data structures deemed to be important to users, they can be interrogated to find information much like databases. This querying of information in a topic map is a result of the facet feature (Pepper, 2013). Facets are expressed through query statements, which are compiled using a Topic Map Query Language (TMQL). TMQL is a XML-based language protocol. The TMQL standard home page describes several query languages for topic maps. These include tolog (expressed specifically in lowercase), TMRQL and Empolis TMQL.

Scope: The term *'topic characteristics'* refers to the name of the topic, what Associations it participates in and what Occurrences it has. The limit of validity with which topic characteristics are used, is referred to as Scope. Scope is therefore used to describe the context in which something is said about a topic. Furthermore, Scope does not only remove ambiguity, it also allows different "viewpoints" of the topic map (Pepper, 2013). Figure 5.4 shows how Scope can be applied to a topic map to add context to the Topics, while also serving as a viewpoint.

In this illustration, 'BEFORE' is a complete view of the topic map, while 'AFTER' has been scoped down to show only specific relationship types. The main difference between Facets and Scope, is that Facets query specific information about *'Topics'* and *'Associations'*, while Scope can narrow the full view by showing only specific *'Topic types'*.

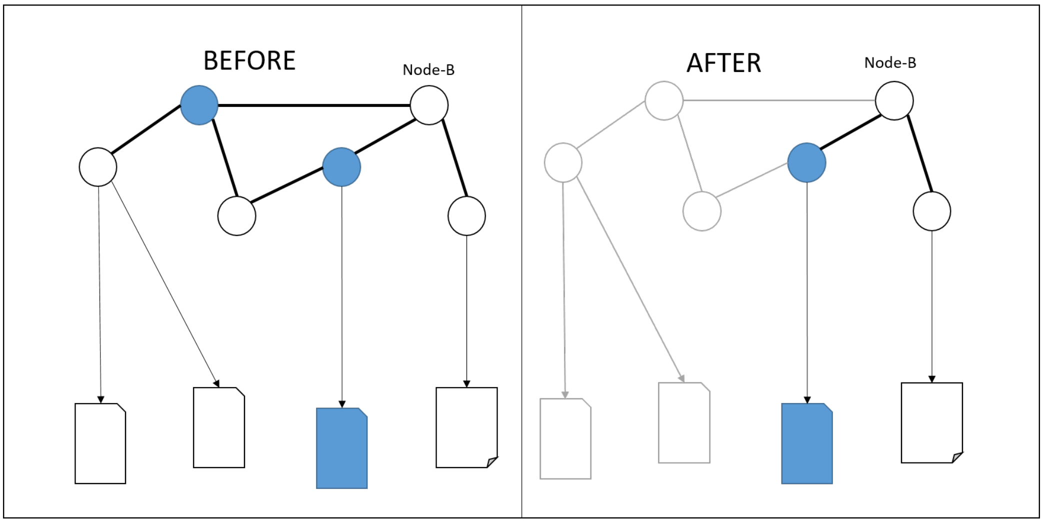


Figure 5.4: Scope feature applied in a topic map

5.5 Output of a Topic Map

Topic maps can be graphically represented in any way as long as it confirms to the Topic Map Standard rules. Among the most popular methods of graphically representing topic maps is the Graphic Topic Map (GTM). GTM is an ISO standard proposal for graphically explaining Topic Map Data Models (TMDM) on whiteboards, as well as within diagram-based software such as Microsoft PowerPoint. More complex TMDM can be expressed in topic map design applications such as Ontopia and TMNav. These applications use topic map engines to generate complex topic maps based on constraints.

Topic Map Engine Topic map engines make up the core of every topic map application. They provide a comprehensive way of building topic map applications. Topic map engines allow for topic map structures to be created, modified and managed through topic map applications (Hatzigaidas, Papastergiou, Tryfon, & Maritsa, 2004).

Therefore, to effectively author a complex topic map it is necessary to use a topic map application that provides an easy-to-use interface for the creation of TMDMs (Hatzigaidas et al., 2004).

Part 2: TMDM for Network Security

5.6 Constructing the Topic Map

The main objective of this research is to construct a topic map that shows how competency frameworks and CBL can be mapped together. Therefore, in correlation with this objective, a topic map is created specifically to represent network security competencies. The competencies displayed in the topic map are abstracted directly from the competency frameworks and CBL frameworks. The selection process for the competency framework and CBL is based on finding the simplest way to express the research solution. The process of developing the proposed topic map is described in the following steps, which are followed in this chapter:

1. Deciding what competency framework and CBL framework to use for the topic map.

2. Deciding how to best align and map the competency framework and CBL framework selected in the previous step.

3. Developing a TMDM to represent the relationships in the topic map graphically.

4. Expressing the TMDM on a topic map application.

5. Examining and analysing the relationships within the topic map to interpret useful data that can be leveraged for decision-making.

There are many possible ways of mapping competency frameworks and CBL together. This is perhaps best described by the classical phrase *"There's more than one way to skin a cat"*. With that said, one possible way of accomplishing the mapping is to break down the individual properties of the competency framework and CBL framework and to observe how well they synchronise. Since the main property of a competency framework is to describe competencies from a high-level point of view, the competencies from this framework can be represented as Topics describing the "What" element of the topic map. CBL frameworks, on the other hand, are much more detailed in describing what is expected from the competency. As such, they can be represented through Occurrences, which are the "How" element of the high-level competencies. This design would, in fact, correlate well with how topic maps traditionally deal with information structures

> *"The topic map can act as a high-level overview of the domain knowledge contained in a set of resources and also as a way for experts to model their knowledge in a structured way. This allows non-experts to grasp the basic concepts and their relationships before diving down into the resources that provide more detail"* - (Ahmad et al., 2014)

This quote hints at the idea that the knowledge layer of a topic map (Topics) can act as a high-level overview of a domain, while the resource level of the topic map can point to resources (Occurrences) for more detail. Essentially, what this dissertation solution is doing, is presenting a method of mapping two type of frameworks (common framework and specific framework described earlier) by using an IS technology such as a topic map. Figure 5.5 is an illustration of the proposed mapping between competency frameworks and CBL. The illustration shows competencies from competency frameworks as Topics and depicts CBL as the Occurrences of the topic.

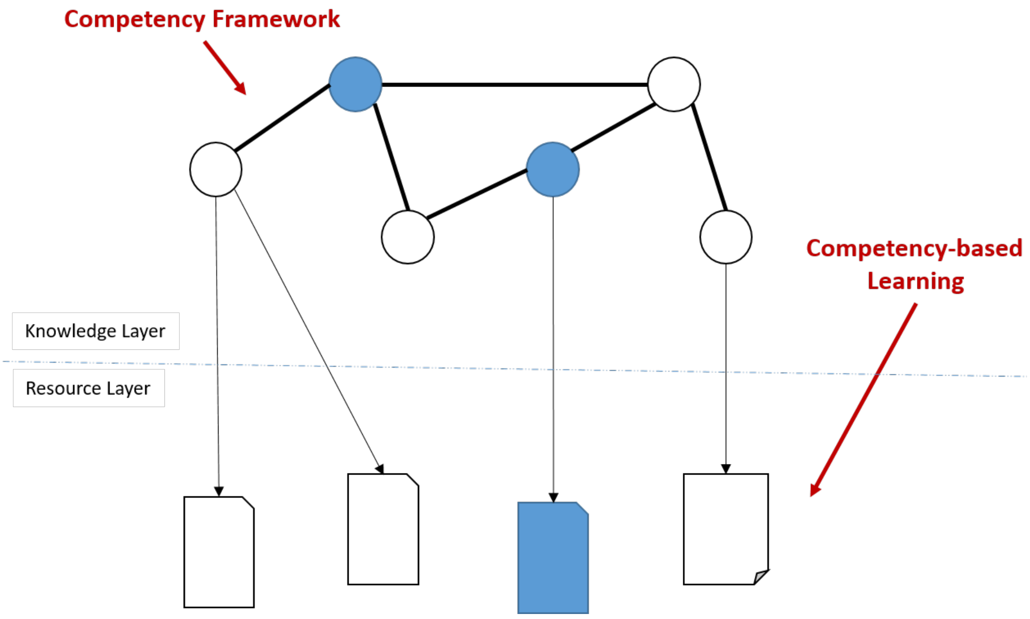


Figure 5.5: Basic topic map structure

5.6.1 Challenge of Mapping Competencies

To fully express a holistic mapping of competencies, the first step is to synchronise the competency framework with the CBL framework. This is to allow relationships between competencies to flow smoothly across the topic map. This alignment of competencies proves to be a challenge, because the individual competency frameworks and CBL frameworks are developed by independent bodies. Although these bodies may share the same interpretation of what competency is, they have different ways of representing competencies in their competency frameworks and CBL frameworks. For instance, the SFIA framework (discussed in chapter 3) focuses on the competence element of competencies, while the NICE Framework focuses on describing the performance element. Cisco, as a CBL framework, focuses a lot on vendor technology, while SANS GIAC focuses less on vendor technology and has fewer emphases on technology than Cisco. Thus, all the considered frameworks, whether it be competency frameworks or CBL, have their relative strengths and weaknesses. The objective is to select the frameworks that present a simple way of holistically representing the relationship between competencies in network security.

5.6.2 Selecting Competency framework and CBL

As previously discussed in Section 4.2, network security is a discipline that integrates with other disciplines such as *'Information Security'* and *'Networks'*.As such, some competency frameworks like SFIA may not address network security directly as a competency, but may have several other competencies that relate to network security in some capacity. From the frameworks discussed previously in Chapter 3, two were considered as most relevant, namely the SFIA and NICE Frameworks.

SFIA: The SFIA Framework was selected because it is able to represent competencies from multiple levels of competence. This allows even a single competence to be appreciated from multiple perspectives. Although this feature may be used by other competency frameworks such as e-CF, SFIA is still the most widely used competency framework in the world. Furthermore, it is also used professionally by the Institute of Information Technology Professionals South Africa (IITPSA).

NICE: Unlike the SFIA Framework, the NICE Framework has a flat-bed structure in the sense that it does not represent competencies at multiple levels. It does, however, provide a wide array of competencies in network security that allow for a smooth integration of Topics and Occurrences.

With regard to CBL, only the Cisco CBL framework was selected. This is because the SANS GIAC focuses heavily on competencies outside network security. This is problematic because as an occurrence of a topic, the CBL must be sufficiently detailed. Furthermore, when GIAC is compared to the Cisco framework, Cisco's CBL framework proves to be significantly better suited for representing CBL from a network security point of view.

5.6.3 Instances of the Topic Map

The primary objective in creating the topic map is to demonstrate that it is possible to map a competency framework and CBL holistically by using a topic map.

Thus, the core of this solution is representing how these frameworks can be mapped together to express network security competencies holistically. As such, the topic map is not restricted to using only specific frameworks to achieve the objective. It is possible to use interchangeable frameworks and still get the same utility from using the topic map. With that said, it is important to note that there is a one-to-one relationship between the frameworks and the topic map. This means that only one competency framework and only one CBL framework can be used for a single topic map. This realisation gives rise to the idea of using different *'instances'* to show that a network security topic map can use interchangeable frameworks to illustrate the same utility, regardless of the frameworks used.

There are two instances of the topic map that are presented as the solution Proof of Concept. In the previous section, three candidate frameworks (SFIA, NICE, and the Cisco Framework) were identified as favourable frameworks for mapping. As such, these frameworks are used in the topic map, but in different instances. The first instance will map the SFIA framework with the Cisco CBL framework, while the second instance of the topic map will map the NICE Framework with the Cisco CBL framework. These instances of the topic map are described in more detail below:

The first instance: is a topic map that maps competencies from SFIA and Cisco framework together. This instance is later referred to as the SFIA-Cisco topic map. In this instance, emphases during design was placed on aligning SFIA levels of competence with Cisco levels of certification. Doing so provided a way of representing what competence should be given to an individual who possesses competencies at a specific Cisco certification level. In Chapter 3, a comparison between SFIA levels of competency and Cisco certification levels was done. From this comparison, attributes of the topic maps were designed.

The second instance: of the topic map is the mapping between the NICE and Cisco frameworks. This instance is later referred to as the NICE-Cisco topic map. In this topic map emphases during design was on competencies and the understanding of specific technologies required for each of the competencies described by NICE.

The levelling scheme is artificially created in this second instance through the introduction of a new variable. This artificial level is created because there is no prescribed levelling scheme in the NICE Framework. The artificial levelling scheme created in this topic map focuses more on evaluating the understanding of competencies.

Although different levelling schemes were used during the design of the topic maps, both instances of the topic map followed the same principle which allowed the competency framework to be mapped with the CBL framework.

5.7 Designing the Topic Map

In the previous section, it was decided how the proposed network security topic map design will look conceptually. This section sheds light on the deeper mechanics of the design. Therefore, this section will provide an explanation of the network security topic map instances and their components.

5.7.1 Topics used in Topic Map

The basic components of any topic map, as described earlier, are Topics, Associations and Occurrences. In the network security topic map, higher knowledge about the frameworks is described in topic types. These topic types are linked together through some form of association. Occurrences are the resources that stem from the topic type relationships. Table 5.1 shows all the topic types used in both instances of the topic map. Although it was stated in the previous section that competency frameworks would represent the Topics (topic types) and CBL would represent the Occurrences, the topic map does have topic types that correlate with CBL. These Topics types are, however, not the actual Occurrences. Instead, they are used to abstract knowledge about the characteristics of the Occurrences. The top portion of the table is dedicated to showing the topic types created for the SFIA and Cisco instance, while the bottom section shows the topic types for the NICE and Cisco instance. All the topic types are represented in uppercase so that they are easier to distinguish from the rest of the text in the paragraph.

Table 5.1: All Topic types included in the Topic Map

Topic Types: SFIA-Cisco
COMPETENCY
SFIA LEVEL
DOMAIN
JOB ROLE
CERTIFICATION
EXAM
TECHNOLOGY
Topic Types: NICE-Cisco
COMPETENCY
JOB ROLE
CERTIFICATION
EXAM
TECHNOLOGY
TAXONOMY-LEVE

In the table, *'COMPETENCY'*, *'SFIA LEVEL'* and *'DOMAIN'* were created based on properties from the SFIA framework, whereas *'CERTIFICATION LEVEL'*, *'EXAM'* and *'TECHNOLOGY'* were inspired by the Cisco framework. *'JOB ROLE'* is a topic type that is independent from the frameworks. It was created to add context to the two frameworks. In the second instance, only *'COMPETENCY'* is carried from the NICE Framework and the same topic types from the Cisco framework were also used in the second instance. *'JOB ROLE'* is also used in this second instance, but another new topic type, TAXONOMY-LEVEL, is added. These topic types are discussed in further detail below:

- **COMPETENCY** refers to the competencies taken directly from the competency frameworks.

- **SFIA LEVEL** is a levelling scheme used by SFIA. It represents levels of competence related to competencies.

- **DOMAIN** consists of four sub-topic types, namely *'INFLUENCE'*, *'AUTONOMY'*, *'COMPLEXITY'* and *'BUSINESS SKILL'*. These topic types are used to express a more holistic view of competence at different SFIA levels.

- **CERTIFICATION** is a levelling scheme used by Cisco. It represents the level of competency expected based on mastery-learning (discussed in Chapter 3).

- **EXAM** relates to a Cisco exam. Each exam consists of a number of detailed learning outcomes and relates to a certification level.

- **TECHNOLOGY** refers to the technology that should be learned from a learning outcome. A technology may be understood at different taxonomy levels and may be related to a competency.

- **TAXONOMY-LEVEL** is a topic type created outside the frameworks. It is a levelling scheme used by technology to describe different levels of cognitive knowledge that can be applied using a technology.

- **JOB ROLE** is the only topic type used in both instances. It represents a network security job role. Multiple job roles can relate to one or more job positions.

Each topic type used in the topic map consists of multiple instances of the topic type. These individual instances of the topic types are too many to be listed in this section, but they can be seen in appendix C.

5.7.2 Associations used in Topic Map

The second task as discussed in step 2 from Section 5.6, is to graphically represent the Associations between each of the topic types. Each of the Associations is a relationship between two or more Topics. These relationships are described in detail with the aid of visual representations. The SIFA-Cisco topic map has five Associations which are, competency-level, job-competency, exam-certification, exam-technology and sfia-cisco-level. It also has two additional dynamic relations, while the NICE-Cisco topic map has four Associations which are, competency-technology, technology-taxonomy-level, exam-certification and job-competency, and only has one dynamic relationship.

Competency-level: Figure 5.6 illustrates the association between three topic types. These topic types are associated by the association type called competency-level.

This association type links the DOMAIN topic with the appropriate SFIA LEVEL and feeds this information to COMPETENCY. Thus, each competency will have a description of the domain type based on the SFIA levels applicable to that competency. For example, SFIA *'Level 4'* describes the domain area *'Complexity'* as *"Work includes a broad range of complex technical or professional activities, in a variety of contexts. Investigates defines and resolves complex issues"*. This description is then passed to *'Information Security'* at *'Level 4'*.

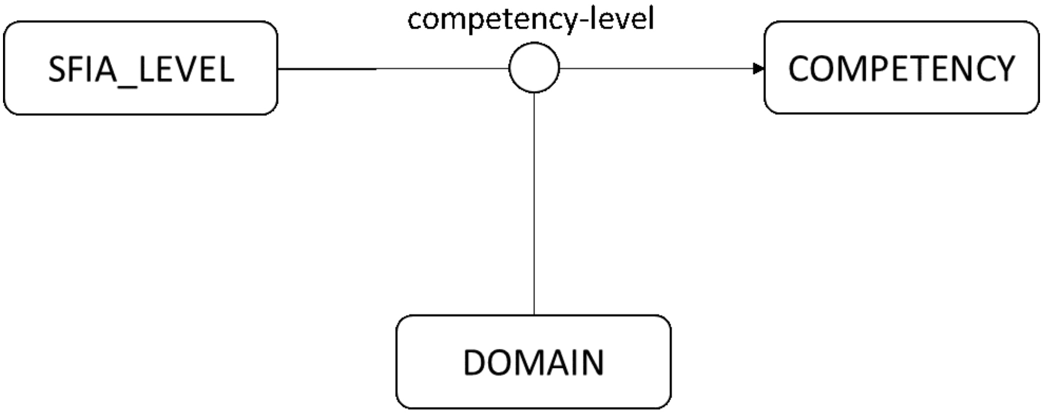


Figure 5.6: Relationship used to create competency levels

in the image, a pointed arrow is used to illustrate the flow of information in the association. Generally, information in topic maps will always flow universally across both directions. But since Figure 5.6 is only a representation to help the reader understand the context of the association, the use of arrows is acceptable.

Job-competency: Figure 5.7 also uses a multi-relationship association between its topic types, SFIA LEVEL, COMPETENCY and JOB ROLE, which are all linked together by the association type called job-competency. This association takes a level from SFIA and links it directly with the corresponding competency. This link is then fed into JOB ROLE, thus allowing the appropriate competency to be allocated to the job role at the right level. For example, the job role *'Security Manager'* may require *'Information Security'* at a SFIA *'Level 4'*.

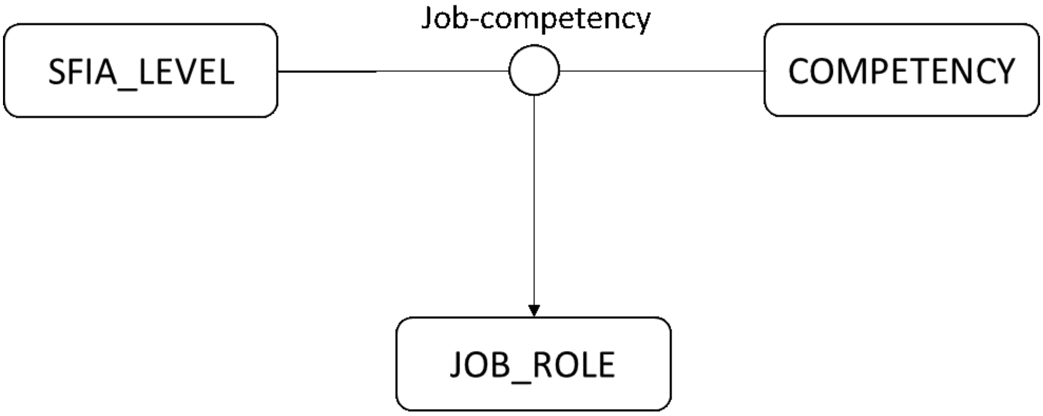


Figure 5.7: The competencies required for job role

Exam-certification: This association type is bi-directional. As such, it is conveyed using bi-directional arrows. This relationship is between the Topics CERTIFICATION and EXAM, as illustrated in Figure 5.8. This association is the first association type based on the characteristics of the occurrence field. The two topic types are associated by exam-certification. This association links CERTIFICATION with the appropriate exams. Furthermore, since the certification levelling scheme used by CERTIFICATION is based on mastery-learning, an ascending CERTIFICATION instance will automatically have all the predecessor EXAM instances. For example, *'Associate'* is a CERTIFICATION instance which requires the *'210-260 IINS'* EXAM and the predecessor for *'Associate'* is *'Entry'* which requires the *'100-105 ICND1'* EXAM. Thus, when someone wants to achieve *'Associate'* level, they have to pass two exams (*'100-105 ICND1'* and *'210-260 IINS'*) due to this hierarchical structure.

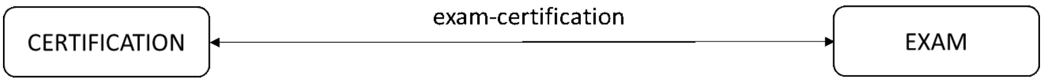


Figure 5.8: Exams required to obtain certification

Exam-technology: The second bi-directional relationship is between TECHNOLOGY and EXAM. This is also the second association that is based on the characteristics of the occurrence field. The two topic types are associated by exam-technology, as illustrated in Figure 5.9.

This association takes the TECHNOLOGY used in an occurrence and links it to an EXAM. For example, the TECHNOLOGY instance *'VPN'*, which is a property of *'Network Security'*, is included in the *'210-260 IINS'*, *'300-209 SIMOS'* and *'400-251'* EXAMs.

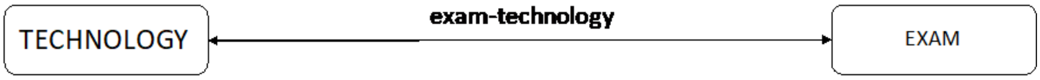


Figure 5.9: Technologies accessed in each of the exams

SFIA-Cisco-level: The next bi-directional relationship links topic types from both the SFIA and Cisco frameworks (Figure 5.10). Therefore, this association is the first implicit relationship between the two frameworks. This association type essentially aligns the SFIA levelling scheme with the Cisco levelling scheme. The objective of this association is to align the level of understanding of competencies (CERTIFICATION) with the level of competence (SFIA) that should be expected at that particular level. For example, the CERTIFICATION level *'Professional'* correlates with the competence of *'Enable'* from the SFIA LEVEL. This alignment of levelling between the Cisco and SFIA frameworks, is based on the comparative analysis conducted in Section 3.6 of Chapter 3.

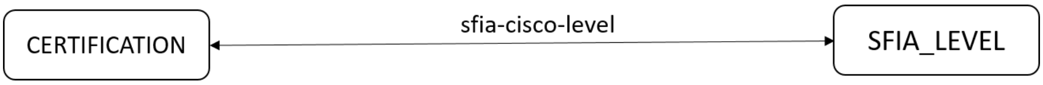


Figure 5.10: This relationship bridges SFIA levels with Cisco levels

Dynamic relationships: The next two bi-directional relationships that will be discussed, differ from the previous relationships, because they are dynamic relationships. Unlike all the previous relationships, a dynamic relationship is not manually created through association types. The first dynamic relationship (Figure 5.11) is created when a user runs a query statement linking instances of COMPETENCY with instances of TECHNOLOGY. This relationship is dynamic, because it is not implicitly created in the topic map. Instead, it only exists when it is called upon through a query statement. This is why the image in Figure 5.11 has no association name and is illustrated with a dotted link between the topic types. This relationship is meant to query COMPETENCY and abstract information about the TECHNOLOGY used in the COMPETENCY occurrence. This dynamic relationship is significant, because it indirectly links information from one framework with another framework.

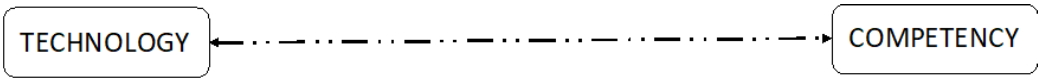


Figure 5.11: Dynamic relationship between technology and competency.

The next dynamic relationship queries the topic map to determine which instances of EXAM correlate with a specific JOB-ROLE instance. The aim of this relationship is to determine which exams should be taken to meet specific job role requirements. For example, if the user wants to determine which exams a candidate would take to entire the *'Security Manager'* position. Figure 5.12 illustrates this dynamic relationship by using the dotted arrow between the topic types.

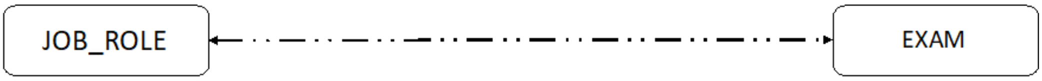


Figure 5.12: Dynamic relationship between competencies and job roles.

Technology-taxonomy-level: This is an association used by the NICE-Cisco topic map. It links the TAXONOMY-LEVEL with the TECHNOLOGY as illustrated in Figure 5.13. The aim of this association is to create a means of assessing the different levels of understanding of a technology based on the competency. The topic type called TECHNOLOGY is a representation of the technology used in the learning outcomes (learning outcomes are Occurrences of the COMPETENCY topic type). For example, *'VPN'* is a technology used in some competencies and is described through learning outcomes. The learning outcomes specify what is expected from the competency. A learning outcome for *'Network Security'* may specify *"Configure and Apply VPN tunnelling in a site-to-site network"*. This learning outcome correlates with the *'Apply'* (level 3) Taxonomy level, thus *'VPN'* is required at a *'level 3'*.

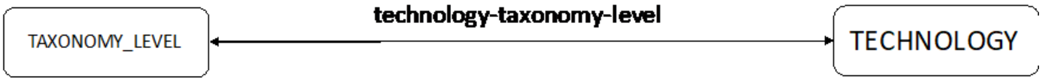


Figure 5.13: Relationship used to associate different taxonomy levels with specific technologies

Job-competency This association type is specifically used by the NICE-Cisco topic map and is illustrated in Figure 5.14. This association links COMPETENCY with JOB-ROLE. The aim of this association is to determine what competencies are required for specific job roles. For example, *'Network Security'* is a competency that is used by *'Network Administrators'*. Basically, this association is a variation of job-competency as used by the SFIA-Cisco topic map.

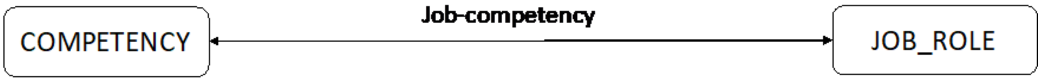


Figure 5.14: Relationship used to create job competencies

Competency-technology: This second last association (Figure 5.15), is a multi-relationship association between EXAM, TECHNOLOGY, and COMPETENCY. This association links TECHNOLOGY with EXAM and this information is then fed into the topic COMPETENCY. The aim of this association is to determine the exam and technology related to a competency, based on the learning outcome (Occurrences of competencies). This association is a variation of the exam-technology used by the SFIA-Cisco topic map.

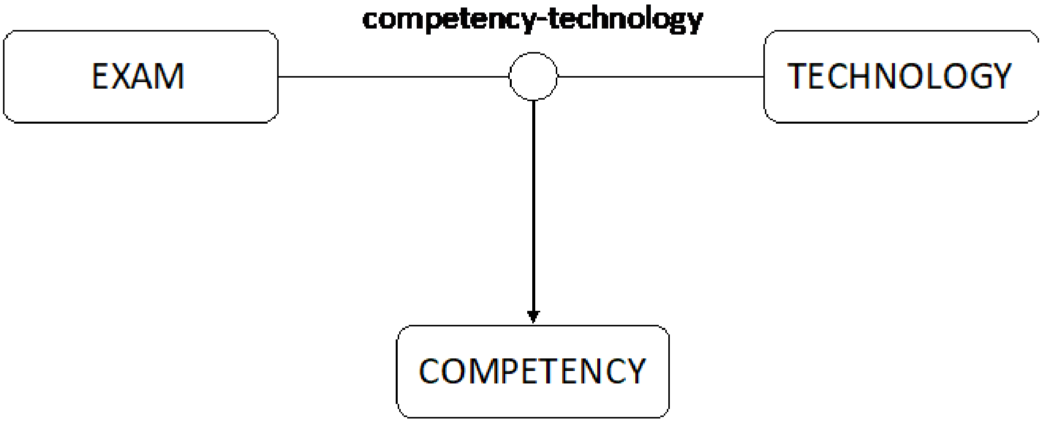


Figure 5.15: Relationship used to link competencies with technology type

The last relationship that is described is a dynamic relationship used by the NICE-Cisco topic map, this relationship indirectly links JOB-ROLE with CERTIFICATION, as illustrated in Figure 5.16. The aim of this association is to determine which job roles are available at specific certification levels. This allows the user to assess their certification ambitions with the related job roles. For example, a user may want to upgrade their *'Associate'* level certification to *'Professional'*. They can then use the topic map to assess what job roles will be available at the *'Professional'* level.

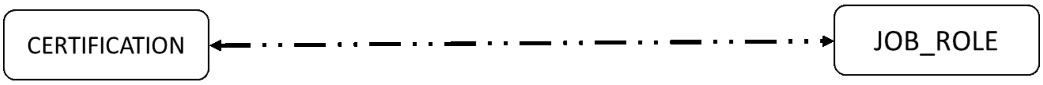


Figure 5.16: Dynamic relationship created to query certification need for job roles.

The Associations discussed in this section can be summed up in four quadrants. These quadrants are based on the type of relationships and the topic maps that implement the relationships. The quadrants are as follows:

- **Quadrant 1:** depicts Associations used by the SFIA-Cisco topic map (Figure 5.5, 5.6, 5.7, 5.8, 5.9, 5.10, 5.11, 5.12)

- **Quadrant 2:** depicts Associations used by the NICE-Cisco topic map (Figure 5.13, 5.14, 5.15, 5.16)

- **Quadrant 3:** depicts Associations used by both SFIA-Cisco and NICE-Cisco (Figure 5.5, 5.14)

- **Quadrant 4:** depicts the dynamic relationships not implicitly specified in the topic map (Figure 5.11, 5.12, 5.16)

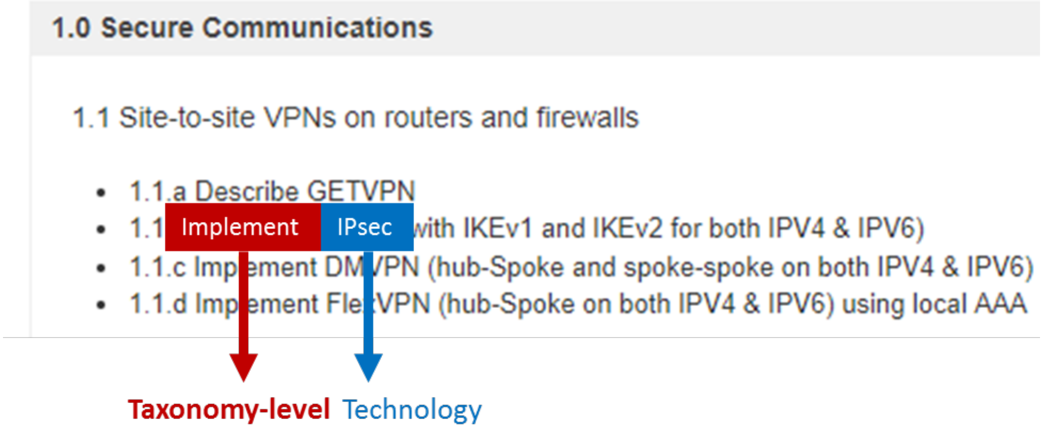
Although both the SFIA-Cisco and the NICE-Cisco topic map may have different ways of representing Associations, both are essentially seeking the same utility from the Associations. The next section discusses the occurrence field of the topic map.

5.7.3 Occurrences used in Topic Map

Occurrences are the last component that needs to be discussed to complete the TAO of the network security topic map. Occurrences were described in Section 5.3 as a means of storing information about a topic. Hence, it was decided in Section 5.6 that the Occurrences field would contain competency information from CBL that relates to the COMPETENCY instances. This information that is abstracted from the CBL is in the form of learning outcomes. Learning outcomes were discussed in Section 3.5.1 as elements that need to be mastered to be competent at a task. Learning outcomes are a good representation of the deeper context of a competency, because they are specific, measurable and written in a behavioural form. From the learning outcomes, a lot of information about the competency can be interpreted. This includes information about the technology used in a competency, what exams are required to achieve that competency and what level of understanding is expected from the competency. Figure 5.17 illustrates a sample of competencies taken from the Cisco *'300-209 SIMOS'* exam.

In this image a list of learning outcomes for implementing VPN technology is illustrated. The image shows what information can be abstracted about the competency from the learning outcome section and include the following:

- **Taxonomy level**, which is abstracted from the verb used in the Bloom's Taxonomy learning outcome. This is illustrated using the red textbox.
- **Technology**, which is abstracted from the concept being tested. This is illustrated using the blue textbox.
- **Exam** which is abstracted from the Cisco website



1.0 Secure Communications

1.1 Site-to-site VPNs on routers and firewalls

- 1.1.a Describe GETVPN
- 1.1 with IKEv1 and IKEv2 for both IPV4 & IPV6)
- 1.1.c Implement DMVPN (hub-Spoke and spoke-spoke on both IPV4 & IPV6)
- 1.1.d Implement FlexVPN (hub-Spoke on both IPV4 & IPV6) using local AAA

Figure 5.17: Abstracting topic types from learning outcomes

Learning Outcomes: The attributes of the learning outcomes (taxonomy-level, technology and exam) are represented in the topic map as topic types. This is because the attributes are not Occurrences themselves, but are higher knowledge about the Occurrences. Figure 5.18 illustrates how information about a learning outcome is abstracted from the occurrence field. This information is then stored in the topic types TECHNOLOGY, EXAM and TAXONOMY-LEVEL and then interlinked with other topic types as represented by the cloud. This abstraction allows the topic map to determine which technologies are shared across competencies, what network security exams are required to achieve competencies and what level of understanding of a competency is required by a job role.

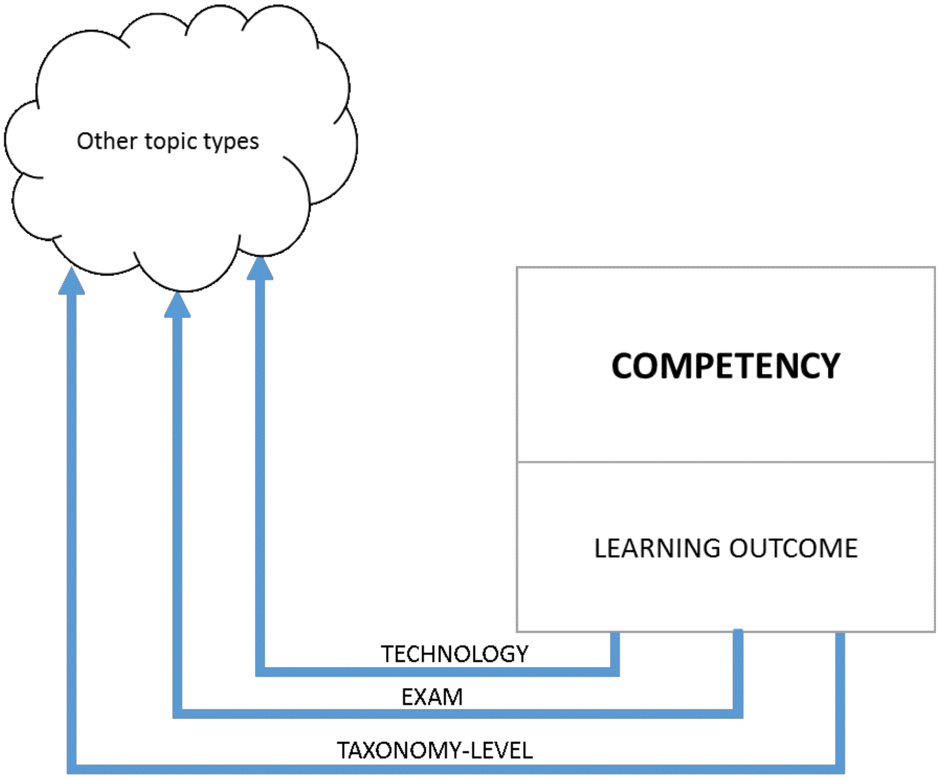


Figure 5.18: Creating topic types from learning outcomes

Other Occurrence Types: Although Occurrences are different from traditional Topics, occurrence types are essentially topic types themselves. As such, they can have Associations with other topic types. DESCRIPTION is a system occurrence type parameter used to represent a description of something. This occurrence type is used across multiple topic types to give a description of an instance. For example, DESCRIPTION is used by DOMAIN to give a definition of the DOMAIN instance. It is also used by COMPETENCY to give a description to a competency. Another occurrence type that is used, is EXAM-DOCUMENT. This occurrence type points to external documents about an exam. WEBSITE is another occurrence type which points to an external URL website address. The occurrence types discussed are shown in the table below.

Table 5.2 shows the occurrence types, the data types held by the occurrence types and what topic types the Occurrences apply to. The first column represents the occurrence type, the second column is the type of data that the occurrence holds, the third column represents the topic types that use that occurrence type and the last column shows which topic map instance uses the occurrence type (either SFIA-Cisco, NICE-Cisco or both).

Table 5.2: All Occurrence types in Topic Map

Occurrence type	**Data type**	**Topic type**	**Instance**
LEARNING-OUTCOME	string	COMPETENCY	BOTH
DESCRIPTION	string	COMPETENCY SFIA LEVEL DOMAIN JOB ROLE CERTIFICATION EXAM TECHNOLOGY TAXONOMY-LEVEL	BOTH
EXAM-DOCUMENT	doc	EXAM	BOTH
WEBSITE	uri	CERTIFICATION COMPETENCY EXAM	BOTH

Having completed the TAO of the network security topic map, the next step, as discussed in Section 5.6, is to graphically represent the topic map as a TMDM. This is accomplished through the use of GTM and is discussed in the next section.

5.8 TMDM Representation

A TMDM is a model representation of a topic map (Section 5.5). It can be represented graphically by using GTM. GTM is a proposed standard for notating topic maps (Section 5.5). This section describes the TMDM models for the network security topic map and explains the flow of information in the topic map. This section also explains the notation used in the TMDM.

5.8.1 TMDM Notation

Figure 5.19 is a sample from one of the TMDMs. It is used as an illustration to explain the notation used in the modelling scheme. A TMDM entity is basically made up of three fields. The top field, called the *'Association field'* describes the association relationships as discussed in Section 5.7.2. The *'Association name'* is the name of the association. *'Association role'* states how the topic type will link with other topic types in this association. This is expressed in the form *'Relationship-type.topic-map-name:topic-type-name'*.

The second field is the *'Instance field'*, which holds information about the instance of a topic type. Each line of this field is an instance of an association. *'Topic map name'* gives the name of the topic map. The *'nws'* topic map name shown on the diagram, is short for network security. There are other variables that this field can hold such as *'dc'* and *'tm'*. These variables are system parameters. The next attribute is *'Topic type name'* and stores the name of the topic type. While *'Relationship type'* states the type of relationship that an instance of the topic type can take in an association relationship, this is a choice between four possible parameters as shown below.

- **One-to-one:** This parameter means that only one value can be given to the Association role and is denoted as *'1..1'*.
- **One-to-Many:** This parameter means that at least one value must be given to the Association role field, but more values can be added if needed. This parameter is denoted using *'1..*'*.

- **Zero-to-One:** In this parameter type, only a single value can be added to the Association role or it can be left empty, thus giving this field a null value. This parameter is denoted as *'0..1'*.
- **Zero-to-Many:** This the last parameter type. It means that many values can be added as variables in the Association role, but the field can also be left empty. This parameter is denoted as *'0..*'*.

The last field is the *'Occurrence field'*, which holds information about the Occurrences of a topic. This field is expressed as *'topic-map-name:Occurence-type-name:Data-Type'*, where *'Data type'* refers to the type of data that an occurrence type can hold. Each line in this field also represents an instance of the occurrence type.

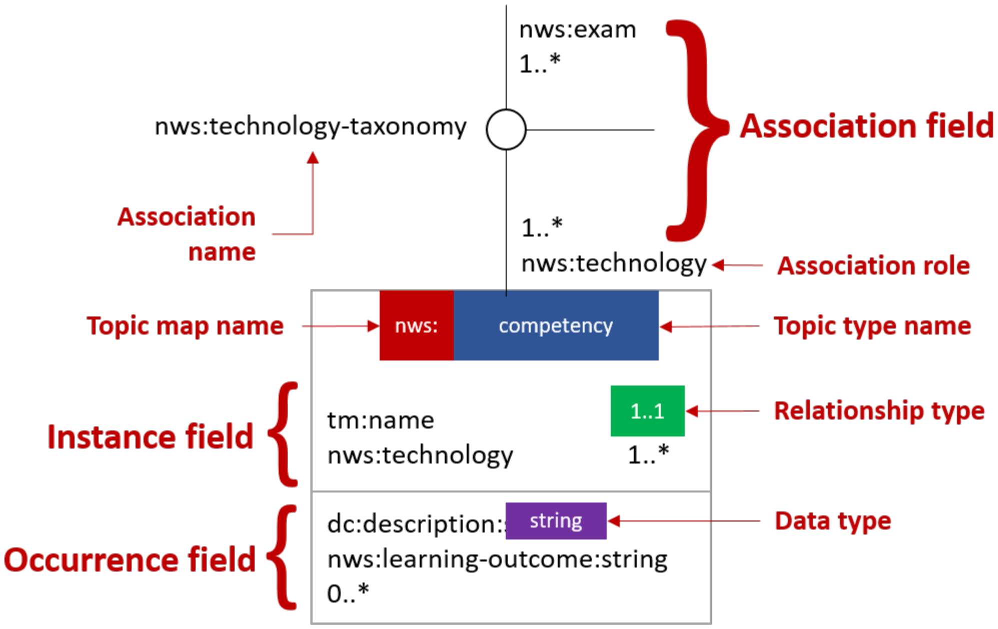


Figure 5.19: Sample of a topic type and it's relationships

5.8.2 TMDM Models

This section presents the TMDMs. The two images depicted in Figures 5.20 and 5.21 respectively, are two different TMDM models. Figure 5.20 represents SFIA-Cisco, while Figure 5.21 represents NICE-Cisco. The TMDMs in this section are essentially compilations of all the previous information from all the previous sections to produce two complete models of the topic map. Furthermore, the flow of information in the topic map is omnidirectional. This means that any topic type in the topic map can serve as a starting point when trying to determine the general flow of information, but since this is a topic map about competencies, the COMPETENCY topic type will be used as the starting point for both TMDMs.

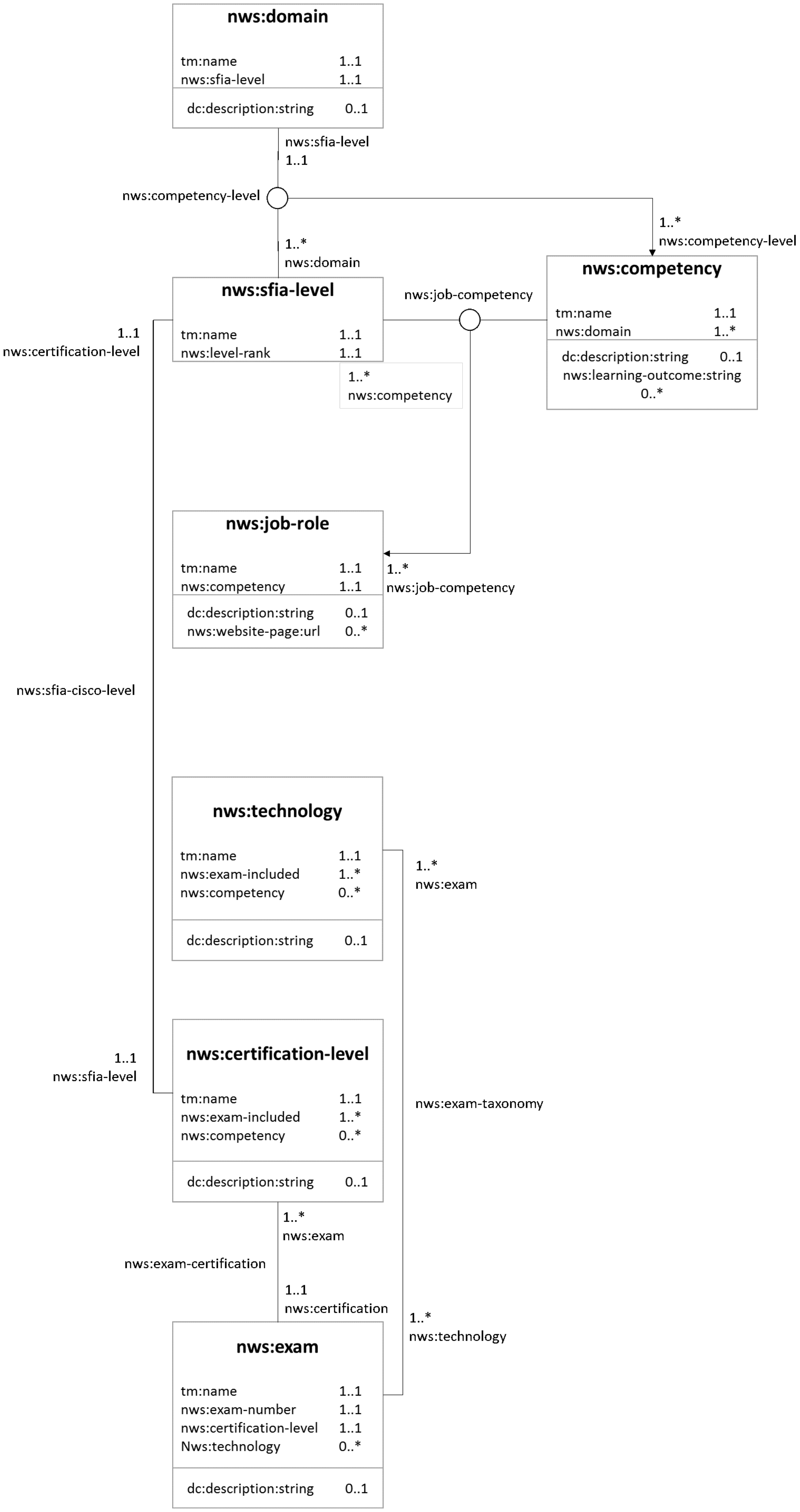


Figure 5.20: SFIA-Cisco TMDM

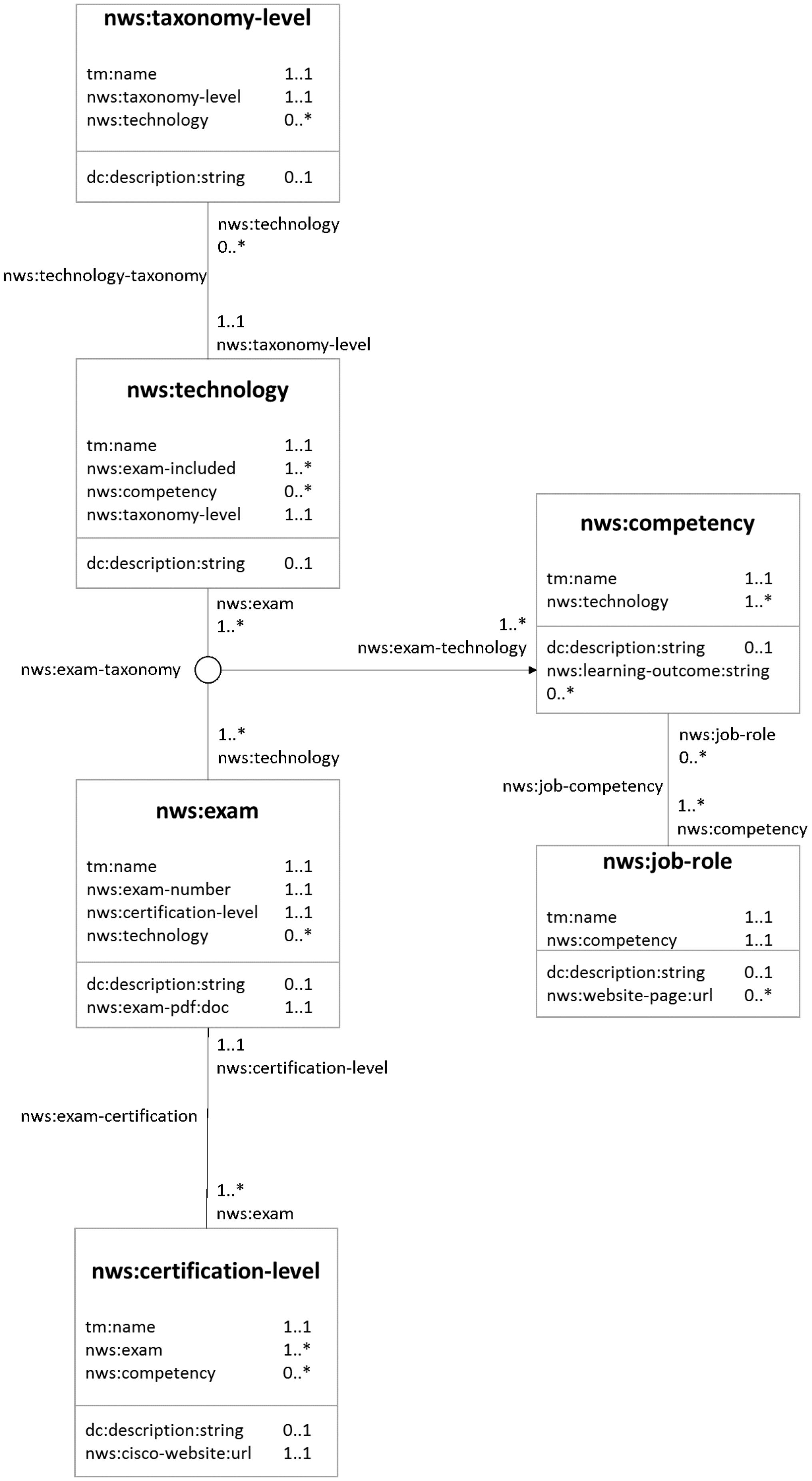


Figure 5.21: NICE-Cisco TMDM

SFIA-Cisco: The first TMDM that is discussed is the SFIA-Cisco TMDM. Information flow in this TMDM is broken down into eight steps. To get a better understanding of the context of the steps, it is advisable to cross-reference this section with Section 5.7.2.

1. The first association type *'competency-level'* maps the SFIA LEVEL with the DOMAIN and then feeds this information into COMPETENCY. The relationship between these three topic types splits competencies into multiple hierarchy levels, which have their own description of DOMAIN at each level. This information from *'competency-level'* is further fed into JOB ROLE through JOB ROLE's relationship with COMPETENCY.

2. The association *'job-competency'* takes the SFIA levelling scheme and applies it to COMPETENCY. This creates multiple levels of the same competency, which information is then fed into JOB ROLE.

3. The association types from step 1 and 2 (*'competency-level'* and *'job-competency'*) operate synchronously in providing information to JOB ROLE. Through their simultaneous use, JOB ROLE is able to determine competencies at different levels and the domains of those levels used by the competencies.

4. The other major flow of information is from the association between SFIA-LEVEL and CERTIFICATION. This association aligns the SFIA levelling scheme with the Cisco levelling scheme, thus providing a bridge between information from the SFIA framework (DOMAIN, SFIA LEVEL and COMPETENCY) and the Cisco framework (CERTIFICATION, TECHNOLOGY and EXAM).

5. The *'exam-certification'* association specifies which exams are related to a certification level. This information about the EXAM instances can be used to determine the exams required to achieve a competency at multiple Cisco and SFIA levels.

6. Information about the technology related to an exam is also aggregated into the flow of information. This is accomplished through the association type *'exam-technology'*, which exists between EXAM and TECHNOLOGY. This association type determines the technology used in a competency at different levels.

7. The interconnectedness of all the topic types introduces two additional relationships. These additional relationships are created dynamically. The first of the dynamic relationships is accomplished through the interconnectedness of five topic types (TECHNOLOGY, EXAM, CERTIFICATION, SFIA-LEVEL and COMPETENCY). It creates an indirect link between COMPETENCY and TECHNOLOGY.

8. The second dynamic relationship indirectly links EXAM with JOB ROLE. This relationship allows information about an instance of EXAM to be queried in order to determine which exams should be taken to meet specific job role competency requirements. This second dynamic relationship is also accomplished through the interconnectedness of five topic types (EXAM, CERTIFICATION, SFIA-LEVEL, COMPETENCY and JOB ROLE).

NICE-Cisco: The second TMDM to be discussed is the NICE-Cisco. It is advisable to cross-reference this section with Section 5.7.2. Information flow in this TMDM is divided into five steps:

1. The association type *'exam-taxonomy'*, supplies information about the technology and the exam related to a competency from the TECHNOLOGY and EXAM topic types and then feeds this information into COMPETENCY.

2. The *'technology-taxonomy'* association allows information about the level of understanding of a technology to be stored in the TECHNOLOGY topic type. This information is then accessible to COMPETENCY, because of its association with TECHNOLOGY.

3. Similarly, the *'exam-certification'* association describes what exams are needed to complete competencies at specific certification levels. This information about the exam is stored in EXAM, which is linked to

COMPETENCY, thus creating an indirect link that allows COMPETENCY to access exam-certification information.

4. All the information that has been fed directly and indirectly into COMPETENCY, becomes accessible to JOB ROLE through its association with COMPETENCY.

5. The dynamic relationship described in Section 5.7.2, indirectly links instances of CERTIFICATION with instances of JOB ROLE. This milestone is achieved through the interconnection of two topic types (EXAM and COMPETENCY) with CERTIFICATION and JOB-ROLE.

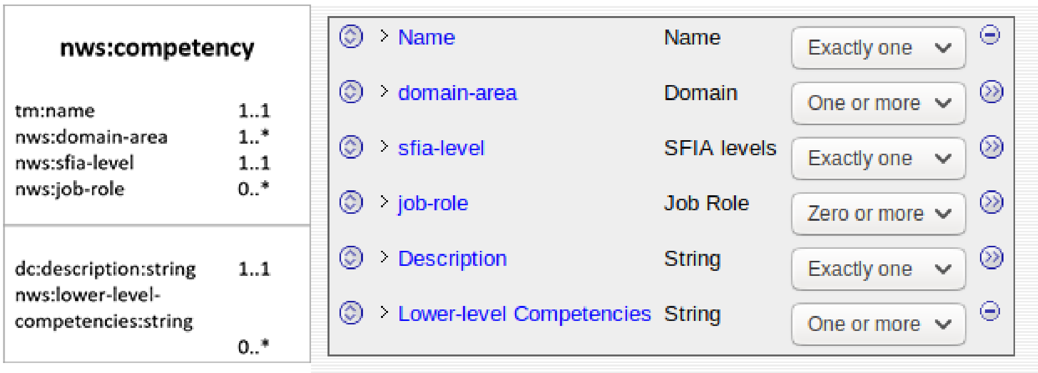
5.8.3 Images of Topic Map

This section provides images of the network security topic map. This section relates to the fourth step of constructing a topic map, as discussed in Section 5.6. During this step, the TMDMs (Figures 5.20 and 5.21) from the previous section are loaded onto topic map applications. A series of images are then generated from the applications to show the functionality of the topic map with respect to the use of topic map features to better represent competencies. Two topic map applications were used:

- **Ontopia:** This application was used to create the actual topic map as an XML file extension.

- **TMNav:** The XML file extensions were loaded into TMNav for visualising the topic map and performing additional functions such as Scope, Facet and Merging

By using these two applications, a complete ontology of the topic map was created. The ontology represents how the topic map connects information about competencies. The first image, illustrated in Figure 5.22, is a side-by-side comparison between the TMDM designed in Section 5.8.2 and an image of the SFIA-Cisco topic map as it was created in the Ontopia platform. This image portrays how the topic map was created with the aid of the topic map application. The attributes from the TMDM correlate directly with the structural design used in the topic map application.



nws:competency

tm:name	1..1
nws:domain-area	1..*
nws:sfia-level	1..1
nws:job-role	0..*
dc:description:string	1..1
nws:lower-level-competencies:string	0..*

Name	Name	Exactly one
domain-area	Domain	One or more
sfia-level	SFIA levels	Exactly one
job-role	Job Role	Zero or more
Description	String	Exactly one
Lower-level Competencies	String	One or more

Figure 5.22: TMDM comparison with image from the topic map application

The second image illustrated in Figure 5.23, is a screenshot of the SFIA-Cisco topic map as represented in Ontopia. The centre point represents the starting point of the topic map. From this starting point different instances of competencies branch out.

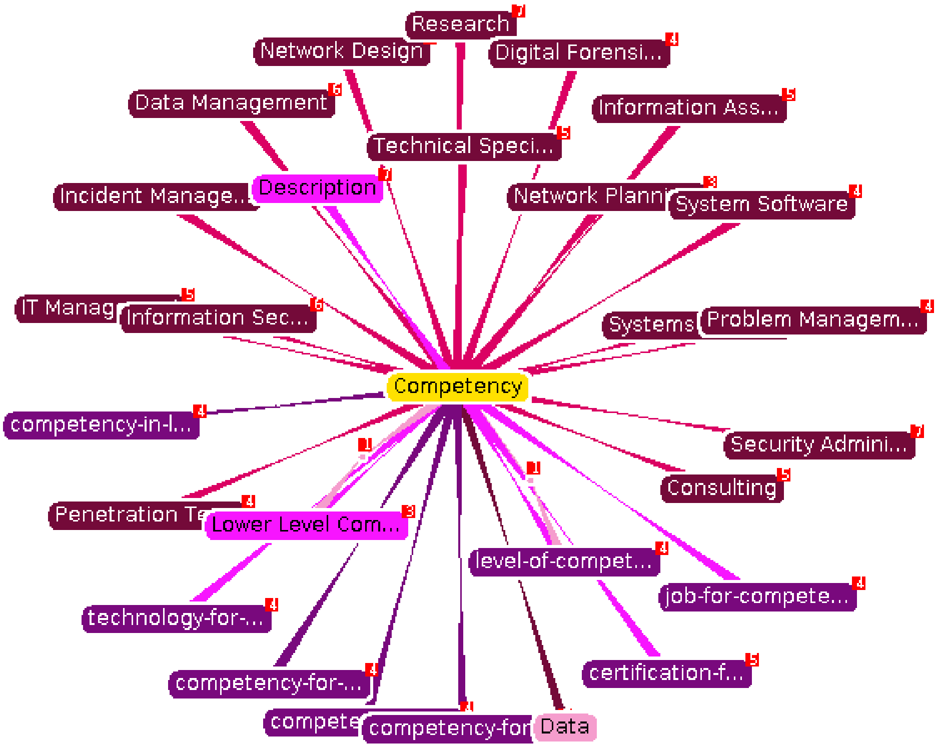


Figure 5.23: Topic Map starting point in Ontopia

Information flow in the topic map can be tracked individually by clicking on any of the connected Topics. Figure 5.24 shows the topic "INCIDENT MANAGEMENT" when it is clicked from the initial starting point. From this point, it expands to other sub-sections. The rectangular shapes represent Topics, while the lines between the shapes represent the association between Topics. In this regard, the topic map operates similarly to a mind map, because it is able to plot information and show how information is related.

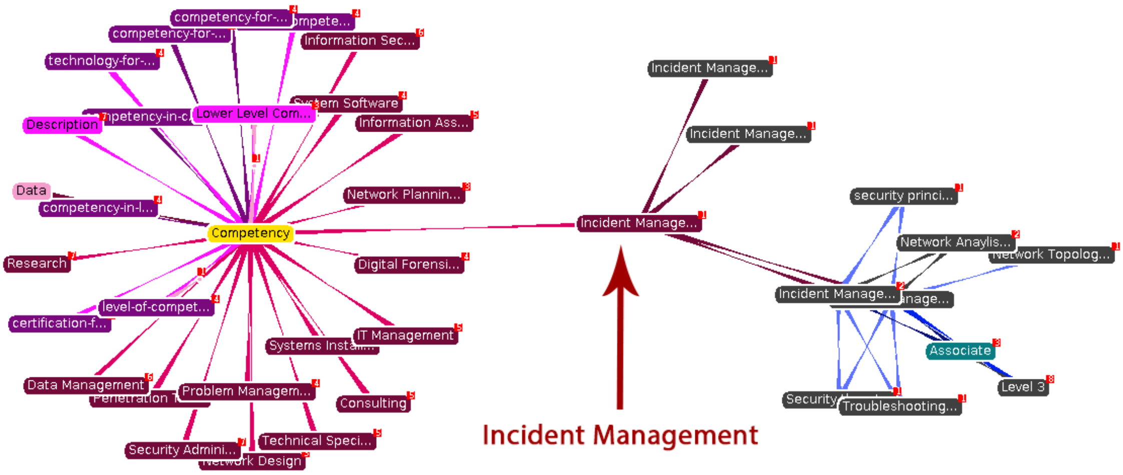


Figure 5.24: Topic Map expanding from starting point in Ontopia

It is also possible to see all the topic nodes in the topic map to get a full picture of all the relationships that are formed in the topology. This is represented in Ontopia through five levels of expansion. The first level of expansion symbolises the initial starting point. Figure 5.23 is an example of a level one expansion scenario. The next level of expansion is actually a node up from all the other Topics on the previous level. Figure 5.24 shows an instance of the topic map with only one node expanded, while a level two expansion would expand every node in the topology to one level up. The last level of expansion shows all the nodes expanded and all the relationships between them, as illustrated in Figure 5.25. In this screenshot, every node from the initial starting point in Figure 5.23 is expanded to create a full picture of a topic map ontology. This depiction of the topic map is based on the design discussed in Section 5.8.2. As such, it is possible to move from one topic relationship to another based on the eight steps discussed in Section 5.8.2.

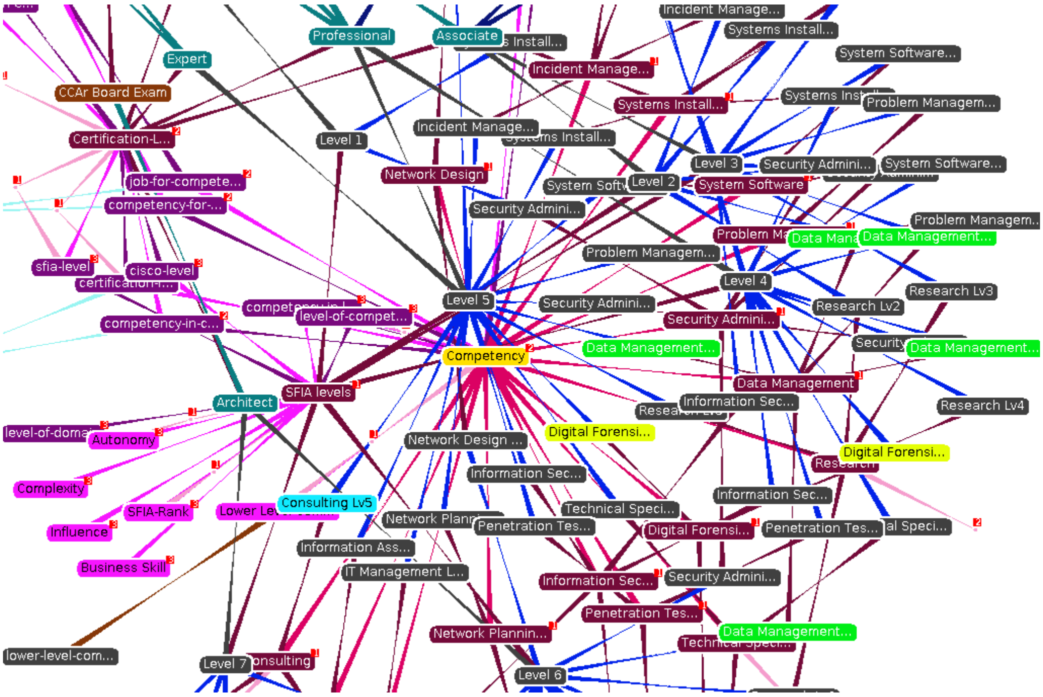


Figure 5.25: Topic Map full expansion in Ontopia

5.8.4 Scope

From the previous image in Figure 5.25, it is apparent that the topic map ontology reaches a state where it is too complex to represent visually in a single view. To solve this problem, the topic map feature ‘Scope’, which was discussed in Section 5.4, can be used to narrow down relationships to specific viewpoints. As such, certain Topics can be included as viewable relationships and others as hidden relationships. This allows the topic map user to create different viewpoints of the ontology by filtering topic types. Figure 5.26 is the BEFORE image, which represents the full ontology of the topic map because it shows all the relationships. Figure 5.27 is the AFTER image. It shows the topic map ontology after the ‘Scope’ feature is applied. This creates a viewpoint of the topic map with some relationships hidden from view. The viewpoint that has been created in Figure 5.27 focuses around the Job role “TEAM MANAGER”, as illustrated by the red arrow. In this viewpoint, all relationships that are connected directly and indirectly to “TEAM MANAGER”, are visible.

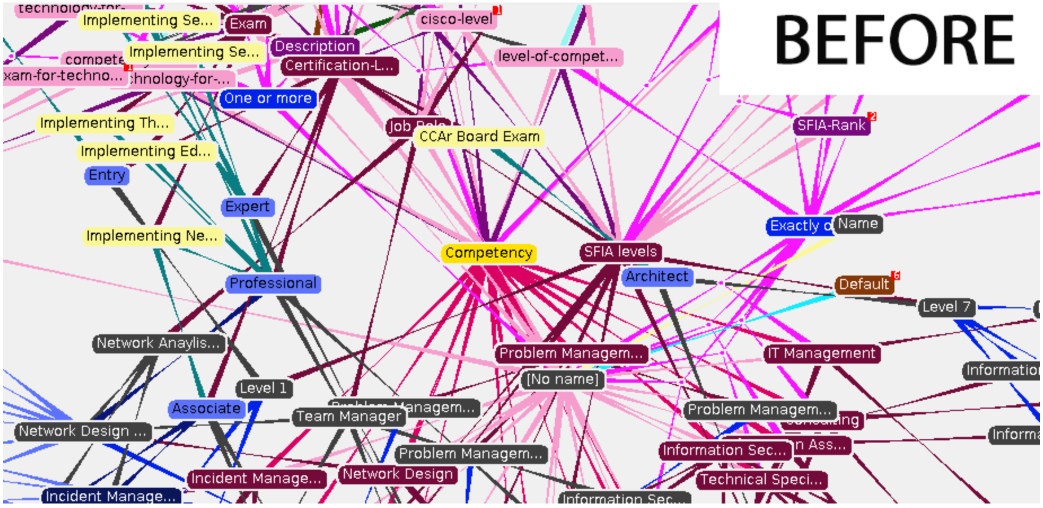


Figure 5.26: Before Scope feature is applied in the topic map

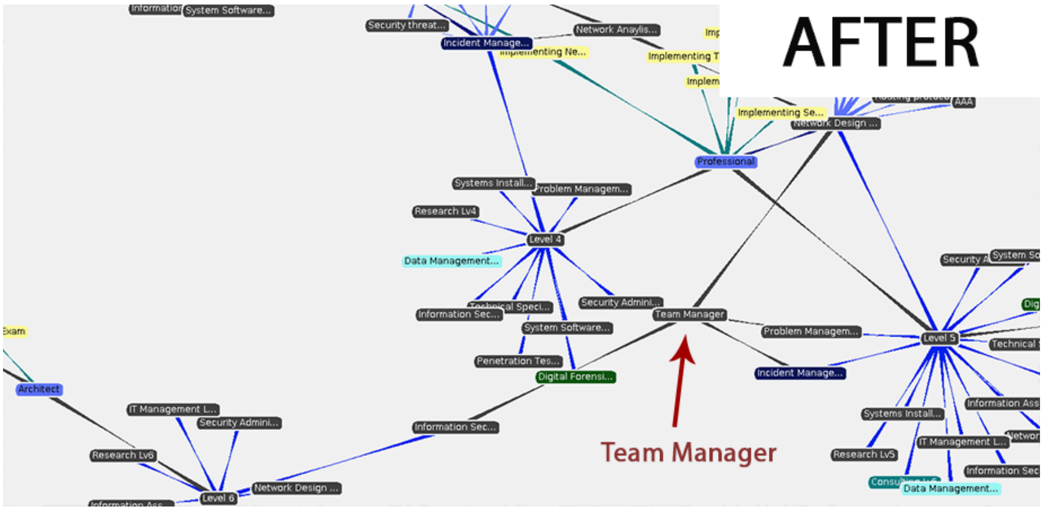


Figure 5.27: After the Scope image is applied and viewpoint is created

5.8.5 Facet

The other way to narrow down the topic map ontology to show only specific relationships is to apply ‘Facets’. Facets are another topic map feature discussed in Section 5.4. Facets allow the topic map to be filtered by querying information about Topics, Associations and Occurrences. As such, Facets can do more than just narrow down information. They are also used to create dynamic relationships between Topics.

Dynamic relationships, which were discussed in Section 5.7.2, are created when users execute a query statement. The advantage of dynamic relationships is that they are not explicitly stated in the topic map like other association types. Instead, dynamic relationships are automatically created only when they are called upon through query statements. All suitable dynamic relationships are described in Section 5.7.2. Figure 5.28 is a query statement that will return results for all technologies that are used in 'Incident Management' at SFIA level 3. This query statement is for the first dynamic relationship, illustrated in Figure 5.11:

```
SELECT $A from

instance-of ($A, technology),

competency-level ($B: competency, $C: sfia-level), competency-
technology ($B: competency, $A: technology),

{located-in ($B: containee, incident-management: container)},

{located-in ($C: containee, level-3: container)}.
```

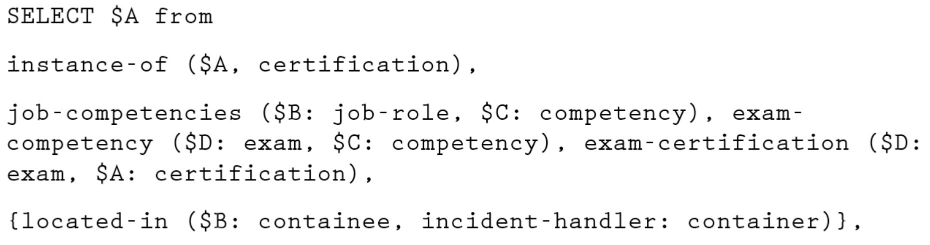
Figure 5.28: Query statement for the first dynamic relationship

The second query statement is illustrated below in Figure 5.29. This query statement returns all exams that are required for the 'Incident Handler' job role. This query statement is for the second dynamic relationship, illustrated in Figure 5.12:

```
SELECT $A from

instance-of ($A, exam),

job-competency ($B: job-role, $C: competency), competency-
certification ($C: competency, $D: certification-level), exam-
certification ($D: certification-level, $A: exam),

{located-in ($B: containee, incident-handler: container)},
```

Figure 5.29: Query statement for the second dynamic relationship

The last query statement is illustrated in Figure 5.30. It returns the certification level that is required for the 'Incident Handler' job role. This query statement is for the third dynamic relationship, illustrated in Figure 5.16:



```
SELECT $A from

instance-of ($A, certification),

job-competencies ($B: job-role, $C: competency), exam-
competency ($D: exam, $C: competency), exam-certification ($D:
exam, $A: certification),

{located-in ($B: containee, incident-handler: container)},
```

Figure 5.30: Query statement for the third dynamic relationship

Part 3: Evaluating the Topic Map

5.9 Demonstrating Topic Map Utility

In accordance with the Design Science process, the applicability of the topic map has been demonstrated through a Proof of Concept. A Proof of Concept is a demonstration, in principle, that a certain concept is feasible and has practical potential. Through a Proof of Concept, it is possible to prove that the topic map can provide value. In this instance, the topic map is demonstrated through the use of competencies in job roles. As discussed in Chapter 3, competencies relate to job roles, because they are used to create job roles. Traditionally, competencies are aggregated to help create job roles. This is a trend that is seen as useful for both competency frameworks and CBL frameworks. In this instance, the topic map will map network security competencies that are typical for CSIRT job positions such as a CSIRT Incident Handler and a CSIRT Team Manager. Furthermore, the topic map will use the facet feature (discussed in Section 5.8.5) to filter between competencies and identify useful relationships between the competencies. This is discussed later in Section 5.10.3. According to McClelland (2007), each job role normally has between five to ten competencies, which are used as a guide when developing the job roles in the topic map.

As pointed out in Chapter 2 Section 2.5 *"A Proof of Concept should state clearly what is to be proven, how it will be proven and to what degree"*.As such, the topic map's usability for job roles will be demonstrated. It will then be evaluated through the use of a Focus Group, which is discussed later in Section 5.10.1. The focus of the demonstration and the evaluation is to prove the utility of the topic map.

5.10 Evaluation Process

Since the topic map is essentially a combination of both competency frameworks and CBL, it has many applications in the CM cycle. The CM cycle was introduced in Section 3.4 as the process of managing how competencies are introduced, integrated and maintained in the organisation. Section 3.4.3 further discussed how the SFIA framework was applicable in the CM cycle. Much like the SFIA framework, the topic map can also be implemented in the CM cycle phases as illustrated in Table 5.3.

Table 5.3: Topic Map application in CM

CM Cycle	**Topic Map use**
Recruitment Succession Planning	Can be used to set criteria for recruitment
Employment Selection	Can be used to assist in decision-making about competency-related activities
Performance Management	Can be used to perform skills gap analysis
Training and Development	Can be used to develop competencies

5.10.1 Focus Group Evaluation

To evaluate the different uses of the topic map, as mentioned above, a Focus Group was used, as described in Section 2.5. The Focus Group consisted of ten participants (excluding the researcher, supervisor and Focus Group facilitator).

The participants were selected based on who the topic map would be most applicable to, or who would benefit the most from using the topic map. As such, the Focus Group consisted of various IT people who worked directly with hiring personnel or who are involved in network security CBL programmes. The objective of this Focus Group was to demonstrate and evaluate the utility of the topic map in a given scenario. Three activities were presented to the participants, who were then asked to study the topic map (both the NICE-Cisco and SFIA-Cisco) alongside the NICE Framework, the SFIA framework and the learning outcomes from the Cisco framework. The participants were then asked to complete each scenario based on the topic map or based on the frameworks. Participants were then given the opportunity to compare the efficiency of the topic map against the frameworks and to comment on the utility of the topic map

5.10.2 Scenario

These scenarios compare the use of competency frameworks and CBL against the topic map. The aim of the scenarios is to test the utility of the topic map by applying it in contexts that would normally use competency frameworks or CBL frameworks.

Scenario 1

Company X has decided to open a new branch in Port Elizabeth. You have been tasked with designing a job description for a CSIRT Incident Handler..

The aim of this activity is to test how the topic map can help to design job positions more easily than the use of competency frameworks alone. Much like competency frameworks, the topic map can also be used to group competencies in order to create job roles. In this instance, participants were given the company's competency needs, along with the NICE Framework and the topic map. They were then asked which instrument was more proficient in designing job roles.

Scenario 2

A candidate has applied for the CSIRT Incident Handler position. Your task now is to evaluate the candidate's level of competency against what is required for the position.

The aim of this activity is to evaluate how well the topic map can be used in a skills gap analysis. A skills gap analysis is the activity of identifying and comparing an individual's competency profile against what is expected of the job position. If there is a gap between what the person has and what is expected, competencies need to be developed to fill this gap. Traditional competency frameworks can only identify competency gaps in the gap analysis. They cannot, however, directly help to develop competencies, but the topic map can both identify and develop them. In this instance, participants were given the candidate's competency profile to compare against the CSIRT Incident Handler job position developed in scenario 1.

Scenario 3

The company has recently opened a new job position for a CSIRT Team Manager. The company decided to open the position to employees first and then to the public. You are tasked with evaluating how to upgrade the current level of competency possessed by employees, so they can meet the job position requirements.

The aim of this activity is to validate that the topic map can provide value for both organisational and personal use. This is because the topic map can be used to identify competencies for job positions (organisational use) and also to help individuals understand what competencies they need to develop and how they can develop them if they want higher job positions (personal use). This would prove that the topic map can produce value for both CM and CBL. In this instance, participants were given the topic map and a competency profile for an employee.

5.10.3 Topic Map and Decision Making

Traditionally, competency frameworks are used as reference guides to help organisations implement competency effectively. However, they are limited in this capacity because they can only identify competencies and do not directly contribute to informed decision-making. Unlike competency frameworks, the topic map can contribute directly to decision-making. This is because the topic map is able to create relationships between competencies that may not have been realised without the mapping. The creation of relationships is accomplished through the use of facets, which act as query machines. Facets create temporal relationships between competencies in the topic map, thus allowing the user to abstract specific information about any competency as it relates to other competencies. In the Focus Group, participants were shown how the topic map could be used as a supportive decision-making tool. This was accomplished by executing the query statements illustrated in Section 5.8.5.

5.10.4 Findings and Suggestions

The results gathered from the participants indicated that they all agreed that the topic map provided better utility in assessing network security competencies than traditional tools. Feedback indicated that the topic map's ability to map high-level competencies with low-level task-oriented competencies was useful in recruiting candidates for job roles and for performing a skills gap analysis. Further feedback indicated that the topic map was useful for organisational use and also for helping candidates pursue future competencies for job roles. Some of the responses from the Focus Group members are as follows:

- "The NICE Framework is very bulky and not easy to pin down specific competencies for job descriptions, while the topic map does make an easier means for selecting task-oriented competencies provided that the Associations where properly mapped together"

- "I agree that the topic map provides better value, provided that the competencies were selected properly for the job role"

- "Employees could use the topic map to evaluate their competencies against what is required for job roles"

- "I also strongly agree that the topic map mapping features make it better for job descriptions, because of a number of details it can provide for low-level job descriptions and still also provide higher job descriptions at the same time"

Some members expressed the opinion that their own initial views on the utility of the topic map were less favourable, but that they changed their views after the Focus Group discussions. This could indicate a need for more clarity in the instructions on how the topic map should be used.

Thus, from the feedback gathered from the Focus Group, it is concluded that all the participants agreed that the use of topic maps for assessing network security competencies is a useful concept that has the potential for providing value as a CM tool.

5.11 Conclusion

This chapter focused on the development of topic maps as the solution for mapping competencies in network security. The chapter was separated into three parts. The first part dealt with understanding the components and features of a topic map. The second part of the chapter discussed how the topic map was constructed in this research. The construction of the topic map was based on the Design Science process. In accordance with the paradigm, the construction process was divided into the five steps discussed in Chapter 2. These five steps correlate with the research objectives discussed in Chapter 1. The third part of this chapter addressed the demonstration and evaluation of the topic map. The topic map was demonstrated through a Proof of Concept to prove that the topic map could be used within the context of representing occupational competencies for job roles in network security. The evaluation of the topic map's utility was conducted through a Focus Group. The results of the Focus Group indicated that all the participants agreed that the topic map provided value in assessing competencies, more so than traditional methods of assessing competencies. As such, this chapter demonstrated the validity of introducing topic maps as a solution to mapping competencies

Chapter 6

Conclusion

6.1 Introduction

The aim of this study was to develop a topic map that could represent network security competencies holistically. The study identified an opportunity for mapping high-level competencies with lower-level competencies. The topic map itself sought to provide an alternative method of assessing occupational competencies, which could then be integrated into the CM process. Furthermore, the study outlined that Design Science research was adopted as the research paradigm and highlighted the philosophical stance and methodological approach that were followed in order to develop and evaluate the topic map.

This concluding chapter provides an overview of the research questions and objectives, and a subsequent summary of the findings and contributions in relation to the research thesis statement discussed in Chapter 1. As such, this chapter will start by providing a summary of the previous chapters, and will then follow with a description of how the research has solved the problem. A summary of the contributions and the limitations of the research will subsequently follow.

6.2 Solving the Problem

The problem that was addressed through this research study was the lack of competency frameworks or CBL programmes that could holistically represent network security competencies. To address this problem, the primary research objective was to *"design a topic map that can holistically represent network security competencies"*. In order to achieve this primary research objective, a number of secondary research objectives were defined. The remainder of this section will address these secondary objectives.

Research Objective: *Identify suitable competency frameworks and CBL for the topic map.*

The identification of suitable competency frameworks and CBL for mapping was important, because it was the first step to fully expressing a holistic mapping of competencies. In this capacity, the competency framework represented high-level competencies, while CBL represented low-level, task oriented competencies. The selection process was based on selecting frameworks that would lead to the simplest way of expressing the desired holistic mapping. As such, it was important to select competency frameworks and CBL that were easily integratable and that also aligned well with one another.

Furthermore, it was also decided that only a single competency framework and a single CBL programme would be mapped at a time. This generated different instances of the topic map, based on different combinations of competency frameworks and CBL. There were two main reasons for this decision:

1. Different frameworks had different ways of representing competencies, so it would lead to conflict if more than one competency framework or CBL framework was used at a time

2. All the considered frameworks had their own strengths and weaknesses that influenced the decision about which frameworks to use.

Due to these two reasons, two instances of the topic map were mapped. The first instance was a combination of the SFIA competency framework and the Cisco CBL framework.

SFIA was selected because it was the most widely used competency framework in ICT and it could represent competencies from multiple levels. The use of SFIA allowed even a single competence to be appreciated from multiple perspectives. However, the drawback to using SFIA was that the framework covered very few competencies directly linked to network security. The second instance was a combination of the NICE competency framework and the Cisco CBL framework. The NICE Framework was selected because it possessed the most descriptive competencies relevant to network security. As such, it allowed for a simple way of integrating high-level and low-level competencies in network security. However, the drawback to this framework was the fact that it could not represent competencies at multiple levels like SFIA. In both instances of the topic map, the Cisco CBL framework was used. This is because Cisco's CBL programme represented low-level, task-oriented competencies for network security much better than other CBL programmes.

Research Objective: *Determine a suitable methodology for the construction of the topic map.*

The second objective related to the manner in which the topic map was constructed. It was important to decide on a methodology that was design-oriented. Hence, Design Science was selected as the research paradigm. The Design Science approach focused on designing and evaluating artefacts that contributed to both solving an organisational problem and communicating knowledge about the design to Research. As a result, the research produced a topic map that was applicable to assessing occupational competencies in CM and it was also able to communicate knowledge about the design of the artefact. This research study followed the Design Science process as outlined in Section 2.4. As such, the topic map was designed according to the 'Design and Development Phase' of the Design Science process. It was then demonstrated through a Proof of Concept in accordance with the 'Demonstration Phase' of the Design Science process and, finally, it was evaluated by a Focus Group in the 'Evaluation Phase' of the Design Science process. Furthermore, the research study was able to adhere to the seven Design Science guidelines expressed in Table 6.1.

Table 6.1: Design Science Guidelines as applied in the research study

Guideline	**Research relevance**
Design Science research must produce a feasible artefact in the form of a construct, a model, a method, or an instantiation.	The artefact that will be produced by this research is a model in the form of a topic map. Topic maps provide a practical way of mapping IS concepts.
The objective of Design Science research is to develop technology-based solutions to important and relevant business problems.	This research focuses on attempting to solve an organisational problem as discussed in Chapter 1 Section 1.3, by using an IS tool, which is the topic map. As such, this research adheres to this guideline.
It is necessary to demonstrate the utility, quality and efficiency of a design artefact through rigorous, well-executed evaluation methods.	The topic map is rigorously evaluated through a well-defined research method in the form of a Focus Group. The context of the Focus Group is introduced in Section 2.5 and the results are reported in Section 5.10.1.
Effective Design Science research must provide clear and verifiable contributions in the areas of the design artefact, design foundations, and/or design methodologies.	The knowledge contribution of this research study is the topic map and the method in which the topic map is developed. The topic map itself contributes knowledge of how to holistically represent network security competencies, while the method of developing the topic map contributes knowledge of how to map high-level frameworks (competency frameworks) and low-level (CBL frameworks) together.
Design Science research relies upon the application of rigorous methods in both the construction and evaluation of the design artefact.	Research rigour is obtained through following the prescribed Design Science research process introduced in Section 2.4 and applying sound research methods as discussed in Section 2.5.
The search for an effective artefact requires the use of available means reach desired ends while satisfying laws in the problem environment.	This research study followed the Research Methodology described in this section of the dissertation. The Research Methodology describes the methods used to construct a solution for the problem described in the problem statement.
Design Science research must be presented effectively both to technology-oriented as well as management-oriented audiences.	The communication is done through this dissertation.

Research Objective: *Verify the proposed topic map through demonstration of its application.*

The last research objective relates to the verification of the research study. This verification was conducted through a demonstration and evaluation of the topic map.

Demonstration: The significance of the topic map was demonstrated through a Proof of Concept. This meant that the topic map was placed in a situational context to prove that the topic map could be used within the context of representing occupational competencies for job roles in network security. As such, the topic map was able to map network security competencies that are typical for CSIRT job positions such as Incident Handler and Team Manager. Furthermore, the topic map was demonstrated through Facets, which were used to identify useful relationships between competencies for job roles.

Evaluation: The utility of the topic map was then evaluated through a Focus Group. This formed part of the 'Evaluation Phase' of the Design Science process. In the Focus Group, ten participants were given a situational scenarios, where the topic map was compared against traditional methods of assessing competencies. The results of the Focus Group indicated that all the participants agreed that the topic map provided value in assessing competencies, more so than traditional methods of assessing competencies.

6.3 Summary of Contribution

Design Science research requires two contributions, the first contribution is in the form of the artefact and the second contribution is in the form of knowledge on how to design the artefact. These are summarised briefly below:

1. The first contribution is in the form of the network security topic map, which is demonstrated through a business scenario. The topic map can be used in CM to represent high-level and low-level, task-oriented competencies. As such, it provides value both for organisational assessment of competencies and for training competencies.

2. The second contribution is in the mapping of high-level with low-level competencies. This second contribution is particularly important, because it emphasises the mapping and not the topic map itself. Literature from the Problem Area in Chapter 1 indicates that there is a need for this mapping and this research study was able to produce a comprehensive method of mapping competencies. As such, this research focuses on mapping competencies with the use of a technology, namely the Topic Map Standard. However, it is also possible to achieve the mapping whilst using other technology such as the Resource Description Framework (RDF), which also provides mapping very similar to the Topic Map Standard.

These two contributions fall within different quadrants of the *'Knowledge contribution model'* discussed in Section 2.3.2. The first contribution fits into the *'Improvement'* quadrant, because the research introduces an improved way of assessing competencies through the use of a topic map. The second contribution, however, fits into the *'Exaptation'* quadrant, because the research adopts the topic map technology, which is normally used in web development and uses the technology in a new context. This is expressed in Figure 6.1, which illustrates all four quadrants in the *'Knowledge contribution model'*.

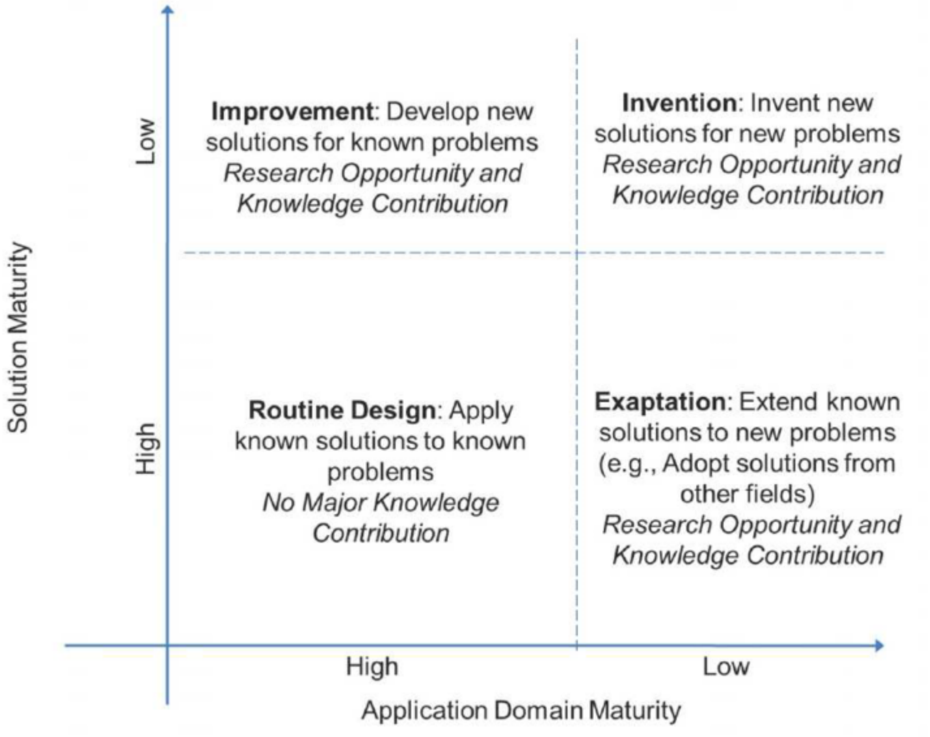

Improvement: Develop new solutions for known problems
Research Opportunity and Knowledge Contribution
Invention: Invent new solutions for new problems
Research Opportunity and Knowledge Contribution
Routine Design: Apply known solutions to known problems
No Major Knowledge Contribution
Exaptation: Extend known solutions to new problems (e.g., Adopt solutions from other fields)
Research Opportunity and Knowledge Contribution
Solution Maturity
Low
High
High
Low
Application Domain Maturity

Figure 6.1: Knowledge contribution framework (Hevner and Chatterjee, 2012)

The other contribution of the study is the documentation. This documentation could prove useful to other researchers conducting research into topic maps. Currently, there are very few resources available online that comprehensively describe how to create topic maps.

6.4 Limitations of Research

This research project faced a number of challenges and obstacles that limited the research. These limitations are largely related to technology, but some relate to competencies:

- The first limitation relates to the tools that were used to express the topic map in Section 5.8.3. The software applications for topic maps are traditionally aimed at software developers. As such, most of the available online platforms are developer engines and are not user-ready.

- The second limitation relates to the topic map applications (Ontopia and TMnav) used in the research. As stated above, there were very few user-ready applications to choose from and the applications that were available, were open source and had inadequate support. It was very difficult to install the applications, because installation documentation was unclear. A lot of the hyperlinks for downloading topic map applications were broken. Furthermore, there were lots of software bugs and errors that could not be reported. As such, the researcher had to work around a lot of these issues, which ultimately affected the topic map's utility.

- The third limitation relates to support for topic maps online. There has been a drastic decrease in support and documentation for topic maps because the main topic map pioneers ventured into other projects. This has left a hole in the topic map industry. As of 6 November 2017 the Ontopia website (www.ontopia.net) has gone offline. This was one of the main websites for topic map information. Many other researchers have also voiced their disappointment about this issue. It is believed that a lack of leadership and funding has led to this decrease in development in the topic map industry, but it is also believed that the topic map technology itself is, in fact, useful (Strehle, 2015).

- The fourth limitation relates to the mapping of competencies. A major challenge was faced in mapping higher up organisational competencies, because they were more related to business contexts and showed less technology emphasis when compared to lower down organisational competencies. This made it difficult to describe job roles for top management positions. Furthermore, it was also difficult to map competencies related to attitude or the Affective Domain. A lot of the competencies mapped in the topic map relate to cognitive knowledge or the Psychomotor Domain, but little information is given in relation to the Affective Domain.

Although these limitations affected the research, they did not curtail the direction of the research. In the end, the research objective was still achieved in spite of these limitations.

6.5 Publications from Research

This research study has produced a number of research submissions, which are listed below. The full text for each of the articles is included in appendix A.

Published papers *Assessing the Effectiveness of the Cisco Networking Academy Program in Developing Countries.*

This paper demonstrated the conceptual connection between the NICE Framework and the Cisco network security CBL programme used in Higher Education Institutions courses. It focused on assessing the Cisco Network Academy as an effective blended learning programme through the use of competencies in Higher Education.

Submitted, but not published

1. *Towards an integrated skills competency framework for CSIRT personnel*

   This paper proposed the integration of high-level competencies with low-level task-oriented competencies for assessing CSIRT competencies.

2. *Topic Map for Network Security Competencies*

   This paper is a revision of the previous paper, it proposes the use of a topic map for integrating competencies in competency frameworks with competencies in CBL programmes.

6.6 Future Research

This research study focused on demonstrating that topic maps could be used to represent competencies in network security. Further research can go beyond demonstrating the concept and can focus on the application of the topic map in further detail. The topic map also has the potential to develop from a Proof of Concept into a full application that can be used by organisations.

Furthermore, the topic map is capable of mapping competencies beyond just network security. Other ICT disciplines such as communication networks and information security can benefit from the mapping of competencies

Higher Education presents another opportunity for demonstrating the utility of the topic map. Currently, higher education institutions are integrating occupational competencies into their curriculum. Institutions such as the Nelson Mandela Metropolitan University and the Open University are using content from CBL programmes such as the Cisco certification programme (Yekela, Thomson, & Niekerk, 2017; Smith & Moss, 2010), while other institutions, such as Curtin University of Technology, are mapping competency frameworks, such as SFIA, as part of their curriculum (Von Konsky, 2008).

In this research, the mapping of high-level and low-level competencies was achieved with the topic map technology and standard. However, there are other technologies, such as RDF technology, that can also produce the same mapping abilities as the topic map (RDF Working Group, 2014; Garshol, 2007). Research into other technologies for mapping could produce a better and more capable artefact.

Topic Maps and Network Science

The second contribution of this research was the method of mapping competencies. This method can be developed further through the application of Network Science. Network Science is the extensive study of the behavioural properties of network topologies, which includes complex networks. A network in this capacity is described as a set of items, called vertexes, with connections between them, called edges (Barabási, 2013). This is illustrated in Figure 6.2. Network Science seeks to understand the relationship between the vertexes. The analysis of network properties can lead to new knowledge that may not have been realised without an understanding of the relationship between network components (Barabási, 2013). Criminology was able to use Network Science in successfully mapping ISIS and 911 attacks (Zhang, 2017). Epidemiology was able to use Network Science to improve the deployment of vaccines so that the spread of Tuberculosis could be contained effectively (Cook et al., 2007). In Sociology Network Science was used by Facebook to suggest friend requests and place advertisements (Boccaletti, Latora, Moreno, Chavez, & Hwang, 2006).

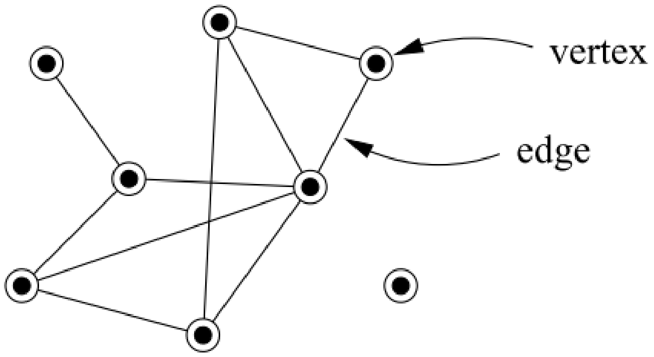


Figure 6.2: Network topology as expressed in Network Science (Barabsi, 2013)

As such, Network Science can be used as a method for understanding the relationships between competencies in the topic map. A topic map is technically also described as a conceptual network. Therefore, topic maps can work together well with Network Science to help understand and express network topologies better. Figure 6.3 is a screenshot adapted from the SFIA-NICE topic map. This image shows the complex relationship between competencies in the topic map. These competencies and their associations can be expressed as a network topology, with the competencies representing *'vertexes'* and the associations representing *'edges'*. The Network Science principles can be used to understand and report on the relationships shown in Figure 6.3.

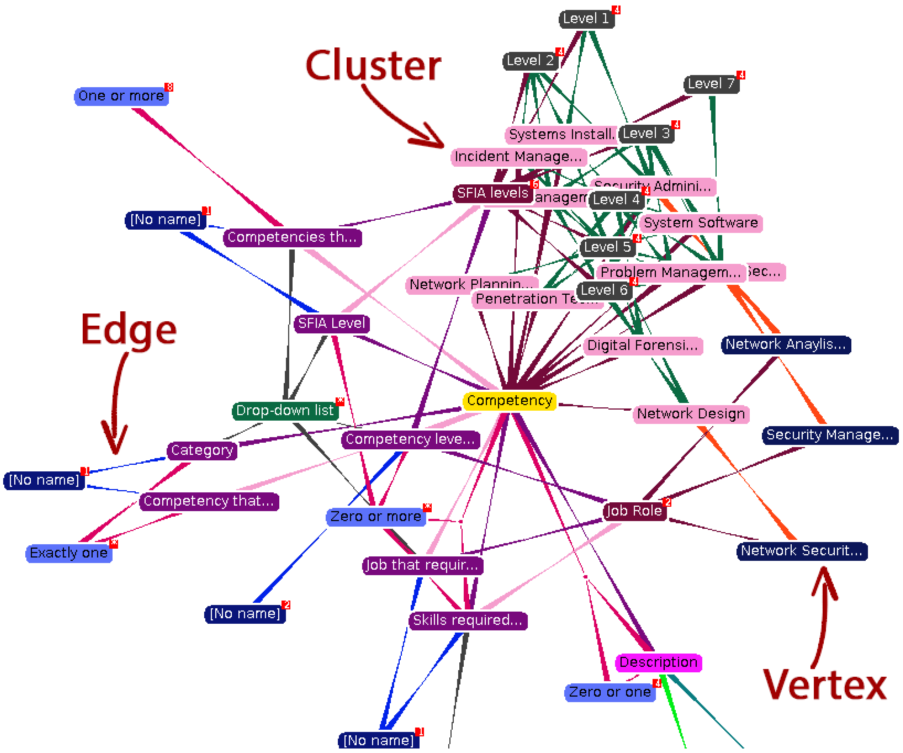


Figure 6.3: Topic map expressed as a Network Science network topology

The integration of Network Science with topic maps would be a new development that has not yet been published. As such, it would be a new contribution in the research space.

6.7 Conclusion

Topic maps are a useful technology for representing network security competencies. They can be used as a CM tool for assessing occupational competencies. This research was able to map high-level competencies with low-level, task-oriented competencies through the use of topic map technology. Further research into different methods of mapping competencies may lead to new research

References

Warren, R., & Edwards-adrian, S. *Talent Management: A holistic approach to managing your workforce.* Los Angeles.

Adnan, M., Just, M., Baillie, L., Gunes, H., Adnan, M., Just, M., & Baillie, L. (2015). Investigating the work practices of network security professionals. *Information & Computer Security*, *23*(3), 347–367.

Ahmad, R., Sahib, S., & Nor'Azuwa, M. P. (2014). Effective measurement requirements for network security management. *International Journal of Computer Science and Information Security*, *12*(April 2014), 1–8.

Ahmed, K., & Moore, G. (2005). An Introduction to Topic Models. *The Architecture Journal*(July), 1–12.

Al-rawi, A., Lansari, A., & Bouslama, F. (2006). Integrating IT Certifications in Networking Courses : Cisco CCNA Versus CompTIA Network +. (August 2000), 11–24.

ASIS. (2017). *Standards and Guidelines.* `https://www.asisonline.org/Standards-Guidelines/Standards/Pages/default.aspx`. ([Online; accessed 2017-08-30])

Barabási, A.-l. (2013). *Network science.*

Beyond Security. (2016). *NERC-CIP Network Security Requirements.* `https://www.beyondsecurity.com/vulnerability{\_}assessment{\_}requirements{\_}nerc-cip.html`. ([Online; accessed 2017-09-15])

Boccaletti, S., Latora, V., Moreno, Y., Chavez, M., & Hwang, D. U. (2006). Complex networks: Structure and dynamics. *Physics Reports*, *424*(4-5), 175–308.

Boyatzis, R. E. (2008). Competencies in the 21st century. *Journal of Management Development*, *27*(1), 5–12.

CIPD. (2004). *Recruitment, retention and turnover.* www.cipd.co.uk/NR/rdonlyres/E6FB179B-8ADB-4C68-ABBB-B03F00A57B48/0/2983recruitretnsurvey04.pdf.

CIS. (2017). *CIS Controls.* https://www.cisecurity.org/controls/. ([Online; accessed 2017-09-19])

Cisco Systems. (2010a). *Cisco NERC CIP v5 Compliance Solutions* (Tech. Rep.). San Jose, CA: Cisco Systems.

Cisco Systems. (2010b). *What is Network Security?* https://www.cisco.com/c/en/us/products/security/what-is-network-security.html. ([Online; accessed 2017-09-18])

Cisco Systems. (2015). *Cisco Security Certifications* (Tech. Rep.). Cisco Learning.

Cisco Systems. (2017). *Training & Certifications.* https://www.cisco.com/c/en/us/training-events/training-certifications/certifications.html. ([Online; accessed 2017-09-23])

Clark, D. (2015a). *Bloom's Taxonom Affective Domain.* http://www.nwlink.com/{~}donclark/hrd/Bloom/affective{_}domain.html. ([Online; accessed 2017-10-10])

Clark, D. (2015b). *Bloom's Taxonom Psychomotor Domain.* http://www.nwlink.com/{~}donclark/hrd/Bloom/psychomotor{_}domain.html. ([Online; accessed 2017-10-10])

Coertze, J. J. (2013). A FRAMEWORK FOR INFORMATION SECURITY GOVERNANCE IN SMMEs.

Collin, A. (1989). Managers' Competence: Rhetoric, Reality and Research. *Personnel Review*, *18*(6), 20–25.

Cook, V. J., Sun, S. J., Tapia, J., Muth, S. Q., Argüello, D. F., Lewis, B. L., Rothenberg, R. B., & McElroy, P. D. (2007). Transmission

Network Analysis in Tuberculosis Contact Investigations. *The Journal of Infectious Diseases*, *196*(10), 1517–1527.

CPP. (2017). *What is the Talent Management Life Cycle?* `http://www.cppblogcentral.com/cpp-connect/what-is-the-talent-management-life-cycle/`. ([Online; accessed 2017-09-08])

Cronin, P., Ryan, F., & Coughlan, M. (2008). *Undertaking a literature review: A step-by-step approach.*

Draganidis, F., & Mentzas, G. (2006). Competency based management: a review of systems and approaches. *Information Management & Computer Security*, *14*(1), 51–64.

Dubois, D. D. (1993). *Competency-based Performance Improvement: A Strategy for Organizational Change.* HRD Press.

ENISA. (2006). *A step-by-step approach on how to set up a CSIRT.* `https://www.enisa.europa.eu/publications/csirt-setting-up-guide/at{\_}download/fullReport`.

European Committee for Standardization. (2014). *User guide for the application of the European e-Competence Framework 3.0* (Tech. Rep.). European Committee for Standardization.

Fallis, A. (2013). No Title No Title. *Journal of Chemical Information and Modeling*, *53*(9), 1689–1699.

Feisel, L., D. Peterson, G., & Emeritus, D. (2002). A Colloquy on Learning Objectives For Engineering Education Laboratories.

Frankl, M. (2016). *UVic Learning and Teaching Centre (LTC) August 2016 PROGRAM COMPETENCIES VS . LEARNING OUTCOMES* (Tech. Rep. No. August). University Canada West.

Garshol, L. M. (2007). *Comparing Topic Maps and RDF.* `http://www.garshol.priv.no/blog/92.html`. ([Online; accessed 2017-11-02])

Grant, S. (2006). Frameworks of competence: common or specific? *Proceedings of International Workshop in Learning Networks for Lifelong Competence Development March 3031 Sofia Bulgaria*, 111–116.

Gregor, S., & Hevner, A. R. (2013). POSITIONING AND PRESENTING DESIGN SCIENCE Types of Knowledge in Design Science Research. *MIS Quarterly*, *37*(2), 337–355.

H. Randall, M., & Zirkle, C. (2005). Information Technology Student-Based Certification in Formal Education Settings:Who Benefits and What is Needed. *JITE*, *4*, 287–306.

Hatzigaidas, A., Papastergiou, A., Tryfon, G., & Maritsa, D. (2004). TOPIC MAP EXISTING TOOLS : A BRIEF REVIEW by. In *International conference on theory and applications of mathematics and informatics - ictami 2004,* (pp. 185–201). Thessaloniki, Greece TOPIC.

Hevner, A. R. (2007). A Three Cycle View of Design Science Research. *Scandinavian Journal of Information Systems*, *19*(2), 87–92.

Hevner, A. R., & Chatterjee, S. (2012). *Integrated Series in Information Systems Volume 28* (Vol. 28). Spring Street, New York, NY 10013, USA: Springer Science+Business Media.

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design Science in Information Systems Research. *Design Science in IS Research MIS Quarterly*, *28*(1), 75–105.

Homer, M. (2001). Skills and competency management. *Industrial and Commercial Training*, *33*, 59–62.

Howell, W., & Fleishman, E. (1982). *Human Performance and Productivity* (Vol 2 ed.). Hillsdale, NJ: Erlbaum.

HR-XML. (2004). *Competencies (Measurable Characteristics).* `http://www.ec.tuwien.ac.at/{~}dorn/Courses/KM/Resources/hrxml/HR-XML-2{\_}3/CPO/Competencies.html`.

IITPSA. (2017). *Professional Practice Sector Headlines by ITWEB* (No. October). `https://www.iitpsa.org.za/professional-practice/`. ([Online; accessed 2017-09-09])

Iles, P. (2001). *Employee resourcing.*

ISACA. (2017). *DS5.10 - Network Security.* `https://www.isaca.org/Groups/Professional-English/ds5-10-network-security/Pages/Overview.aspx`. ([Online; accessed 2017-09-18])

ISO. (2010). *ISO/IEC 27033:2017 Information technology Security techniques Network security* (2017 ed.).

Jackson, S. E., & Schuler, R. S. (2003). *Managing Human Resources Through Strategic Partnerships.* Thomson/South-Western.

Killcrece, G., Kossakowski, K.-P., Ruefle, R., & Zajicek, M. (2003). Organizational Models for Computer Security Incident Response Teams (CSIRTs). (December).

Klimburg, A. (2012). *National Cyber Security Framework Manual.* Tallinn, Estonia: NATO CCD COE Publication.

Konsky, B. R. V., & Miller, C. (2013). Embedding Professional Skills in the ICT Curriculum. In *30th ascilite conference* (pp. 883–887).

L. Cardy, R., & Selvarajan, T. T. (2006). Competencies: Alternative frameworks for competitive advantage. *Business Horizons*, *49*, 235–245.

Lammle, T. (2013). *CCNA Routing and Switching Study Guild* (3 ed.). John Wiley Sons.

Lawler, E. E. (1994). From job-based to competency-based organizations. *Journal of Organizational Behavior*, *15*(1), 3–15.

Le Deist, F. D., & Winterton, J. (2005). What Is Competence? *Human Resource Development International*, *8*(1), 27–46.

M. Jr. Spencer, L., & M. Spencer, S. (2008). Competence at Work: Models for Superior Performance.

March, S. T., & Smith, G. F. (1995). Design and natural science research on information technology. *Decision Support Systems*, *15*(4), 251–266.

Markowitsch, J., & Plaimauer, C. (2009). Descriptors for competence: towards an international standard classification for skills and competences. *Journal of European Industrial Training*, *33*(8/9), 817–837.

Marrelli, A. F. (1998). An introduction to competency analysis and modeling. *Performance Improvement*, *37*(5), 8–17.

Mcclelland, D. (2007). *Introduction to Competencies.* `http://www.nwlink.com/{~}donclark/hrd/case/compet1.html`. ([Online; accessed 2017-06-24])

Meyer, T. (1996). *Creating competitiveness through competencies: Currency for the 21 st century.* Johannesburg, South Africa: Sigma press.

Montante, R., & Khan, Z. (2001). Specialized Certification Programs in Computer Science. In *Proceedings of the thirty-second sigcse technical symposium on computer science education* (pp. 371–375). New York, NY, USA: ACM.

National Institute of Science and Technology. (2013). *The National Cybersecurity Workforce Framework* (Tech. Rep.).

NERC. (2016). *CIP Standards* (No. 5). `http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx`. ([Online; accessed 2017-10-02])

NIST. (2017). *NIST SPECIAL PUBLICATIONS (SP)* (No. June). `http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-192.pdf`. ([Online; accessed 2017-08-28])

Oates, B. J. (2006). *Researching Information Systems and Computing.* SAGE Publications.

Olivier, M. S. (2013). *Information Technology Research: A practical guide for computer science and informatics* (Vol. 53, 3 ed.). 1064 Arcadia Street, Hatfield, Pretoria: Van Schaik Publishers.

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A Design Science Research Methodology for Information Systems Research. *Journal of Management Information Systems*, *24*(3), 45–78.

Pepper, S. (2013). *The TAO of Topic Maps Finding.* `http://www.ontopia.net/topicmaps/materials/tao.html`. ([Online; accessed 2016-04-15])

Plessius, H., & Ravesteyn, P. (2016). Mapping the European e-Competence Framework on the domain of Information Technology : a comparative 1 Introduction 2 Theoretical Background. In *29th bled econference digital economy* (pp. 459–471). Bled, Slovenia.

Purao, S. (2002). Design research in the technology of information systems: Truth or dare. *Pennsylvania State University*(April).

RDF Working Group. (2014). *Resource Description Framework (RDF).* `http://www.w3.org/standards/techs/rdf`. ([Online; accessed 2017-11-10])

Reza, S., & Javadein, S. (2013). Human Resource Manager Selection Based on Logarithmic Fuzzy Preference Programming and TOPSIS Methods. *International Journal of Human Resource Studies*, *3*(2), 14–27.

Rodriguez, D., Patel, R., Bright, A., Gregory, D., & Gowing, M. K. (2002). Developing competency models to promote integrated human resource practices. *Human Resource Management*, *41*(3), 309–324.

Rudzajs, P., Penicina, L., Kirikova, M., & Strazdina, R. (2010). Towards Narrowing a Conceptual Gap between IT Industry and University. *Scientific Journal of Riga Technical University. Computer Sciences*, *41*(1), 9–16.

SANS. (2015). Critical Security Controls v6.0. 1–2.

Schofield, A. (2014). *2014 JCSE ICT Skills Survey* (Tech. Rep.).

Selmer, J., & Chiu, R. (2004). Required human resources competencies in the future: a framework for developing HR executives in Hong Kong. *Journal of World Business*, *39*(4), 324–336.

SFIA Foundation. (2015). *SFIA6 The complete reference guide.* `https://www.sfia-online.org/`.

Sienkiewicz, Ł. e. (2014). Competency-based human resources management The lifelong learning perspective. *Educational Research Institute.*

Slavin, R. E. (1996). Research on cooperative learning and achievement what we know, what we need to know. *Contemporary Educational Psychology*, *21*, 43–69.

Smith, A., & Moss, N. (2010). Large Scale Delivery of Cisco Networking Academy Program by Blended Distance Learning.

SouthAfrica.info. (2016). *ICT 'key to African growth, development' South* (No. August). `http://www.southafrica.info`. ([Online; accessed 2016-06-10])

Stallings, W. (2006). *Standards for Information Security Management.* `https://www.cisco.com/c/en/us/about/press/internet-protocol-journal/back-issues/table-contents-38/104-standards.html`. ([Online; accessed 2017-09-20])

Stewart, D. W., & Shamdasani, P. N. (1990). *Focus groups: theory and practice.* Sage Publications.

Strehle, T. (2015). *Topic Maps (as a standard) are dead.* `https://www.strehle.de/tim/weblog/`. ([Online; accessed 2017-10-20])

Szasz, P., Louridas, M., Harris, K. A., & Grantcharov, T. P. (2016). Strategies for increasing the feasibility of performance assessments during competency-based education : subjective and objective evaluations correlate in the operating room. *The American Journal of Surgery*(2016), 1–8.

Tate, W. (1995). *Developing Managerial Competence: A Critical Guide to Methods and Materials.* Gower.

Telha, A., Rodrigues, A., Páscoa, C., & Tribolet, J. (2016). The competency architecture as error limiting element and efficiency enhancer in business processes. *Procedia Computer Science Ana Telha et al. Procedia Computer Science*, *100*(100), 665–670.

Trinder, J. C. (2008). Competency Standards - a Measure of the Quality of a Workforce. In *The international archives of the photogrammetry, remote sensing and spatial information sciences. . beijing 2008* (Vol. Vol. XXXVI, p. 165). Beijing, China.

U.S. OPM. (2017a). *Information Technology (IT) Management Series 2210 (Alternative A).* `https://www.opm.gov/policy-data-oversight/classification-qualifications/general-schedule-qualification-standards/2200/information-technology-it-management-series-2210-alternative-a/`. ([Online; accessed 2017-09-10])

U.S. OPM. (2017b). *OPM ' s MOSAIC Studies and Competencies.* `https://www.opm.gov/policy-data-oversight/assessment-and-selection/competencies/`. ([Online; accessed 2017-09-10])

Von Konsky, B. R. (2008). Defining the ICT profession: A partnership of stakeholders. *Proceedings of the 21st Annual Conference of the National Advisory Committee on Computing Qualifications*, 15–22.

Wahba, M. (2012). *Competence Standards for Technical and Vocational Education and Training TVET* (Tech. Rep.).

Woodruffe, C. (1992). What is meant by competency? In R. Boam & P. Sparrow (Eds.), *Designing and achieving competency.* New York.

Yekela, O., Thomson, K.-L., & Niekerk, J. van. (2017). Assessing the Effectiveness of the Cisco Networking Academy Program in Developing Countries. In *Information security education for a global digital society* (Vol. 503, pp. 27–38). Springer, Cham.

Zhang, W. (2017). Network criminology : the criminology based on network science. *Network Biology*, *7*(1), 1–9.

Appendix A

Academic Publications

Appendix A includes the academic papers that were written throughout the duration of the study. These papers include the following:

1. Assessing the Effectiveness of the Cisco Networking Academy Program in Developing Countries
2. Towards an integrated skills competency framework for CSIRT personnel
3. Topic Map for Network Security Competencies

A.1 Assessing the Effectiveness of the Cisco Networking Academy Program in Developing Countries

This paper demonstrated the conceptual connection between the NICE Framework and the Cisco network security CBL programme used in Higher Education Institutions courses. It focused on assessing the Cisco Network Academy as an effective blended learning programme through the use of competencies in Higher Education

An Educators Perspective on Information Security Behaviour: A Case Study

Odwa Yekela, Kerry-Lynn Thomson and Johan van Niekerk

Nelson Mandela Metropolitan University, Port Elizabeth, South Africa.
(odwa.yekela, kerry-lynn.thomson, johan.vanniekerk)@nmmu.ac.za

Abstract. With the growing dependency of users on computers, technology and the internet, the protection of information and information systems is of utmost importance. Current computing graduates will become tomorrow's users and protectors of information and information systems. It is, therefore, essential that higher education institutions provide adequate information security education to enable these graduates to protect information and related information systems. This information security education should, preferably, be a part of their formalized studies. This paper discusses the opinions and experiences of computing educators regarding the extent to which information security is currently integrated within computing curricula and the current information security behaviour of computing students and educators. A total of twenty educators, from six South African higher education institutions, voluntarily participated in this study. Results indicated that there was limited information security integration within computing curricula at these higher education institutions. This could potentially negatively impact the information security behaviour of computing graduates.

Keywords: Information security behaviour, computing students, pervasive information security, information security education, computing curricula.

1. Introduction

User behaviour accounts for the majority of security breaches experienced by organisations, although often not with malicious intent to cause harm. Users who have not been educated with regard to information security could be easy targets for hackers because of their ignorance. Therefore, educated and trained users could be a critical success factor in order to mitigate threats within organisation [1,2]. Once computing graduates leave higher education institutions, many become employees within organisations. Computing in this context refers to Computing Science (CS), Information Systems (IS) and Information Technology (IT).

The Association for Computing Machinery (ACM) curricular guidelines [3] describe what characteristics computing graduates should have once they have completed their degrees. The CS guidelines explain that a graduate "*needs a set of general principles, such as sharing a common resource, **security**, and concurrency*. The IS guidelines refer to Information Assurance and Security (IAS) as IT security and risk management. It also states that this is an elective course. [3,4]. The IT

M. Bishop et al. (Eds): WISE 10, IFIP AICT 503, pp. 27-38, 2017.
DOI: 10.1007/978-3-319-58553-6_3

guidelines specifically state that an IT graduate should have an "*understanding of professional, ethical, legal, **security** and social issues and responsibilities*" [4]. Furthermore, the IT guidelines describe IAS as an integrative knowledge area that should be pervasive throughout other knowledge areas [4]. Pervasive, in this context, is defined as "*existing in all parts of a place or thing; spreading gradually to affect all parts of a place or thing*" [5]. Therefore, these computing guidelines suggest that graduates from these disciplines should be conscious of information security, particularly when they become employed within organisations. It is important that they stay abreast of industry trends, as these graduates need to be able to solve current real world problems. If the curriculum does not offer the necessary tools needed to solve these real world problems, then the higher education institution has failed [4].

Education is often the only way to convince users of the need to do things differently [6]. Schneider [7] argues that an educated workforce is essential to building trustworthy systems. In the same way, computing graduates who are conscious of information security could build systems that protect information. According to [6], users will often refuse to accept the need for new, responsible behaviour patterns until they have acquired the relevant information security knowledge, skills and insight.

According to [8], information security culture shapes and guides information security behaviour. Similarly, an organisation's information security culture is cultivated by the information security behaviour of its users [9]. If an information security culture does not exist within an organisation, the behaviour of new employees, for example computing graduates, coming into the organisation could influence the cultivation of an information security conscious culture [10,11]. As information security threats continue to be a grave concern, the importance of information security education cannot be stressed enough in computing curricula [12].

This research uses semi-structured interviews to determine the opinions and experiences of computing educators regarding the extent to which information security is integrated in computing curricula, as well as the information security behaviour of computing students and educators. Section 2 discusses information security behaviour, while Section 3 explains the purpose of this study. Section 4 describes how this research was conducted including the interview process, participants and the structure of the questionnaire. Section 5 highlights the results and findings, while Section 6 provides a discussion and Section 7 concludes.

2. Information Security Behaviour

Information security is not solely a problem of technology, but more often than not, it is a human problem. The greatest threat to information security could be employees who are not information security conscious [13, 14]. Information security behaviour refers to the behaviour of employees when they engage with information systems, including hardware, software and network systems. Such security-related behaviours have major implications for information security [15]. Depending on its nature, employee behaviour may either pose a risk or reduce threats to information security. Information security behaviour is classified into four broad categories, according to Guo [15]. These categories include security assurance behaviour, security compliant behaviour, security risk-taking behaviour and security damaging behaviour.

Security Assurance Behaviour: Security assurance behaviour (SAB) refers to intentional behaviours that employees carry out actively to protect information assets and information systems. In other words, this behaviour refers to employees that are information security conscious. This is the most desirable behaviour from an information security management perspective. Examples of SAB include identifying and being aware of threats and implementing the necessary security measures to counteract those threats. A significant characteristic of SAB is that it implies conscientious action, which means that employees make an effort to behave securely. This means that employees are going further than what is required or expected of them to do [15].

Security Compliant Behaviour: Security compliant behaviour (SCB) refers to intentional or unintentional behaviours that adhere to organisational information security policies. According to [16], SCB may be intentional in that employees make a conscious effort to avoid infringing security policies. It may also be unintentional in that employees may do something without thinking about security issues in mind, although their behaviour might still be adhering to security policies. Employees in the SCB group can be viewed as doing what they are required to do [15]. Individuals are motivated by different characteristics to comply with information security policies. These characteristics may be inherently related to personality, habits and skills. Environmental factors, for example, information security culture, may also influence an individual either to comply with or to violate security policies [17].

Security Risk-taking Behaviour: Security risk-taking behaviour (SRB) refers to intentional behaviours that may put information systems at risk, although not with the intentional motive to cause damage. In other words, employees may put organisations at risk unintentionally by, for example, writing down passwords, leaving sensitive documents lying around or visiting websites that are not secure. This behaviour can be likened to that of a non-malicious security violation [18]. Employees in this group are not doing what they are supposed to do [15].

Security Damaging Behaviour: Security damaging behaviour (SDB) refers to intentionally damaging behaviours that can cause significant damage to information systems. These behaviours are malicious and deliberate, and can be subject to punishment under the laws and regulations of the society rather than policies. Examples of SDB include industrial espionage, fraud and information theft. Essentially, employees that are categorised in this group are intentionally doing what they are prohibited from doing. There are similarities between employees in the SRB and SDB groups in that they are both doing what they are prohibited from doing. However, the difference between the two groups is in the consequences of their behaviours. In the case of SDB, the consequence is direct damage to information systems, while in the case of SRB, the consequence is risk, which may not necessarily cause damage [15].

Based on this discussion regarding the different security-related behaviours, it is evident that SAB is the ideal behaviour to ensure information security. Ultimately, within an organisation information security should be second nature to employees, which means it should not be a conscious effort, but a subconscious one and part of their everyday behaviour.

When computing students graduate from higher education institutions, they are likely to be employed by organisations. As such, they will be expected to protect organisational information systems and related information assets. Therefore, they need to be educated on how to provide the required protection. Ideally, this should be done before graduating. Higher education institutions are responsible for producing computing graduates who are information security conscious and who meet industry needs with regard to information security [19].

Computing students who have not been educated with regards to information security could typically fall into the SRB category. This is mainly due to the fact that they may not be aware that their actions or inactions, pose a risk to information assets and information systems. The ideal situation would be one where computing students demonstrate SAB before graduating and becoming employees. Over time, this could lead to an information security culture where the normal behaviour in higher education institutions is SAB.

3. Purpose of the Study

It is currently not known to what extent information security is integrated into undergraduate computing curricula in South African higher education institutions. In addition, the information security behaviour demonstrated by computing students and educators in unknown. The purpose of this study was, therefore, to address two main objectives. The first objective was to determine the extent to which information security is currently integrated into computing curricula. The second objective was to determine the current information security behaviour of computing students and educators. In order to meet these objectives, this study gathered opinions and experiences from computing educators at six South African higher education institutions.

4. Research Process

This section explains the process that was followed in order to collect data from the participants. In addition, it describes the semi-structured interview process, the participants, as well as the design of the questionnaire that was used as a basis for the interviews conducted.

Interview Process: A semi-structured interview was conducted with twenty participants with the aid of a questionnaire to gather the opinions of the participants. Participation in this study was voluntary and participants remain anonymous.

Participants: The participants were selected from six South African higher education institutions. Three were from CS, eight from IT and nine from IS.

Questionnaire Design: The questionnaire was divided into two sections with each section focusing on a single objective.

Section 1 - To determine the extent to which information security is currently integrated within computing curricula: Table 1 consists of a comprehensive list of questions and the question type contained in Section 1 of the questionnaire. This section consisted of closed (yes/no) and open-ended questions.

Table 1: Section 1 Questions

Section 1 Questions		Type
1.1	Do you teach any security-related modules?	Closed
1.2	If yes, which level?	Open-ended
1.3	Is information security pervasively integrated within other modules?	Closed
1.4	If yes, which modules?	Open-ended
1.5	Do you think information security should be an important part of your specific discipline?	Closed
1.6	If yes, why? If no, why not?	Open-ended
1.7	What are your views on the pervasive integration of information security within your discipline?	Open-ended
1.8	Do you think that your colleagues share the same views with regards to the pervasive integration of information security?	Closed
1.9	If yes, why? If no, why not?	Open-ended
1.10	Do you foresee any perceived challenges with regards to the pervasive integration of information security?	Closed
1.11	If yes, what perceived challenges do you foresee?	Open-ended

The primary aim of Section 1 was to ascertain the opinions of the participants on whether information security was currently integrated within their undergraduate computing curriculum and their general views on the pervasive integration of information security.

Section 2 - To determine the current information security behaviour of computing students and educators: Table 2 indicates the list of questions and the question type contained in Section 2 of the questionnaire. This section consisted of closed (yes/no) and open-ended questions.

Table 2: Section 2 Questions

Section 2 Questions		Type
2.1	Do you think that your students behave in a secure manner?	Closed

2.2	If yes, how so? If no, why do you say so?	Open-ended
2.3	Are you aware of any information security behavioural policies within your institution?	Closed
2.4	Are students aware of these behavioural policies?	Closed
2.5	Are there any consequences for "incorrect" behaviour?	Closed
2.6	If so, what are they?	Open-ended
2.7	In your opinion, does an information security culture exist within your department amongst your students and colleagues?	Closed
2.8	If yes, how so?	Open-ended
2.9	How would you influence a student or colleague to behave more securely?	Open-ended

The purpose of Section 2 was to determine the opinions and observations of participants with regard to the information security behaviour of their students, as well as their colleagues. The following section provides the results and findings of this research.

5. Results and Findings

The purpose of this section is to provide the results and findings of the semi-structured interviews based on the questionnaire described in the previous section.

Section 1 - To determine the extent to which information security is currently integrated within computing curricula: Table 3 represents the number of participants who answered “yes” or “no” to the closed questions for the first objective. It is important to note that the table does not show the complete list of questions for this section, as some were open-ended questions. However, answers to both the closed and open-ended questions are discussed in this section.

As shown in Table 3, 11 (55%) of the participants indicated that they did not teach any specific security-related modules (Question 1.1). In response to Question 1.2 in Table 1, the 9 (45%) participants who answered “yes” to Question 1.1 indicated they taught security-related modules ranging from 1st year through to 5th year of study.

For Question 1.3, it must be noted that even though the question asked if information security was pervasively integrated, on further enquiry most participants misinterpreted the term *pervasive*. 14 (70%) of the participants indicated that there are certain modules that include only a few aspects of information security, for example, secure passwords (Question 1.3). Therefore, these participants misinterpreted this as being pervasive. Examples of the modules where information security aspects were mentioned include: information security, project management, e-business, databases, application development and forensics (Table 1, Question 1.4). 19 (95%) of the participants agreed that information security should be an important part of their discipline (Question 1.5). In response to Question 1.6 (Table 1), one participant indicated that people interact with information and information systems on a daily basis; thus they should be able to protect those information systems. Other participants indicated that it is important for everyday life as information security is a real world problem. The participants' perceptions on the pervasive integration of information security is that it is important to integrate information security. However, many participants mentioned that it should be contextualised within the applicable modules (Table 1, Question 1.7).

Table 3: Section 1 Closed Questions and Responses

Section 1 Closed Questions		Yes	No
1.1	Do you teach any security-related modules?	9 (45%)	11 (55%)
1.3	Is information security pervasively integrated within other modules?	14 (70%)	6 (30%)
1.5	Do you think information security should be an important part of your discipline?	19 (95%)	1 (5%)
1.8	Do you think that your colleagues share the same views with regards to pervasively integrating information security?	19 (95%)	1 (5%)
1.10	Do you foresee any perceived challenges with regards to pervasively integrating information security?	18 (90%)	2 (10%)

19 (95%) participants indicated that they thought their colleagues shared the same views as they did with regard to pervasively integrating information security (Question 1.8). It was indicated that only those colleagues with some information security background knowledge shared the same views with regard to the integration of information security (Table 1, Question 1.9). However, 18 (90%) of the participants indicated that they foresaw challenges with regard to the pervasively integration of information security into their modules. In answer to the open-ended Question 1.11 (Table 1), some of the perceived challenges they foresaw included: not enough time within their existing modules to include information security; information security is too technical; and educators do not know *how* to integrate information security within their respective modules.

Section 2 - To determine the current information security behaviour of computing students and educators: Table 4 represents the number of participants who answered "yes"' or "no" for each closed question.

Table 4: Section 2 Closed Questions and Responses

Section 2 Closed Questions		Yes	No
2.1	Do you think that your students behave in a secure manner?	6 (30%)	14 (70%)
2.3	Are you aware of any information security behavioural policies within your institution?	0 (0%)	20 (100%)
2.4	Are students aware of any ICT-related policies?	9 (45%)	11 (55%)
2.5	Are there any consequences for "incorrect" behaviour?	17	3

		(85%)	(15%)
2.7	Does an information security culture exist in your department amongst colleagues?	14 (70%)	6 (30%)

As can be seen in Table 4, 14 (70%) of the participants indicated that their students do not behave securely (Question 2.1). In relation to Question 2.2 (Table 2), examples provided by the participants indicated that their students did not behave in a secure manner as they tend to share passwords and accounts. They also do not log off their computers and they do not scan their USB sticks.

All of the participants (100%) indicated that no specific information security behavioural policies exist at their respective institutions. Upon further investigation, participants mentioned that their higher education institutions had ICT usage policies that students had to comply with (Question 2.3). 9 (45%) of the participants indicated that their students were aware of the ICT usage policies (Question 2.4). Furthermore, 17 (85%) of the participants indicated that there were consequences for incorrect ICT usage policy behaviour (Question 2.5). Consequences provided by participants for "incorrect" ICT usage behaviour (Table 2, Question 2.6) include: disciplinary hearings; disabling accounts; community service; and banning students from laboratories.

14 (70%) of the participants specified that an information security culture does exist within their department amongst colleagues (Question 2.7). However, it was indicated by participants that the security culture that does exist within their department seems to be limited to physical security. Locked office doors, passwords protecting examination papers when sent via email and logging off unattended computers were some examples highlighted as evidence of a security culture (Table 2, Question 2.8).

Some examples highlighted by participants with regard to how they would influence students and colleagues to behave more securely included (Table 2, Question 2.9): knowledge, education and awareness; contextualised examples; scenarios; scare tactics; and case studies.

6. Discussion

The ACM computing curricular guidelines [3,20,4] clearly present IAS as an integrative knowledge area that should permeate other knowledge areas. However, results from the survey show that information security is not pervasively integrated within computing curricula. Participants indicated that possible challenges for pervasive integration could be that educators did not know how to integrate security; they do not have enough time within their modules; and that information security is too complex. More focus should be placed on ways to incorporate information security practically within these modules so that it permeates throughout each computing discipline.

Participants generally acknowledged the importance of information security as being an integral part of any ICT practitioner's daily life. The participants from the information systems discipline in particular emphasised that information was at the core of what they did within their discipline. However, from this study it was seen that many participants misunderstood the term *pervasive* with regard to integrating information security into their modules. It was generally assumed that if there was a module that focused on information security it was adequately integrated into the curriculum.

However, after clarifying what is meant by the pervasive integration of information security, the majority of the participants were willing to consider the integration of information security into their modules. The participants indicated that they would prefer small, contextualised information security examples that are applicable to each of their specific modules. In addition, many indicated that they were not equipped with any guidelines on *how* to integrate information security concepts into their modules. This poses a great challenge because the ACM states that information security should be a pervasive theme, but they do not suggest ways in which this can be done.

The majority of participants indicated that their students did not act in a secure manner. This result suggests that there is a significant need for change in information security behaviour. Information security education could play an important role in equipping the students with the necessary knowledge, skills and insight to influence their behaviour.

Most of the participants indicated that a physical security culture existed within their work environment. Information security culture could influence the information security behaviour of computing students. However, results showed that an information security culture does not exist within these higher education institutions. If an information security culture does not exist within computing departments, it is possible that computing students will not act in a secure manner.

From this study, it can be concluded that many computing educators in South Africa are not *consciously* doing enough to positively influence the information security behaviour of their computing graduates through the pervasive integration of information security into their modules. However, in order to do this, guidelines are required on *how* to integrate information security pervasively to empower them to do this. Through this education, the information security behaviour of computing students could be positively influenced.

7. Conclusion

In order to adequately protect the information assets of an organisation, it is important for users to acquire the necessary information security knowledge through education. The results from the semi-structured interviews suggest that participants generally accepted that information security is an important part of everyday life and thus should be taught in computing curricula. It is evident from these participant responses that there is little to no pervasive information security integration at these higher education institutions. It is believed that if computing students were exposed to information security, this could positively influence the information security behaviour of these students. However, if educators are not interested or do not see the need for this integration, it would be very difficult for the students to acquire the required information security knowledge, skills and insight. In the same way that uneducated users are the weakest link with regards to information security, educated users could be the strongest link with regards to the protection of information.

8. 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.

9. References

1. Al Awawdeh, S. & Tubaishat, A., (2014). An information security awareness program to address common security concerns in IT unit. *ITNG 2014 - Proceedings of the 11th International Conference on Information Technology: New Generations*, pp.273–278.
2. Cox, J., (2012). Information systems user security: A structured model of the knowing-doing gap. *Computers in Human Behavior*, 28(5), pp.1849–1858.
3. ACM, (2013). *Computer Science Curricula 2013: Curriculum Guidelines for Undergraduate Degree Programs in Computer Science*.
4. Lunt, B.M. et al., (2008). *Information Technology 2008 Curriculum Guidelines for Undergraduate Degree Programs in Information Technology*.
5. Oxford Dictionaries, (2015). Oxford Dictionaries- Language matters. *Oxford online dictionary*. Available at: http://www.oxforddictionaries.com/definition/learner/pervasive [Accessed December 1, 2016].
6. Schein, E.H., (1999). *The corporate culture survival guide: Sense and nonsense about culture change.*, San Francisco, CA: Calif.:Jossey-Bass.
7. Schneider, F.B., (2013). Cybersecurity education in universities. *IEEE Security and Privacy*, 11(August), pp.3–4.
8. Hu, Q. et al., (2012). Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture*. *Decision Sciences*, 43(4), pp.615–660
9. Da Veiga, A. & Eloff, J.H.P., (2010). A framework and assessment instrument for information security culture. *Computers & Security*, 29(2), pp.196–207.
10. Van Niekerk, J. & von Solms, R., (2005). A holistic framework for the fostering of an information security sub-culture in organizations. *Issa*, pp.1–13.
11. Von Solms, R. & von Solms, B., (2004). From policies to culture. *Computers and Security*, 23, pp.275–279.
12. Yoon, C., Hwang, J.-W. & Kim, R., (2012). Exploring factors that influence students' behaviors in information security. *Journal of Information Systems Education*, 23(4), pp.407–416.
13. Öğütçü, G., Testik, Ö. M., & Chouseinoglou, O. (2015). Analysis of personal information security behavior and awareness. Computers & Security, 56, 83–93. http://doi.org/10.1016/j.cose.2015.10.002
14. Shropshire, J., Warkentin, M., & Sharma, S. (2015). Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. Quaternary Geochronology, 49, 177–191. http://doi.org/10.1016/j.cose.2015.01.002

15. Guo, K. H. (2013). Security-related behavior in using information systems in the workplace: A review and synthesis. Computers & Security, 32(1), 242–251. http://doi.org/10.1016/j.cose.2012.10.003
16. Guo, K. H. (2013). Revisiting the human factor in organizational information security management. ISACA Journal, 6, 1–5.
17. Padayachee, K. (2012). Taxonomy of compliant information security behavior. Computers and Security, 31(5), 673–680. http://doi.org/10.1016/j.cose.2012.04.004
18. Guo, K. H., Yuan, Y., Archer, N. P., & Connelly, C. E. (2011). Understanding nonmalicious security violations in the workplace: A composite behavior model. Journal of Management Information Systems, 28(August 2015), 203–236. http://doi.org/10.2753/MIS0742-1222280208
19. Talib, M. A., Khelifi, A., & Ugurlu, T. (2012). Using ISO 27001 in teaching information security. In IECON 2012 - 38th Annual Conference on IEEE Industrial Electronics Society (pp. 3149–3153). Montreal, QC: IEEE. http://doi.org/10.1109/IECON.2012.6389395
20. Topi, H., Valacich, J. S., Wright, R. T., Kaiser, K., Nunamaker, J. F., Sipior, J. C., & de Vreede, G. J. (2010). IS 2010: Curriculum guidelines for undergraduate degree programs in information systems (pp. 359–428).

A.2 Towards an integrated skills competency framework for CSIRT personnel

This paper proposed the integration of high-level competencies with low-level task-oriented competencies for assessing CSIRT competencies.

Towards an integrated skills competency framework for CSIRT personnel

BLIND COPY

***Abstract*—One of the challenges of establishing and managing a CSIRT is finding the right personnel with the right competencies to operate the CSIRT. CSIRTs are diverse in nature, the skills that are applicable in a CSIRT depend largely on the services provided by the CSIRT. Competency frameworks, such as the SFIA Framework, are good at defining competencies within ICT disciplines, but they lack the ability to describe how an individual can develop these competencies. Skill specific frameworks, such as Cisco certifications, are good at developing an individual's competencies, however, the framework lacks the ability to holistically address competencies. This research investigates how competency frameworks (SFIA Framework) and skill specific frameworks (Cisco Framework) can be aligned in order to describe the skills requirements for a CSIRT. The concept of a Topic Map is introduced as a way of integrating competency frameworks with skill specific frameworks in order to describe competencies within a CSIRT environment, and the paper further discusses how these competencies may be correlated with job roles.**

***Index Terms*—competency, SFIA, Cisco, competency frameworks, CSIRT, CERT, Topic Map.**

I. Introduction

Communication networks and information systems are necessary for economic and social development, thus computation and networking services are fast becoming universal utilities much like water and electricity [1]. Many organisations rely on Information Communication Technology (ICT) services to sustain critical business functions, these ICT services require specialised ICT skills that aid in supporting business objectives [2] [3]. Due to this reliance on ICT services, safeguarding of communication networks and information systems has become an increasing concern. The protection of information and information assets requires a specialized set of ICT skills. This includes global security initiatives such as the Computer Security Incident Response Team (CSIRT) that require special training or experience. [1].

Institutions such as the South African National Research Network (SANReN) and TENET require CSIRT services in order to protect their constituents from network related attacks. SANReN is a South African high-speed network dedicated to research traffic [4]. TENET on the other hand is a non-profit organisation that acts as an Internet Service Provider to research institutions. SANReN and TENET work closely together, SANReN builds the necessary network infrastructure, while TENET operates the network on behalf of SANReN. The latest collaboration between SANReN and TENET involves the two parties forming a partnership in order to establish and operate a CSIRT for the SANReN network called the SA NReN CSIRT. This research paper focuses on describing the context of skills needed in a CSIRT and will use the SA NReN CSIRT as a case study.

II. CSIRT

Keeping communication networks and information systems secure in todays globally interconnected world has become a challenging task [3]. Many organisation use a CSIRT to respond to security incidents. CSIRTs are defined by many sources as;

> *Organisation or team providing services or support for preventing, handling and responding to computer security incidents [5]*
>
> *Team of IT security experts who respond to security incidents. It provides the necessary services to handle them and support constituents to recover from them. [1]*
>
> *Is a service organisation responsible for receiving, reviewing and responding to computer security incident reports and activities. Its services are targeted for a defined constituency - [3]*

Thus from the definitions discussed, a CSIRT can be described as an organized group of IT experts tasked with the responsibility of preventing, handling and responding to a constituencys computer security incidents. There is no fixed framework for establishing a CSIRT across all organisations, rather the establishment and operation of a CSIRT depends mainly on the type of services the CSIRT is planning on providing to its constituent [5]. Due to the dynamic environment in which CSIRTs operate no two CSIRTs can possess exactly the same set of services, policies and procedures [6]. According to the Handbook for Computer Security Incident Response Teams, a starting point for establishing a CSIRT is describing what the CSIRT will do, who it will be done for, in what environment it will operate and in cooperation with whom [6]. These are the main questions that should be addressed when setting up the requirements for a CSIRT.The SANReN and TENET CSIRT partnership is still at its planning stage and the SA NReN CSIRT has not been established. Therefore, it is imperative that the two partnering organisations work together outlining the mission, purpose and the constituency of the SA NReN CSIRT. For a CSIRT to be successful it is important to understand the needs of the constituent and to provide the appropriate services based on those needs [1].

III. WHAT DO THEY DO?

A CSIRT can operate in a variety of ways and may have different requirements, responsibilities, functions and structures

[7]. What exactly a CSIRT does depends upon the services provided by the CSIRT to its constituency and the policies that have been put in place by the organisation [1]. There have been organisations that decide their CSIRT staff will deal only with incident handling while other organisation's staff implement further tasks such as incident analysis and response, vulnerability handling, intrusion detection, risk assessment, security and penetration testing [3]. However, at a minimum, a CSIRT must at least provide implementation of incident handling [6] . Therefore, a main objective of a CSIRT is to isolate, mitigate the effects of, disable and assist with recovery from an incident.

A. TYPES OF CSIRT

A CSIRT can operate in a hierarchical manner, coordinated by global and regional forums. This includes national CSIRTs followed by sector CSIRTs and finally individual company or organisational CSIRTs [6]. The constituencies that the CSIRTs serve may overlap at times [8]. For example, a national CSIRT may be servicing all sites in a specific country or all Internet users in specific country. Other CSIRTs may also exist within that country that service their own specific constituencies which may overlap with the national CSIRT. SA NReN CSIRT is a national South African incident response initiative that will encompass constituents at a national level. The SA NReN CSIRT may cooperate with other trusted CSIRTs.In cases where the SA NReN CSIRT overlaps with other CSIRTs in responsibility, there needs to be clear communication between the CSIRTs in order to negotiate and try to find a compromise of what is expected between them [8].

B. CSIRT SERVICES

One of the main things that needs to be addressed when establishing a CSIRT is deciding on what services will be provided to the constituency [9]. There are many services that can be provided by a CSIRT, each CSIRT is different and as a result will provide services based on their own mission, purpose and constituency needs [9]. There are three broad categories of CSIRT services which are categorised as reactive, proactive and security quality management services [8].

- Reactive services these are the services that are taken to resolve or mitigate incidents as they occur. Reactive services form the core of CSIRT and are triggered by an event or request [5].
- Proactive services refers to services that are put in place with the objective of preventing incidents from occurring in the first place, thus these services provide assistance and information to help prepare, protect and secure communication networks and information systems from anticipated attacks or events [9].
- Security quality management services refers to services that are well-known, established services designed to improve the overall security of an organisation. These services can be provided by other areas of an organisation and are not necessarily CSIRT- specific [3].

To be effective, a CSIRT should address proactive and reactive issues [6]. As discussed earlier, the type of services and the scope of the services provided by a CSIRT to its constituency depends largely on the mission and purpose of the CSIRT, as well as the service assets available, such as resources and capabilities of the organisation [7]. The mission, purpose and service assets of the SA NReN CSIRT have been developed through a series of workshops between key SANReN and TENET stakeholders. It was decided that the service responsibilities for the SA NReN CSIRT be divided between the two parties. SANReN shall provide the proactive services and TENET shall provide the reactive services for the SA NReN CSIRT [10].

Yet another contributing factor is the technology that is accessible to the organisation. A CSIRT must have the right mix of services, sufficient resources and capabilities, but they will always be limited to the technology that is accessible to them. Thus technology constraints become a concern and organisations must ensure that they keep up to date with technology in order to operate the CSIRT in the most effective manner.

C. CSIRT PROCESSES and POLICES

Organisations usually have a set of defined policies and processes in place to ensure that the organisation is governed and operated in the proper way. ITIL describes policies as formally documented expectations and intentions [11]. An alternative definition of a policy is the governing principle under which the team operates [6]. A process is described as a structured set of activities designed to accomplish a specified objective [11].

1) Policies: In the context of a CSIRT, policies can be grouped into two sets of policies. Policies that are organisational specific (corporate policies) and policies that are CSIRT specific. Organisations may describe and implement specific sets of policies throughout their organisational activities. These policies are unique to each organisation and may be based on legal, geographic and strategic factors. The second category of policies are policies that are specific to the establishment and operation of a CSIRT such as incident reporting and request handling, data classification and prioritisation and communication [6].

CSIRT specific policies may be similar among multiple organisation, whereas organisational specific policies are unique to each organisation. Organisational specific policies dictate the nature of CSIRT specific policies. Organisations must ensure that there is a seamless flow between all the policies. In the context of SA NReN, there is added complexity in policy implementation, as the CSIRT services for the SA NReN CSIRT are separated between two organisations. It is critical that these organisational specific and CSIRT policies do not conflict with one another.

2) Processes: Processes are implemented to minimise errors by providing standardised response [12], thus improving the overall quality and time required to perform an incident response [1]. Processes should be driven by an organisation and integrated into other processes. There should be defined accountability via assigned roles and responsibility [5]; be supported by polices process should be repeatable [12]; be documented and reviewed [13].

In order for a team to operate effectively, there needs to be well-defined policies, procedures and service processes [6]. One of the first issues a team should address in its policies and procedures is the level of service it's willing or able to provide to different parties [6].

D. CSIRT ROLES

The staff roles, responsibility and accountability need to be defined for a CSIRT. The actual assignment will depend largely on the structure of the host organisation. SANReN and TENET have agreed that the TENET Chief Technical Officer (CTO) shall serve as the CSIRT manager and recruit a system administrator with 50% time allocated to CSIRT activities. SANReN shall commit 1.5 full-time equivalent senior network engineering and information security specialists will be recruited and manage the proactive SA NReN CSIRT services.

IV. CSIRT SKILLS AND RESPONSIBILITY LEVELS

People are an important asset to an organisation and represent both a resource and a capability [11]. Cannon further expresses the importance of people as an asset by stating that if capabilities are the capacity for action, people assets are the actors. Finding the right people who possess the appropriate experience, skills and training is one of the challenges when establishing a CSIRT [7].

The Dutch Society for Information Security (PvIB) has raised its concerns about the difficulty in comparing certifications and qualifications with job titles of Information Security Professionals. As a result of this, PvIB has indicated that Information Security Professionals are unable to clearly identify their knowledge and experience on the basis of their job title and supporting certificates [14]. As it turns out, this has become a common problem among Information Communication Technology (ICT) professionals in general. There are so many different perspectives and so much diversity in skills expectations, it is difficult to implement a one shoe fits all response to this question. Generally it is expected that a professional is an individual that

- Has sufficient knowledge and skill within a discipline;
- Is accepted by the community, through certification, licensing or recognition as someone who
- Is capable of practising in the disciple;
- Operates with authority and responsibility;
- Adheres to a strict code of ethics; and
- Provides service to the community.

This raises the question 'Does this definition of a professional adhere to ICT professionals?' [15]. Cameron states that the ICT sector is facing a serious skills shortage and many attempts have been made to address this problem. Organisations struggle to find suitable individuals for specific ICT roles [16]. Thus, a common framework for describing competency was proposed by several parties [17]. These skills competency frameworks focused on describing the necessary attributes an individual needed to have to be recognized as being competent of a skill [17]. The Skills Framework of the Information Age (SFIA) and European e- Competency Framework (e-CF) are the predominant competency frameworks in ICT [18]. SFIA, which was developed by the British Computer Society, has become the most widely accepted of these frameworks. It is recognized in over 200 countries and is being implemented by thousands of organisations for managing their ICT skills resources [19]. SFIA is a skills competency framework that defines a collection of ICT skills. It is further described by the SFIA Foundation as "A common language for skills in the digital world".

A. WHAT IS COMPETENCY?

To understand the context of SFIA it is important to have a firm understanding of what competency is and why it is used as the main attribute in assessing an individuals skills. Competency is what a person is required to do and under what conditions. Competency involves the ability to draw knowledge, skill, attitude and values required to perform activities to a specified standard [20]. Competency standards are the result of functional analysis of a sector or particular domain [20]. Competency standards provide the tools for transforming the sector and cover the whole sector area. Competency standards can be utilised to create frameworks for assessing competency within a given sector [21]. According to SFIA and e-CF, competency forms the core components of a job role, but do not represent a job role holistically [19] [20].

B. SFIAS APPROACH TO COMPETENCY

SFIA can be used as a reference model for managing the skills in an organisation, SFIAs classification of competency is based on the Bloom Taxonomy Model [18]. The Bloom Taxonomy Model consists of three domains of learning. The Cognitive Domain refers to the different stages of knowledge, Affective Domain refers to different stages of attitude and Psychomotor domain, which refers to the different stages of a skill during learning [22]. These Bloom Taxonomy domains strongly correlate with competency (ability draw *knowledge*, *attitude* and *skill*). SFIA divides the context of a job role into three traits. These are Professional Skills (competency of a *skill* at a described level), Behavioural Skills (*attitude* towards an organisation, influence being described as a big factor) and Knowledge (*knowledge* of the sector based on sector standards) these traits are supported by qualification and/or experience [19].

Skills framework such as SFIA allow organisations to map a persons competency against a common reference framework [19]. This framework is multi-dimensional and consists of two axes. One of the axes divides skill traits (knowledge, professional skills and behavioural skills) into skills responsibility which are Autonomy, Influence, Complexity and Business Skill. The other axis describes the level of responsibility that should be given to a specific skill at a specific level of depth. SFIA describes seven of these levels of responsibility [15].

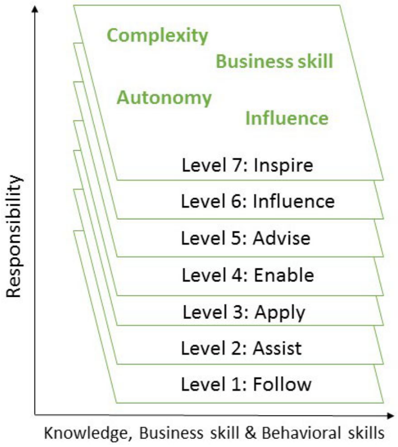


Fig. 1. SFIA Dimensions [19]

Each of the skills consist of the level of responsibility the skill is applicable in, and the amount of autonomy, complexity, influence and business skill required for each level of responsibility described [19].

The SFIA skills framework does not attempt to address all skills that may be held by ICT Professionals nor does it describe every competency in a skill in deep detail [19]. Instead, the SFIA framework can be regarded as a high-level overview of the core competency of ICT skills [19]. SFIA competency levels do not translate to job role, but rather they can be used as components of a job role. For example, the SFIA skill incident management does not represent the complete content of an Incident Manager job role. Competencies can be combined to represent the core content of a job role and a single competency can be assigned to multiple job roles [19]. In addition, SFIA competencies do not try to replace organisation competencies, instead they work alongside core organisational competencies as a supplementary resource [19]. An organisation may have a specific set of core competencies, along with the SFIA competencies. Furthermore, each individual within the organisation may have their own list of competencies they consider or desire as their own. Thus competency frameworks can be viewed from two perspectives. On one hand, there is Competency Management which deals with the defining, recruiting and maintaining of competencies in an organisation allowing organisations to select specific competencies from the framework and match them to projects that are being [23]. On the other hand, there is Competency-Based Learning which is based on competency standards. As mentioned earlier, individuals in an organisation may be pursuing their own career path and this may involve them selecting their own set of competencies from the framework.

C. IDENTIFYING SKILLS IN A CSIRT

Skills and knowledge in a CSIRT should be distributed amongst the team [8]. Having well-defined descriptions that include a list of the roles and responsibilities for each of the CSIRT positions along with the necessary skills, experience, educational background and/or certifications and clearance required can be a helpful tool in identifying and hiring the right staff [7]. Currently, SANReN and its affiliated partners are evaluating candidates' skills based on rigid job role specifications that do not encompass competencies as a whole. This limits an organisation's flexibility over people's skills, as a job role may be based on specific tasks that will be carried out and may not consider other skills a candidate may have that the organisation may find useful at a later stage. SFIA can be used as a tool to help identify the right staff to hire for the SA NReN CSIRT. In a CSIRT service, the SFIA framework can assist SANReN and TENET with Competency Management strategy

- The framework can be used by SANReN and TENET to identify the necessary competencies required to operate the SA NReN CSIRT and the level of responsibility that should be given to a competency given the depth of the skill. It can also assist in identifying the current level of competencies that already exist within the organisation.
- The framework can assist the organisation in selecting the appropriate candidates for the SA NReN CSIRT team. This reduces the risk of selecting a candidate that is competent at a skill, but not at the required level.
- The framework can assist with maintaining the demand for specific skills in the CSIRT, this includes training employees to meet the level of competency required by the CSIRT.

Since SFIA is a high-level framework it does not describe competencies in detail, thus there is an opportunity to fill this gap by using SFIA with a supplementary competency standard framework that provides a detailed overview of the required competencies. Competency-Based Learning is the second aspect of competency frameworks, it is described as a structured approach to learning and assessment directed toward assisting individuals to acquire knowledge, skills and attitude required to perform an activity to a specified standard [24]. Cisco is recognised as a worldwide leader in Communication Networks [**?**]. Ciscos deep understanding of industry and emerging technology has enabled them to set network standards and best-practices which are recommended and practiced on an international scale [25].Cisco focuses on Competency-Based Learning through certification. Certification establishes a standard of competency in a specific sector and job roles [26]. The Cisco Certification Program is the most widely used Competency-Based Learning program in the Communication Network sector. The SFIA Framework provides a common overview of ICT competencies, but does not address network security competencies.

D. CISCOS APPROACH TO COMPETENCY-BASED LEARNING

Cisco is an international corporation that provides a wide range of certifications across a multitude of interrelated network disciplines. These include network designing, network routing and switching and network security [27]. Cisco certification consists of a hierarchy of levels that are correlated with the competencies of each certification path, these levels in ascending order are Entry, Associate, Professional, Expert and Architect. These certificate levels are linked to one another. An example of this is before an individual can be recognised as a Cisco Certified Network Professional (CCNP) security they will have hold a valid Cisco Certified Network Associate (CCNA) security certificate. Thus, an individual must possess competencies of the previous level before attempting the next level [27].

Cisco assesses certification based on competency examinations that test an individuals level of competency in order to receive certification. Candidates who pass the required examinations go on to receive certification correlated to that examination. Certification can have one or more examinations as pre-requisite and multiple certifications can have the same examination as a pre-requisite. Each of the examinations seeks to test an individual at a certain set of competencies. Therefore, similar topics can be discussed across multiple examinations, but not necessarily at the same level of depth or complexity [27]. Individuals can pick sets of competencies based on the Cisco certification path that they would like to do, hence this Competency-Based Learning reflects the second perspective of competency frameworks described earlier.

V. COMPLEXITY OF DESCRIBING COMPETENCY

The attributes of competency consist of knowledge, attitude and skill [20].

- Knowledge - (one of the traits used in the SFIA competency framework) consists of different levels of depth, Bloom Taxonomy describes two sets of cognitive thinking. Lower Order thinking such as recognising, understanding and being able to apply concepts and Higher Order thinking include analysis, evaluation and the creation of new concepts [22].
- Attitude - (another of the traits used in the SFIA competency framework) reflect on an individual's behavioural habits towards something, this also is described by Bloom Taxonomy in different levels of depth. Receiving is recognized as the lowest form of attitude and organisation attitude by value is placed as the highest [22].
- Skills - (this is also a trait used in the SFIA competency framework) which is describes an individual's proficiency at an activity, Bloom Taxonomy uses its Psychomotor domain which describes skills in terms of learning complexity. This includes the unconscious incompetency of a skill right through to the unconscious competency of a skill [22].

It is quite clear that the context of competency is very complex, and is something that must be considered when evaluating an individuals competency. SFIA states that qualification or certification alone does not justify competency [19]. Cisco uses certifications to justify competencies in network security. While these competencies may be important to developing CSIRT roles, an organisation must consider more than technical knowledge when reviewing a candidate [12]. Thus, the SFIA framework alone is not enough to develop the SA NReN CSIRT job roles and neither is certification. This provides the opportunity to use a common framework (SFIA), used in collaboration with a specific framework such as Cisco certification framework (more specifically network security certification framework).

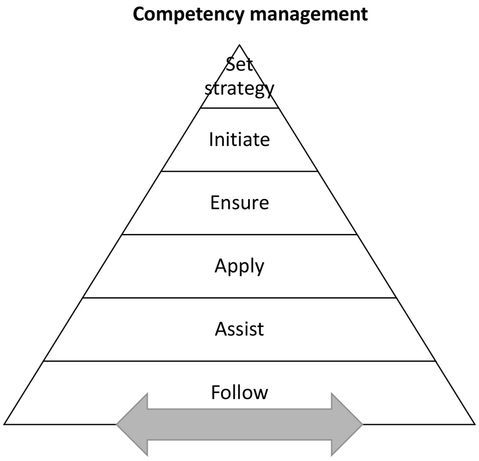


Fig. 2. SFIA level Framework [19]

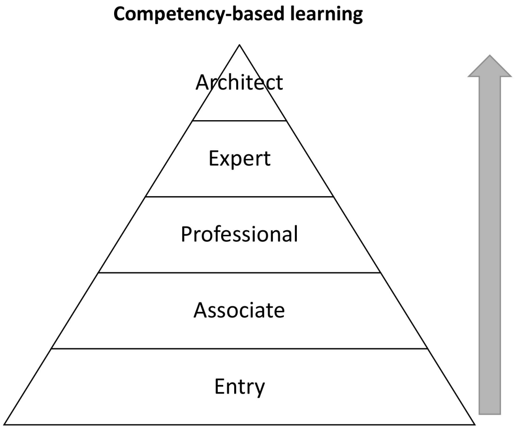


Fig. 3. Cisco level Framework [27]

A. *COMPARING THE DIFFERENCES BETWEEN SFIA AND CISCO IDEOLOGY*

SFIA is described as a durable framework and although technology, jobs and market terminology within the ICT environment changes rapidly, the SFIA framework is still able to describe competencies comprehensively. This is because SFIA does not describe any product or technology-specific skills or knowledge, industry experience or qualifications [19]. Cisco on the other hand, is a product specific framework that is based

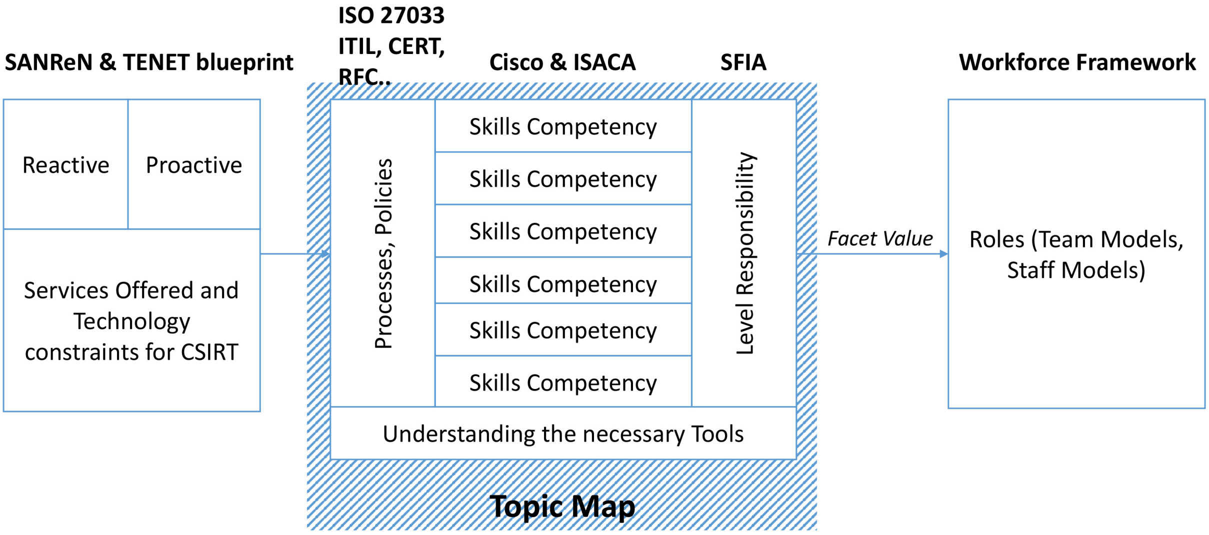


Fig. 4. How a Topic Map of skills competency would embody a CSIRTs skills requirements

mainly on the operation of Cisco technology, and, although the Cisco body of knowledge caters for topics that may not be Cisco specific, the Cisco framework is a technology based vendor specific framework.

A similarity between the SFIA and Cisco frameworks is how levels of competency are assessed. Both SFIA and Cisco follow a criterion-referenced assessment. In criterion assessment, an individual is either seen as competent or not ye [28]. A difference in ideology is how levels of competency are viewed by the framework. SFIA describes what competencies an organisation may use in Competency Management and levels are seen as equal in stature. For example, incident management at level 6 is not seen as superior to incident management at level 5. They are seen as two different sets of competencies that require different forms of responsibility. Cisco certificate levels on the other hand show elements of hierarchy and are based on Competency-Based Learning.For example, an individual holding an Expert certification is seen as superior to other individuals who may have Entry, Associate or Professional certification.

The SFIA framework and Cisco certification framework have been identified as the frameworks of interest in this paper. The two frameworks describe two different viewpoints on how to interpret competency. SFIA provides a high-level overview of competency most useful to organisations in aiding with Competency Management. Cisco on the other hand is a more detailed set of competencies that is geared for individuals building competency in a specific discipline such as network security. Grant defines how common and specific competency frameworks can be merged together using a Topic Map [17]. Topic Maps are an ISO standard (ISO/IEC 13250) for describing knowledge structures and associating them with information resources [29]. Topic Maps provide the meta-model on which a completely flexible application model can be built, such as a meta-framework. Although Topic Maps are a defined standard, there is currently no fixed ontology for how to create Topic Maps [30].

Thus, a Topic Map can be used to create a meta-framework tool for defining and describing skills competencies within a CSIRT, such as the SA NReN CSIRT. The Topic Map will possess characteristics from both Competency Management and Competency-Based Learning. Topic Maps can serve not only as a guide to locating resources for the expert, but also as a way for experts to model their knowledge in a structured way. This allows non-experts to grasp the basic concepts and their relationships before diving down into the resources that provide more detail [30]. Thus the Topic Map can be used by both ICT professionals and non-ICT departments, such as the Human Resource Department, to define specific competencies as required in the organisation and also provides a channel on how individuals can be trained within each competency defined. Each CSIRT has a unique mix of services that it provides to its constituency. As a result, the competency required in a CSIRT competency framework will differ amongst organisations. Topic Maps provide the facet feature which allows a Topic Map to be filtered down to specific resources based on specific values called facet value [30]. An individual organisation can set up facet values to describe competencies within the context of specific job roles.

VI. Topic Map in CSIRT

The use of a Topic Map will assist in identifying the critical skills required to operate a CSIRT, it will then assist in allocating the right amount of responsibility based proficiency of skill as opposed to job role. Organisations will be able to select their own mix of skills from the Topic Map based on the services they wish to provide in their CSIRT, such as incident management, problem management, information security and security administration. Each of the Topic Map skills consist of levels of responsibility as described in the context of SFIA. Some responsibilities in a CSIRT may be shared amongst multiple roles and may be performed by different people depending on the situation [5]. Thus, organisations need to ensure that the right level of responsibility is given to individuals who not only demonstrate competency of a skill, but who demonstrate this competency at a desired level. The Topic Map would include the capability of defining competencies and also being able to point to specific Competency-Based Learning resources. This would assist in answering the questions 'What skills do I need?' 'How much responsibility should I attach to the skills?' and 'How do I train individuals to reach that standard?'. During the selection and aggregation of competencies, the organisation can attach facet values to desired skills in order to create job roles. Different job roles may have similar skills requirements, use of the facet feature allows the Topic Map to identify the relationship between job roles, which gives the organisation the power to filter between different CSIRT roles. Figure 4 illustrates how skills competency relate to other components of a CSIRT. The image further illustrates the significance of using a Topic Map to develop job roles within a CSIRT.

VII. CONCLUSION

The assessment of skills competency is critical to the success of a CSIRT. The current skills competency frameworks do not address competency holistically within the ICT discipline. This limits the available options organisations have when assessing employee and candidates for CSIRT job roles. The use of a Topic Map is proposed as an approach that encompasses skills competency holistically. Topic Map features, such as the facet value, provide flexibility in how skills can be aggregated into a Topic Map to create job roles. This would allow for the assessment of the current skills of a candidate for any specific job, against both higher (overview) level competencies, and more technical (skills-based) competencies. Such Topic Maps can also meaningfully contribute towards the management of continuous professional development of employees in the fast changing network- and cyber-security domain.

REFERENCES

[1] ENISA, "A step-by-step approach on how to set up a CSIRT," ENISA, Tech. Rep., 2006.

[2] A. P. Calitz, "A Model for the Alignment of ICT Education with Business ICT Skills Requirements A Model for the Alignment of ICT Education with Business ICT Skills Requirements," 2010.

[3] G. Killcrece, K.-P. Kossakowski, R. Ruefle, and M. Zajicek, "State of the practice of computer security incident response teams (CSIRTs)," Carnegie Mellon Software Engineering Institute, Tech. Rep., October 2003.

[4] SANReN, "Overview," 2010, retrieved April 20, 2012 from http://www.sanren.ac.za/overview.

[5] C. Alberts, A. Dorofee, G. Killcrece, R. Ruefle, and M. Zajicek, "Defining incident management processes for CSIRTs : A work in progress," Carnegie Mellon University, Tech. Rep., October 2004.

[6] M. J. West-Brown, D. Stikvoort, K.-P. Kossakowski, G. Killcrece, R. Ruefle, and M. Zajicek, *Handbook for Computer Security Incident Response Teams (CSIRTs)*, 2nd ed. Carnegie Mellon Software Engineering Institute, Apr. 2003.

[7] G. Killcrece, K.-P. Kossakowski, R. Ruefle, and M. Zajicek, "Organizational models for computer security incident response teams (CSIRTs)," Carnegie Mellon Software Engineering Institute, Tech. Rep., December 2003.

[8] ENISA, "Good practice guide for incident management," ENISA, Tech. Rep., 2010.

[9] C. University, "CSIRT servicess," 2016. [Online]. Available: http://www.cert.org/incident-management/services.cfm?

[10] L. Staphorst and D. Greaves, "Update on the sa nren csirt," 2015, retrieved April 20, 2016 from http://www.sanren.ac.za.

[11] L. Hunnebeck, *ITIL® Service Design*. London: The Stationary Office (TSO), 2011.

[12] P. Cichonski, T. Millar, T. Grance, and K. Scarfone, "Computer security incident handling guide," NIST, Special Publication 800-61. Revision 2, Aug. 2012.

[13] D. Smith, "Forming an Incident Response Team," in *FIRST Annual Conference proceedings*. AUSCERT, 1994, pp. 1–37.

[14] M. Spruit and F. Van Noord, "Job profiles for information security," 2014.

[15] B. R. Von Konsky, "Defining the ICT profession: A partnership of stakeholders," *Proceedings of the 21st Annual Conference of the National Advisory Committee on Computing Qualifications*, pp. 15–22, 2008. [Online]. Available: http://www.citrenz.ac.nz/conferences/2008/15.pdf

[16] B. H. Cameron, "Enterprise systems education: New directions challenges for the future," *In Proceedings AMCIS2008*, 2008. [Online]. Available: http://aise1.aisnet.org/amcis2008/119.

[17] S. Grant, "Frameworks of competence: common or specific?" *Proceedings of International Workshop in Learning Networks for Lifelong Competence Development March 3031 Sofia Bulgaria*, pp. 111–116, 2006.

[18] P. Rudzajs, L. Penicina, M. Kirikova, and R. Strazdina, "Towards Narrowing a Conceptual Gap between IT Industry and University," *Scientific Journal of Riga Technical University. Computer Sciences*, vol. 41, no. -1, pp. 9–16, 2010. [Online]. Available: http://www.degruyter.com/view/j/rtucs.2010.41.issue--1/v10143-010-0019-5/v10143-010-0019-5.xml

[19] SFIA Foundation, "SFIA6 The complete reference guide," 2015.

[20] European Committee for Standardization (CEN), "User guide for the application of the European e-Competence Framework 3.0," 2014.

[21] E. Serge Ravet, ADPIOS, "Competency-based learning what is competency?" 2013, retrieved April 1, 2016 from (http://transit.ea.gr/.

[22] J. S. Atherton, "Learning and teaching. blooms taxonomy," 2016, retrieved April 5, 2016 from http://www.learningandteaching.info/learning/bloomtax.htm.

[23] J. A. C. B. L. Kevin Streater, Open University and D. S. Group, "Introduction to SFIA in LD and Workplace Learning, Ron McLaren," 2012.

[24] "A Guide to Writing Competency Based Training Materials," *Training*.

[25] T. Lammle, *CCNA Routing and Switching Study Guild*. John Wiley Sons,, 20013.

[26] A. Al-rawi, "2006-818 : INTEGRATING IT CERTIFICATIONS IN NETWORKING COURSES : CISCO CCNA VERSUS COMPTIA NETWORK + Integrating IT Certifications in Networking Courses : Cisco CCNA Versus CompTIA Network +," no. August 2000, 2006.

[27] Cisco Systems, "Training certifications," 2016. [Online]. Available: http://www.cisco.com/c/en/us/about.html

[28] S. Green, "Criterion Referenced Assessment as a Guide to Learning - the Importance of Progression and Reliability," *Africa*, pp. 1–15, 2002.

[29] Topic Maps, "Standards," Apr. 2016, retrieved April 8, 2016 from http://www.topicmaps.org/standards/.

[30] Microsoft, "An introduction to topic maps," 2015, retrieved April 10, 2016 from https://msdn.microsoft.com/en-us/library/aa480048.aspx.

A.3 Topic Map for Network Security Competencies

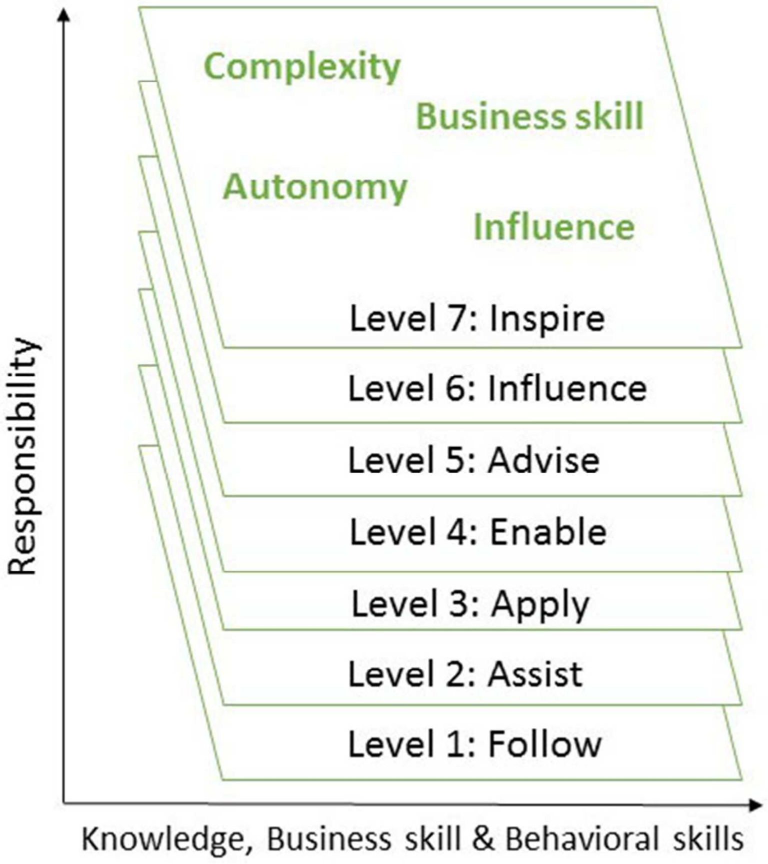
This paper is a revision of the previous paper, it proposes the use of a topic map for integrating competencies in competency frameworks with competencies in CBL programmes.

Information and Computer Security

Emerald Information Management and Computer Security

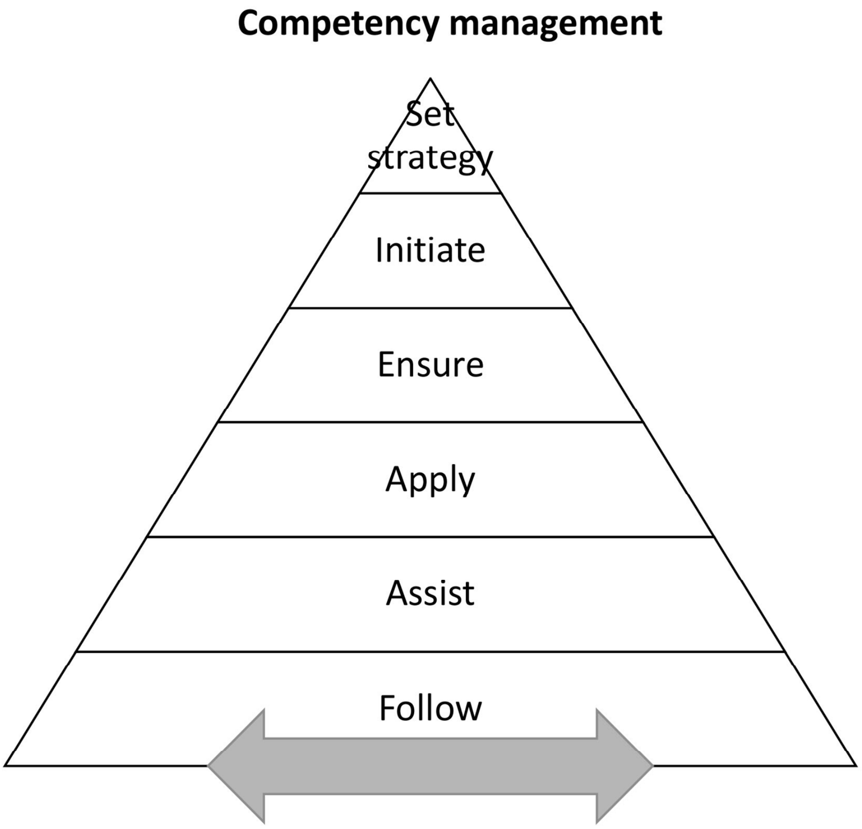
Towards an integrated approach to CSIRT competency modelling

Journal:	*Information and Computer Security*
Manuscript ID	ICS-07-2017-0051
Manuscript Type:	Original Article
Keywords:	Competency, Competency frameworks, CSIRT, CERT, Topic Map



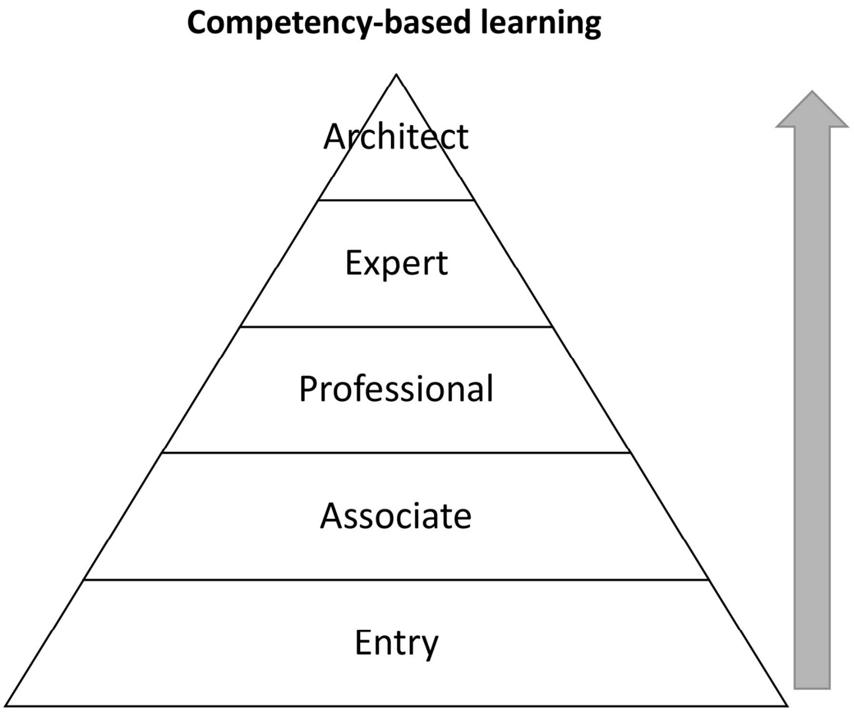
SFIA Dimensions

117x132mm (96 x 96 DPI)



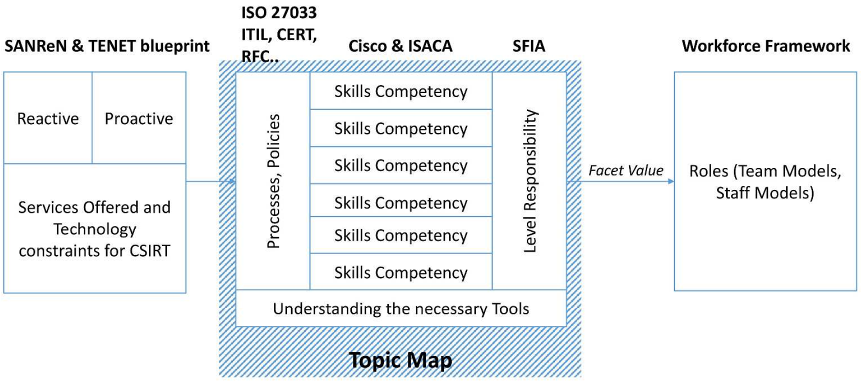
SFIA Levels

142x138mm (300 x 300 DPI)



Cisco levels

154x127mm (300 x 300 DPI)



Incorporation Topic Map into CSIRT

305x137mm (300 x 300 DPI)

Towards an integrated approach to CSIRT competency modelling

BLIND COPY

Abstract

Purpose: This research investigates how competency frameworks and Competency-Based Learning (CBL) can be aligned in order to describe the skills requirements for a Computer Security Incident Response Team (CSIRT).

Design/methodology/approach: This study is derived predominantly from literature reviews. An investigation of existing competency frameworks and competency standards was conducted. The concept of a Topic Map is subsequently introduced as a way of integrating competency frameworks with CBL in order to describe competencies within a CSIRT environment. The paper further discusses how these competencies may be mapped to job roles.

Practical implications: The use of a Topic Map will potentially assist in identifying the critical skills required to operate a CSIRT

Originality/value: There is little research on the integration of competency frameworks and competency standards. This paper introduces a conceptual model for mapping competency frameworks with CBL programs.

Keyboard - competency, SFIA, Cisco, competency frameworks, CSIRT, CERT, Topic Map

INTRODUCTION

Communication networks and information systems are necessary for economic and social development, thus computation and networking services are fast becoming universal utilities much like water and electricity (ENISA, 2006). Many organisations rely on Information Communication Technology (ICT) services to sustain critical business functions; these ICT services require specialised ICT skills that aid in supporting business objectives (Calitz, 2010; Killcrece, Kossakowski & Zajicek, 2003). Due to this reliance on ICT services, safeguarding of communication networks and information systems has become an increasing concern. The protection of information and information assets requires a specialised set of ICT skills. This includes global security initiatives such as the Computer Security Incident Response Team (CSIRT) that require special training or experience (ENISA, 2006).

Institutions such as the South African National Research Network (SANReN) and TENET require CSIRT services in order to protect their constituents from network related attacks. SANReN is a South African high-speed network dedicated to research traffic (SANReN, 2010). TENET on the other hand is a non- profit organisation that acts as an Internet Service Provider to research institutions. SANReN and TENET work closely together, SANReN builds the necessary network infrastructure, while TENET operates the network on behalf of SANReN. The latest collaboration between SANReN and TENET involves the two parties forming a partnership in order to establish and operate a CSIRT for the SANReN network called the SA NReN CSIRT. This research paper focuses on describing the context of skills needed in a CSIRT and will use the SA NReN CSIRT as a case study.

CSIRT

It has become an increasing challenging task to keep communication network and information security secure in today's globally interconnected world (Killcrece et. al., 2003). As such, many organisations use a CSIRT to respond to security incidents. CSIRTs are defined by many sources as;

> *Organisation or team providing services or support for preventing, handling and responding to computer security incidents. (Alberts, Dorofee, Killcrece, Ruefle & Zajicek, 2004)*
>
> *Team of IT security experts who respond to security incidents. It provides the necessary services to handle them and support constituents to recover from them. (ENISA, 2006)*
>
> *Is a service organisation responsible for receiving, reviewing and responding to computer security incident reports and activities. Its services are targeted for a defined constituency. (Killcrece et. al.., 2003a)*

Thus from the definitions discussed, a CSIRT can be described as an organized group of IT experts tasked with the responsibility of preventing, handling and responding to a constituency's computer security incidents. Currently there is no fixed framework for establishing a CSIRT across all organisations, because the establishment and operation of a CSIRT depends mainly on the type of services the CSIRT is planning on providing to its constituent (Alberts et al., 2004). Furthermore, due to the dynamic environment in which CSIRTs operate, no two CSIRTs can possess exactly the same set of services, policies and procedures (West-Brown et al., 2003). According to the Handbook for Computer Security Incident Response Teams, a starting point for establishing a CSIRT is describing what the CSIRT will do, who it will be done for, in what environment it will operate and in cooperation with whom (West-Brown et al., 2003). These are the main questions that should be addressed when setting up the requirements for a CSIRT. The SANReN and TENET CSIRT partnership is still at its planning stage and the SA NReN CSIRT has not been established. Therefore, it is imperative that the two partnering organisations work together outlining the mission, purpose and the constituency of the SA NReN CSIRT. For a CSIRT to be successful it is important to understand the needs of the constituent and to provide the appropriate services based on those needs (ENISA, 2006).

WHAT DO THEY DO?

A CSIRT can operate in a variety of ways and may have different requirements, responsibilities, functions and structures (Killcrece et. al., 2003b). What exactly a CSIRT does depends upon the services provided by the CSIRT to its constituency and the policies that have been put in place by the organisation (ENISA, 2006). There have been organisations that decide their CSIRT staff will deal only with incident handling while other organisation's staff implement further tasks such as incident analysis and response, vulnerability handling, intrusion detection, risk assessment, security and penetration testing (Killcrece et. al., 2003a). However, at a minimum, a CSIRT must at least provide implementation of incident handling (West-Brown et al., 2003). Therefore, a main objective of a CSIRT is to isolate, mitigate the effects of, disable and assist with recovery from an incident.

TYPES OF CSIRT

A CSIRT can operate in a hierarchical manner, coordinated by global and regional forums. This includes national CSIRTs followed by sector CSIRTs and finally individual company or organisational CSIRTs (West-Brown et al., 2003). The type of CSIRT may impact what personnel is hired and what personnel tools an organisation may decide to use. The constituencies that the CSIRTs serve may overlap at times (ENISA, 2010). For example, a national CSIRT may be servicing all sites in a specific country or all Internet users in specific country. Other CSIRTs may also exist within that country that service their own specific constituencies which may overlap with the national CSIRT. SA NReN CSIRT is a national South African incident response initiative that will encompass constituents at a national level. The SA NReN CSIRT may cooperate with other trusted CSIRTs. In cases where the SA NReN CSIRT overlaps with other CSIRTs in responsibility, there needs to be clear communication between the CSIRTs in order to negotiate and try to find a compromise of what is expected between them (ENISA, 2010).

CSIRT SERVICES

One of the main things that needs to be addressed when establishing a CSIRT is deciding on what services will be provided to the constituency (CERT, 2016). There are many services that can be provided by a CSIRT, each CSIRT is different and as a result will provide services based on their own mission, purpose and constituency needs (CERT, 2016). When hiring individual's organisations need to ensure that the candidates are capable of performing and producing the desired CSIRT services. There are three broad categories of CSIRT services which are categorised as reactive, proactive and security quality management services (ENISA, 2010).

- *Reactive* services these are the services that are taken to resolve or mitigate incidents as they occur. Reactive services form the core of CSIRT and are triggered by an event or request (Alberts et al., 2004).
- *Proactive* services refer to services that are put in place with the objective of preventing incidents from occurring in the first place, thus these services provide assistance and information to help prepare, protect and secure communication networks and information systems from anticipated attacks or events (CERT, 2016).
- *Security quality management* services are not directly linked to communication network or information security, they refer to services that are well-known and designed to improve the overall security of an organisation. These services can be provided by other areas of an organisation and are not necessarily CSIRT- specific (Killcrece et. al., 2003a).

To be effective, a CSIRT should address proactive and reactive issues (West-Brown et al., 2003). As discussed earlier, the type of services and the scope of the services provided by a CSIRT to its constituency depends largely on the mission and purpose of the CSIRT, as well as the service assets available, such as resources and capabilities of the organisation (Killcrece et. al., 2003b). The mission, purpose and service assets of the SA NReN CSIRT have been developed through a series of workshops between key SANReN and TENET stakeholders. It was decided that the service responsibilities for the SA NReN CSIRT be divided between the two parties. SANReN shall provide the proactive services and TENET shall provide the reactive services for the SA NReN CSIRT (SANReN, 2015).

Yet another contributing factor is the technology that is accessible to the organisation. A CSIRT must have the right mix of services, sufficient resources and capabilities, but they will always be limited to the technology that is accessible to them at any specific time. Thus technology constraints become a concern and organisations must ensure that they keep up to date with technology in order to operate the CSIRT in the most effective manner.

CSIRT PROCESSES and POLICES

Organisations usually have a set of defined policies and processes in place to ensure that the organisation is governed and operated in the proper way. Processes and Polices also assist employees perform tasks in a consistent manner with less risk of error, thus employees need to understand and apply process and policies as described by the organisation. ITIL describes policies as formally documented expectations and intentions (Hunnebeck, 2011). An alternative definition of a policy is the governing principle under which the team operates (West-Brown et al., 2003). A process is described as a structured set of activities designed to accomplish a specified objective (Hunnebeck, 2011).

1) Policies: In the context of a CSIRT, policies can be grouped into two sets of policies. Policies that are organisational specific (corporate policies) and policies that are CSIRT specific. Organisations may describe and implement specific sets of policies throughout their organisational activities. These policies are unique to each organisation and may be based on legal, geographic and strategic factors. The second category of policies are policies that are specific to the establishment and operation of a CSIRT such as incident reporting and request handling, data classification and prioritisation and communication (West-Brown et al., 2003). CSIRT specific policies may be similar among multiple organisation, whereas organisational specific policies are unique to each organisation. Organisational specific policies dictate the nature of CSIRT specific policies. Organisations must ensure that there is a seamless flow between all the policies. In the context of SA NReN, there is added complexity in policy implementation, as the CSIRT services for the SA NReN CSIRT are separated between two organisations. It is critical that these organisational specific and CSIRT policies do not conflict with one another.
2) Processes: Processes are implemented to minimise errors by providing standardised response (Cichonski et al., 2012), thus improving the overall quality and time required to perform an incident response (ENISA, 2006). Processes should be driven by an organisation and integrated into other processes. There should be defined accountability via assigned roles and responsibility (Alberts et al., 2004); be supported by polices process should be repeatable (Cichonski et al., 2012); be

documented and reviewed (Smith, 1994). In order for a team to operate effectively, there needs to be well-defined policies, procedures and service processes (West-Brown et al., 2003). One of the first issues a team should address in its policies and procedures is the level of service it's willing or able to provide to different parties (West-Brown et al., 2003).

CSIRT ROLES

The staff roles, responsibility and accountability need to be defined for a CSIRT. The actual assignment will depend largely on the structure of the host organisation. SANReN and TENET have agreed that the TENET Chief Technical Officer (CTO) shall serve as the CSIRT manager and recruit a system administrator with 50% time allocated to CSIRT activities. SANReN shall commit 1.5 full-time equivalent senior net- work engineering and information security specialists will be recruited and manage the proactive SA NReN CSIRT services.

CSIRT SKILLS AND RESPONSIBILITY LEVELS

People are an important asset to an organisation and represent both a resource and a capability (Hunnebeck, 2011). Cannon further expresses the importance of people as an asset by stating that if capabilities are the capacity for action, people assets are the actors. Finding the right people who possess the appropriate experience, skills and training is one of the challenges when establishing a CSIRT (Killcrece et. al., 2003b).

The Dutch Society for Information Security (PvIB) has raised its concerns about the difficulty in comparing certifications and qualifications with job titles of information security professionals. As a result of this, PvIB has indicated that information security professionals are unable to clearly identify their knowledge and experience on the basis of their job title and supporting certificates (Spruit & van Noord, 2014). As it turns out, this has become a common problem among Information Communication Technology (ICT) professionals in general. There are so many different perspectives and so much diversity in skills expectations, it is difficult to implement a one shoe fits all response to this question. Generally, it is expected that a professional is an individual that

- Has sufficient knowledge and skill within a discipline.
- Is accepted by the community, through certification, licensing or recognition as someone who Is capable of practising in the disciple.
- Operates with authority and responsibility.
- Adheres to a strict code of ethics.
- Provides service to the community.

This raises the question 'Does this definition of a professional adhere to ICT professionals?' (Von Konsky, 2008). Cameron states that the ICT sector is facing a serious skills shortage and many attempts have been made to address this problem. Organisations struggle to find suitable individuals for specific ICT roles (Cameron, 2008). Thus, a common taxonomy for describing competency was proposed by several parties (Grant, 2006). These skills competency frameworks focused on describing the necessary attributes an individual needed to have to be recognized as being competent of a skill (Grant, 2006). The Skills Framework of the Information Age (SFIA) and European e- Competency Framework (e-CF) are the predominant competency frameworks in ICT (Rudzajs et al., 2010), the National Initiative for Cybersecurity Education (NICE) National Cybersecurity Workforce Framework specialises on defining competency specifically within cybersecurity. SFIA, which was developed by the British Computer Society, has become the most widely accepted of these frameworks and has the most complexity. It is recognized in over 200 countries and is being implemented by thousands of organisations for managing their ICT skills resources (SFIA, 2015). SFIA is a skills competency framework that defines a collection of ICT skills. It is further described by the SFIA Foundation as "A common language for skills in the digital world".

WHAT IS COMPETENCY?

To fully understand the context and complexity of the properties of SFIA it is important to have a firm understanding of what competency is and why it is used as the main attribute in assessing an individual's skills. Competency is what a person is required to do and under what conditions. Competency involves the ability to draw knowledge, skill, attitude and values required to perform activities to a specified standard as illustrated in Figure 1 (European Committee for Standardization, 2014). Competency standards are the result of functional analysis of a sector or particular domain (European Committee for Standardization, 2014). Competency standards provide the tools for transforming the sector and cover the whole sector area. Competency standards can be utilised to create frameworks for assessing competency within a given sector (Serge Ravet, 2013). According to SFIA and e-CF, competency forms the core components of a job role, but do not represent a job role holistically (SFIA, 2015; European Committee for Standardization, 2014).

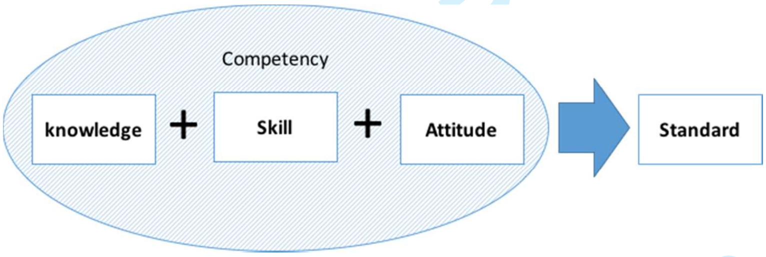


Figure 1: underlining blueprint of the components in competency

SFIAS APPROACH TO COMPETENCY

SFIA can be used as a reference model for managing the skills in an organisation, SFIAs classification of competency is based on the Bloom Taxonomy model (Rudzajs et al., 2010). The Bloom Taxonomy model consists of three domains of learning. The Cognitive domain refers to the different stages of knowledge, Affective domain refers to different stages of attitude and Psychomotor domain, which refers to the different stages of a skill during learning (Atherton, 2016). These Bloom Taxonomy domains strongly correlate with competency (ability draw knowledge, attitude and skill). SFIA characterises these components (knowledge correlates with Cognitive domain, attitude correlates with

Affective domain and skill correlates with Psychomotor domain) according to the context of a job role. These are Professional skills (competency of a skill at a described level), Behavioural skills (attitude towards an organisation, influence being described as a big factor) and Knowledge (knowledge of the sector based on sector standards) these traits are supported by qualification and/or experience (SFIA, 2015).

Competency framework such as SFIA allow organisations to map a person's competency against a common reference framework (SFIA, 2015). This framework is multi-dimensional and consists of two axes. One of the axes divides skill traits (knowledge, professional skills and behavioural skills) into skills responsibility which are '*Autonomy*', '*Influence*', '*Complexity*' and '*Business skill'*. The other axis describes the level of responsibility that should be given to a specific skill at a specific level of depth. SFIA describes seven of these levels of responsibility (Von Konsky, 2008).

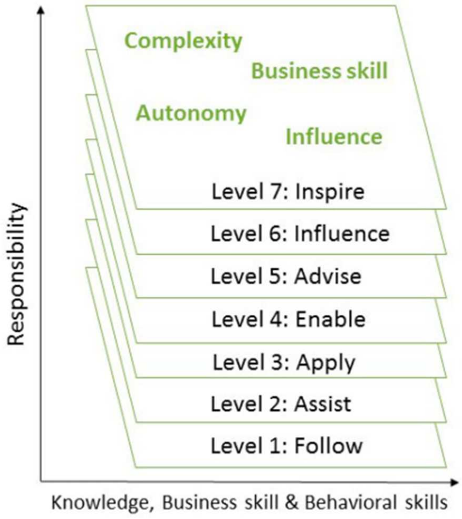


Figure 2: SFIA Dimensions

Each of the skills described in SFIA consist of the level of responsibility the skill is applicable in, and the amount of autonomy, complexity, influence and business skill required for each level of responsibility described (SFIA, 2015).

The SFIA skills framework does not attempt to address all skills that may be held by ICT professionals nor does it describe every competency in a skill in deep detail (SFIA, 2015). Instead, the SFIA framework can be regarded as a high-level overview of the core competency of ICT skills (SFIA, 2015). SFIA competency levels do not translate to job role, but rather they can be used as components of a job role. For example, the SFIA skill incident management does not represent the complete content of an Incident Manager job role. Competencies can be combined to represent the core content of a job role and a single competency can be assigned to multiple job roles (SFIA, 2015). In addition, SFIA competencies do not try to replace organisation competencies, instead they work alongside core organisational competencies as a supplementary resource (SFIA, 2015). An organisation may have a specific set of core competencies, along with the SFIA competencies. Furthermore, each individual within the organisation may have their own list of competencies they consider or desire as their own. Thus competency can be viewed from two perspectives which are illustrated in figure 3. On one hand, there is Competency Management which deals with the defining, recruiting and maintaining of competencies in an organisation allowing organisations to select specific competencies from the framework and match them to projects that are being planned or implemented (Streater et. al., 2012). On the other hand, there is Competency-Based Learning (CBL) which is based on competency standards. As mentioned earlier, individuals in an organisation may be pursuing their own career path and this may involve them selecting their own set of competencies from the framework.

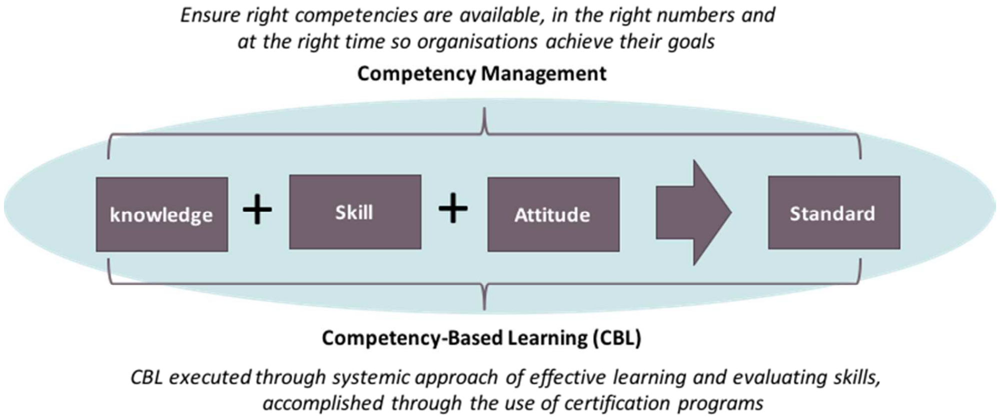

Ensure right competencies are available, in the right numbers and at the right time so organisations achieve their goals
Competency Management
knowledge
+
Skill
+
Attitude
Standard
Competency-Based Learning (CBL)
CBL executed through systemic approach of effective learning and evaluating skills, accomplished through the use of certification programs

Figure 3: Competency Management and Competency-based learning

IDENTIFYING SKILLS IN A CSIRT

Skills and knowledge in a CSIRT should be distributed amongst the team (ENISA, 2010). Having well-defined descriptions that include a list of the roles and responsibilities for each of the CSIRT positions along with the necessary skills, experience, educational background and/or certifications and clearance required can be a helpful tool in identifying and hiring the right staff (Killcrece et. al., 2003b). Currently, SANReN and its affiliated partners are evaluating candidates' skills based on rigid job role specifications that do not encompass competencies as a whole. This limits an organisation's flexibility over people's skills, as a job role may be based on specific tasks that will be carried out and may not consider other skills a candidate may have that the organisation may find useful at a later stage. Competency frameworks can be used as a tool to help identify the right staff to hire for the SA NReN CSIRT. In a CSIRT service, the SFIA framework can assist SANReN and TENET with Competency Management strategy

- The framework can be used by SANReN and TENET to identify the necessary competencies required to operate the SA NReN CSIRT and the level of responsibility that should be given to a competency given the depth of the skill. It can also assist in identifying the current level of competencies that already exist within the organisation.

- The framework can assist the organisation in selecting the appropriate candidates for the SA NReN CSIRT team. This reduces the risk of selecting a candidate that is competent at a skill, but not at the required level.
- The framework can assist with maintaining the demand for specific skills in the CSIRT, this includes training employees to meet the level of competency required by the CSIRT.

Since SFIA is a high-level framework it does not describe competencies in detail especially in network security, thus there is an opportunity to fill this gap by using SFIA with CBL that provides a detailed overview of the required competencies. CBL is the second aspect of competency, it is described as a structured approach to learning and assessment directed toward assisting individuals to acquire knowledge, skills and attitude required to perform an activity to a specified standard [24]. Cisco is recognised as a worldwide leader in network security. Cisco's deep understanding of industry and emerging technology has enabled them to set network security standards and best-practices which are recommended and practiced on an international scale (Lammle, 2013). Cisco focuses on developing CBL programs through certification. Certification establishes a standard of competency in a specific sector and job roles (Al-rawi, 2006). The Cisco certification program is one of the most widely used CBL program in the network security sector. The SFIA Framework provides a common overview of ICT competencies, but does not address network security competencies.

CISCOS APPROACH TO COMPETENCY-BASED LEARNING

Cisco is an international corporation that provides a wide range of certifications across a multitude of interrelated network disciplines. These include network designing, network routing and switching and network security (Cisco Systems, 2016). Cisco certification consists of a hierarchy of levels that are correlated with the competencies of each certification path, these levels in ascending order are Entry, Associate, Professional, Expert and Architect. These certificate levels are linked to one another. An example of this is that before an individual can be recognised as a Cisco Certified Network Professional (CCNP) security they will have hold a valid Cisco Certified Network Associate (CCNA) security certificate. Thus, an individual must possess competencies of the previous level before attempting the next level (Cisco Systems, 2016).

Cisco assesses certification based on competency examinations that test an individual's level of competency in order to receive certification. Candidates who pass the required examinations go on to receive certification correlated to that examination. Certification can have one or more examinations as pre-requisite and multiple certifications can have the same examination as a pre-requisite. Each of the examinations seeks to test an individual at a certain set of competencies. Therefore, similar topics can be discussed across multiple examinations, but not necessarily at the same level of depth or complexity (Cisco Systems, 2016). Individuals can pick sets of competencies based on the Cisco certification path that they would like to do, hence this is why CBL reflects the second perspective of competency described earlier.

COMPLEXITY OF DESCRIBING COMPETENCY

The attributes of competency consist of knowledge, attitude and skill (European Committee for Standardization, 2014).

- Knowledge - (one of the traits used in the SFIA competency framework) consists of different levels of depth, Bloom Taxonomy describes two sets of cognitive thinking. Lower Order thinking such as recognising, understanding and being able to apply concepts and Higher Order thinking include analysis, evaluation and the creation of new concepts (Atherton, 2016).
- Attitude - (another of the traits used in the SFIA competency framework) reflect on an individual's behavioural habits towards something, this also is described by Bloom Taxonomy in different levels of depth. Receiving is recognized as the lowest form of attitude and organisation attitude by value is placed as the highest (Atherton, 2016).
- Skills - (this is also a trait used in the SFIA competency framework) which is describes an individual's proficiency at an activity, Bloom Taxonomy uses its Psychomotor domain which describes skills in terms of learning complexity. This includes the unconscious incompetency of a skill right through to the unconscious competency of a skill (Atherton, 2016).

It is quite clear that the context of competency is very complex, and is something that must be considered when evaluating an individual's competency. SFIA states that qualification or certification alone does not justify competency (SFIA, 2015). Cisco uses certifications to justify competencies in network security. While these competencies may be important to developing CSIRT roles, an organisation must consider more than just technical knowledge when reviewing a candidate (Cichonski et al., 2012). Thus, the SFIA framework alone is not enough to develop the SA NReN CSIRT job roles and neither is certification on its own. This provides the opportunity to map a competency framework together with CBL. In these case SFIA and Cisco where chosen as analogies for describing this mapping between competency frameworks and CBL.

SFIA is described as a durable framework because although technology, jobs and market terminology within the ICT environment changes rapidly, the SFIA framework is still able to describe competencies comprehensively. This is because SFIA does not describe any product or technology-specific skills or knowledge, industry experience or qualifications (SFIA, 2015). Cisco on the other hand, is a product CBL that is based mainly on the operation of Cisco technology, and, although the Cisco body of knowledge caters for topics that may not be Cisco specific, the Cisco framework is a technology based vendor specific framework.

A similarity between the SFIA and Cisco frameworks is how levels of competency are assessed. Both SFIA and Cisco follow a criterion-referenced assessment. In criterion assessment, an individual is either seen as competent or not ye (Green, 2002). A difference in ideology is how levels of competency are viewed by the framework. SFIA describes what competencies an organisation may use in Competency Management and levels are seen as equal in stature. For example, incident management at level 6 is not seen as superior to incident management at level 5. They are seen as two different sets of competencies that require different forms of responsibility. Cisco certificate levels on the other hand show elements of hierarchy and are based on CBL. For example, an individual holding an Expert certification is seen as superior to other individuals who may have Entry, Associate or Professional certification.

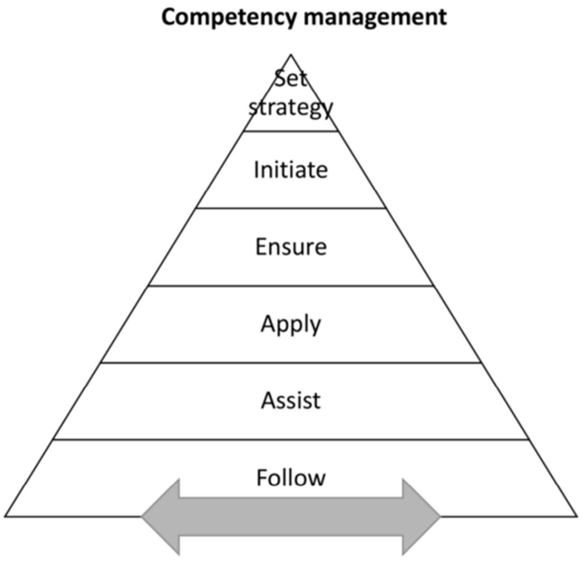


Figure 4: SFIA Levels

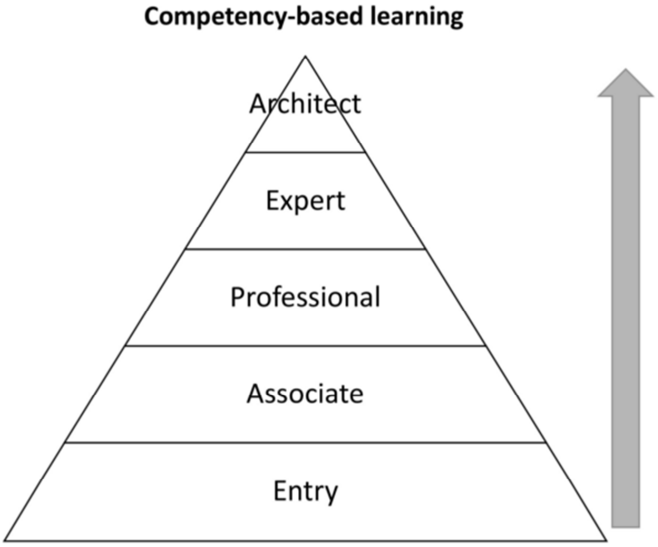


Figure 5: Cisco levels

The SFIA framework and Cisco certification framework have been identified as the frameworks of interest in this paper. The two frameworks describe two different viewpoints on how to interpret competency. SFIA provides a high-level overview of competency most useful to organisations in aiding with Competency Management. Cisco on the other hand is a more detailed set of competencies that is geared for individuals building competency in a specific discipline such as network security. Grant describes some criteria for how competency frameworks and CBL can be merged together using a Topic Map (Grant, 2006). Topic Maps are an ISO standard (ISO/IEC 13250) for describing knowledge structures and associating them with information resources (Topicmaps.org, 2016). Topic Maps provide the meta-model on which a completely flexible application model can be built, such as a meta-framework (the mapped model of competency framework and CBL).

Thus, a Topic Map can be used to create a meta-framework tool for defining and describing skills competencies within a CSIRT, such as the SA NReN CSIRT. The Topic Map will possess characteristics from both Competency Management and CBL. Topic Maps can serve not only as a guide to locating resources for the expert, but also as a way for experts to model their knowledge in a structured way. This allows non-experts to grasp the basic concepts and their relationships before diving down into the resources that provide more detail (Microsoft, 2015). Thus the Topic Map can be used by both ICT professionals and non-ICT departments, such as the Human Resource Department, to define specific competencies as required in the organisation and also provides a channel on how individuals can be trained within each competency defined. Each CSIRT has a unique mix of services that it provides to its constituency. As a result, the competency required in a CSIRT will differ amongst organisations. Topic Maps provide the facet feature which allows a Topic Map to be filtered down to specific resources based on specific values called facet value (Microsoft, 2015). An individual organisation can set up facet values to describe competencies within the context of specific job roles.

TOPIC MAP IN CSIRT

The use of a Topic Map will assist in identifying the critical skills required to operate a CSIRT, it will then assist in allocating the right amount of responsibility based proficiency of skill as opposed to job role. Organisations will be able to select their own mix of skills from the Topic Map based on the services they wish to provide in their CSIRT, such as incident management, problem management, information security and security administration. Each of the Topic Map skills consist of levels of responsibility as described in the context of SFIA. Some responsibilities in a CSIRT may be shared amongst multiple roles and may be performed by different people depending on the situation (Alberts et al., 2004). Thus, organisations need to ensure that the right level of responsibility is given to individuals who not only demonstrate competency of a skill, but who demonstrate this competency at a desired level. The Topic Map would include the capability of defining competencies and also being able to point to specific Competency-Based Learning resources. This would assist in answering the questions ’What skills do I need?’ ’How much responsibility should I attach to the skills?’ and ’How do I train individuals to reach that standard?’. During the selection and aggregation of competencies, the organisation can attach facet values to desired skills in order to create job roles. Different job roles may have similar skills requirements, use of the facet feature allows the Topic Map to identify the relationship between job roles, which gives the organisation the power to filter between different CSIRT roles. Figure 6 illustrates how skills competency relate to other components of a CSIRT. The image further illustrates the significance of using a Topic Map to develop job roles within a CSIRT.

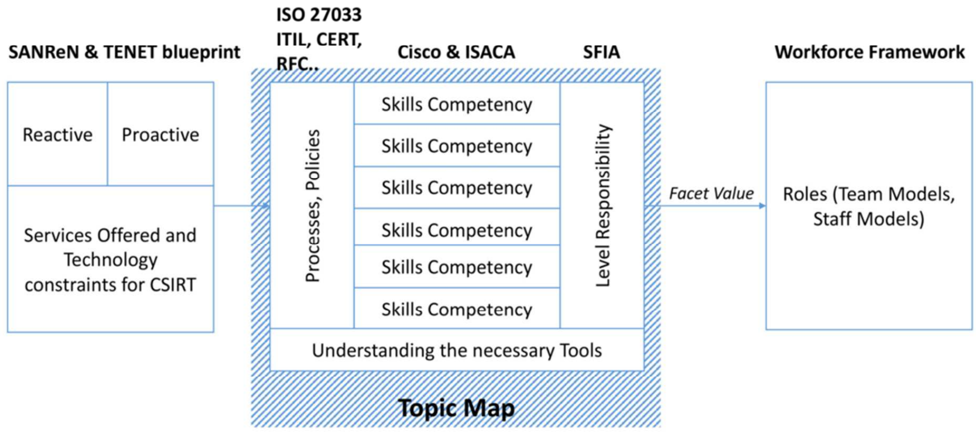


Figure 6: Incorporation Topic Map into CSIRT

CONCLUSION

The assessment of skills competency is critical to the success of a CSIRT. The current skills competency frameworks do not address competency holistically within the ICT discipline. This limits the available options organisations have when assessing employee and candidates for CSIRT job roles. The use of a Topic Map is proposed as an approach that encompasses skills competency holistically. Topic Map features, such as the facet value, provide flexibility in how skills can be aggregated into a Topic Map to create job roles. This would allow for the assessment of the current skills of a candidate for any specific job, against both higher (overview) level competencies, and more technical (skills-based) competencies. Such Topic Maps can also meaningfully contribute towards the management of continuous professional development of employees in the fast changing network- and network security domain.

REFERENCES

Al-rawi, A. (2006), “Integrating IT Certifications in Networking Courses: Cisco CCNA versus CompTIA Network” available at: https://peer.asee.org/integrating-it-certifications-in-networking-courses-cisco-ccna-versus-comptia-network.pdf (accessed 30 April 2016)

Alberts, C., Dorofee, A., Killcrece, G., Ruefle, R. and Zajicek, M. (2004), “Defining incident management processes for CSIRTs: A work in progress,”, *Carnegie Mellon University*, Tech. Rep.

Atherton J. S. (2016), “Learning and teaching. blooms taxonomy”, available at: http://www.learningandteaching.info/learning/bloomtax.htm, (accessed 5 April 2016).

Calitz, A. P. (2010), "A model for the alignment of ICT education with business ICT skills requirements", Doctoral thesis, Nelson Mandela Metropolitan University, available at: contentpro.seals.ac.za/iii/cpro/app?id=2288969262795013&itemId...def

Cameron, B. H. (2008), "Enterprise systems education: New directions challenges for the future", *AMCIS2008*, available at: http://aisel.aisnet.org/amcis2008/119.

CERT. (2016), "CSIRT services", Available: http://www.cert.org/incident-management/services.cfm? (accessed 24 April 2016).

Cichonski, P., Millar, T., Grance, T. and Scarfone, K. (2012), "Computer security incident handling guide," NIST, Special Publication 800-61. Revision 2.

Cisco Systems. (2016), "Training certifications," 2016. available: http://www.cisco.com/c/en/us/about.html (accessed 12 April 2016)

ENISA. (2006), "A Step-by-Step Approach on How to Set up a CSIRT", available at: https://www.enisa.europa.eu/publications/csirt-setting-up-guide/at.../fullReport.

ENISA. (2010), "Good practice guide for incident management", available at: https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management/at_download/fullReport.

European Committee for Standardization. (2014), "User guide for the application of the European e-Competence Framework 3.0", available at: http://www.ecompetences.eu/wp-content/uploads/2014/02/User-guide-for-the-application-of-the-e-CF-3.0_CEN_CWA_16234-2_2014.pdf (accessed 20 April 2016)

Grant, S. (2006), "Frameworks of competence: common or specific?", *International Workshop in Learning Networks for Lifelong Competence Development,* March 3031 Sofia Bulgaria, pp. 111–116.

Green, S. (2002), "Criterion Referenced Assessment as a Guide to Learning - the Importance of Progression and Reliability," Association for the Study of Evaluation in Education in Southern Africa International Conference, pp. 1–15, available at: http://www.cambridgeassessment.org.uk/Images/109693-criterion-referenced-assessment-as-a-guide-to-learning-the-importance-of-progression-and-reliability.pdf (accessed 24 April 2016)

Hunnebeck, L. (2011). "ITIL service design", *London: The Stationary Office* (TSO).

Killcrece, G., Kossakowski, K.-P., Ruefle, R. and Zajicek, M. (2003), "State of the practice of computer security incident response teams (CSIRTs)," *Carnegie Mellon Software Engineering Institute.*

Killcrece, G., Kossakowski, K.-P., Ruefle, R. and Zajicek, M. (2003), "Organizational models for computer security incident response teams (CSIRTs)," *Carnegie Mellon Software Engineering Institute.*

Lammle, T. (2013), "CCNA Routing and Switching Study Guild", John Wiley Sons

Microsoft. (2015), "An introduction to topic maps," available at: https://msdn.microsoft.com/en-us/library/aa480048.aspx. (accessed 20 April 2016)

National Volunteer Skills Centre. (2003), "A Guide to Writing Competency Based Training Materials*", Melbourne Vic, Australia*, available at https://www.k4health.org/sites/default/files/GuidetoWritingCompetencyBasedTrainingMaterials.pdf (accessed 12 April 2016).

Rudzajs, P., Penicina, L., Kirikova, M. and Strazdina, R. (2010), "Towards Narrowing a Conceptual Gap between IT Industry and University," *Scientific Journal of Riga Technical University*. Computer Sciences, vol. 41, no. -1, pp. 9–16, available at: http://www.degruyter.com/view/j/rtucs.2010.41.issue--1/v10143-010-0019-5/v10143-010-0019-5.xml

SANReN. (2010), "Overview", available at: http: //www.sanren.ac.za/overview (accessed 20 April 2012).

SANReN. (2015), "Update on the SANReN CSIRT", available at: http://www.sanren.ac.za. (accessed 22 April 2016)

Serge Ravet. E. (2013), "Competency-based learning what is competency?", available at: http://transit.ea.gr/ (accessed 1 April 2016).

SFIA Foundation. (2015), "SFIA6 The complete reference guide", available at: https://www.sfia-online.org/en/sfia-5/complete-reference/view (accessed 10 April 2016)

Smith, D. (1994), "Forming an Incident Response Team," *FIRST Annual Conference proceedings.* AUSCERT, pp. 1–37.

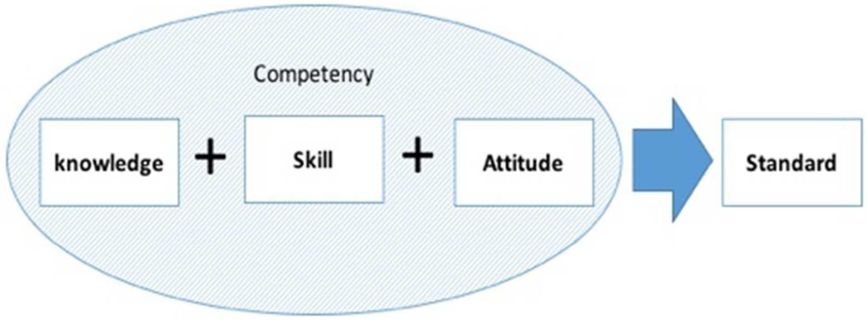
Spruit, M., and Van Noord, F. (2014) "Job Profiles for Information Security".

Streater, K., Atkins, J. and McLaren, R. (2012), "Introduction to SFIA in LD and Workplace Learning, Ron McLaren", BCS Learning and Development Specialist Group.

Topic Maps. (2016), "Standards", available at: http://www.topicmaps.org/standards/ (accessed 20 April 2016).

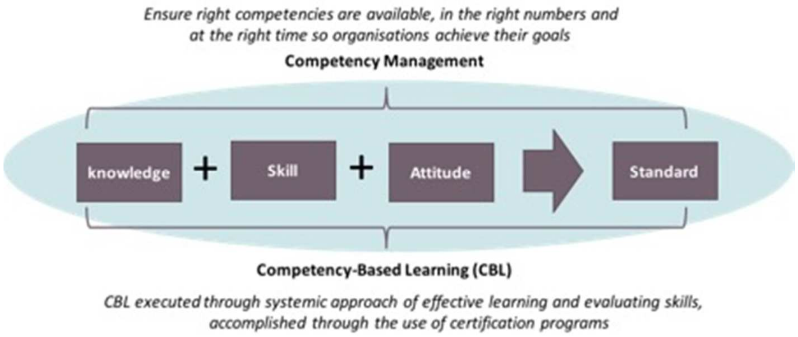
Von Konsky, B. R. (2008), "Defining the ICT profession: A partnership of stakeholders", *21st Annual Conference of the National Advisory Committee on Computing Qualifications*, pp. 15–22, available at: http://www.citrenz.ac.nz/conferences/2008/15.pdf

West-Brown, M. J., Stikvoort, D., Kossakowski, K.-P., Killcrece, G., Ruefle, R. and Zajicek, M. (2003), "Handbook for Computer Security Incident Response Teams (CSIRTs)", 2nd ed. *Carnegie Mellon Software Engineering Institute.*



Underlining blueprint of the components in competency

182x66mm (72 x 72 DPI)


Ensure right competencies are available, in the right numbers and at the right time so organisations achieve their goals
Competency Management
knowledge
+
Skill
+
Attitude
Standard
Competency-Based Learning (CBL)
CBL executed through systemic approach of effective learning and evaluating skills, accomplished through the use of certification programs

Competency Management and Competency-based learning

159x70mm (72 x 72 DPI)

Appendix B

Focus Group Supportive Documents

Appendix B includes the supportive documents that were distributed during the Focus Group session.

1. Evaluation scenarios
2. Company X Competency Needs
3. Candidate Competency Profile
4. Topic Map for Network Security Competencies

Scenarios

1) Company X has decided to open a new branch in Port Elizabeth, you have been tasked with designing a job description for a Network Security Engineer.

   Resources for Activity: *NICE Framework, NICE-Cisco Topic Map and Company X competency needs list*

   a) Which tool provided better set of functions for creating job description in the most effective way?
   b) Topic map, Did the lower level competencies help in developing the job description?

2) A candidate has applied for the Network Security Engineer position, and the new task now is to evaluate is competency level against what is required for the position

   Resources for Activity: *NICE-Cisco Topic Map, Candidate competency profile and Network Security Engineer Job Description*

   a) Did the topic map help in determining the best course of actions for bridging the gap between what competencies are available and what competencies are required?

3) The company has recently opened a new job position for Network Security Manager, the company has decided to open the position to employees first before the public, you are tasked with evaluating how to upgrade the current level of competency possessed by employees, so they can meet the job position requirements

   Resources for Activity: *SFIA-Cisco Topic Map, Candidate competency profile and Network Security Manager Job Description*

   a) Did using the topic map help in evaluating the candidates against the job description?
   b) From a candidate position, did the topic map assist in determining what competencies are needed for future job pursuits

Candidate Competency Profile

Vuyolwethu Mdunyelwa

1. Skill in implementing, maintaining, and improving established network security practices
2. Skill in installing, configuring, and troubleshooting Local Area Network (LAN)
3. Skill in using network management tools to analyse network traffic patterns (e.g., simple network management protocol)
4. Knowledge of systems administration concepts
5. Skill in protecting a network against malware
6. Skill in configuring and utilizing hardware-based computer protection components (e.g., hardware firewalls, servers, routers)
7. Knowledge of root cause analysis for incidents
8. Knowledge of penetration testing principles, tools, and techniques

Candidate Competency Profile

Vuyolwethu Mdunyelwa

1. Information Security Level 6
2. Information Assurance Level 5
3. Network Design Level 5
4. Incident Management Level 5
5. Problem Management Level 5
6. Data Management Level 4

Company X Competency Needs

Perform the actual response activities which include recording, tracking and handling of incidents and analysing related information. Part of this role can include researching mitigation strategies and recovery options. Incident handler also coordinate the guidance (proactive or reactive) that will be provided to the constituency.

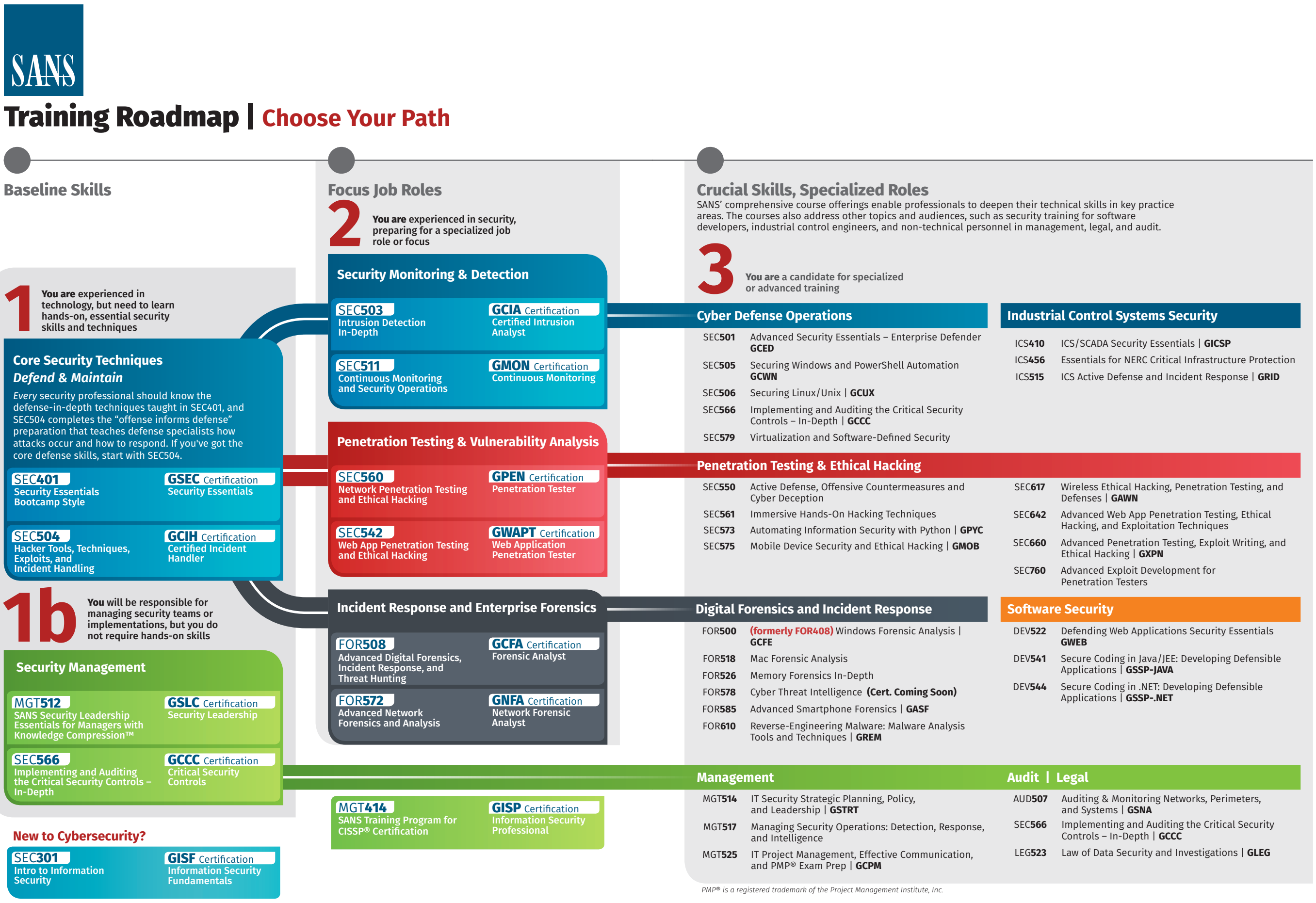
1. Skill in implementing, maintaining, and improving established network security practices
2. Knowledge of Virtual Private Network (VPN) security
3. Skill in protecting a network against malware
4. Knowledge of root cause analysis for incidents
5. Knowledge of encryption algorithms (e.g., Internet Protocol Security [IPSEC], Advanced Encryption Standard [AES])

Appendix C

Topic Map Supportive Documents

Appendix C includes additional documentation from literature and from the topic map system.

1. SANS GIAC certification roadmap poster
2. List of all topic instances in topic map.



SANS

Training Roadmap | Choose Your Path

Baseline Skills

1 **You are** experienced in technology, but need to learn hands-on, essential security skills and techniques

Core Security Techniques
Defend & Maintain

Every security professional should know the defense-in-depth techniques taught in SEC401, and SEC504 completes the “offense informs defense” preparation that teaches defense specialists how attacks occur and how to respond. If you've got the core defense skills, start with SEC504.

SEC**401** Security Essentials Bootcamp Style — **GSEC** Certification Security Essentials

SEC**504** Hacker Tools, Techniques, Exploits, and Incident Handling — **GCIH** Certification Certified Incident Handler

1b **You** will be responsible for managing security teams or implementations, but you do not require hands-on skills

Security Management

MGT**512** SANS Security Leadership Essentials for Managers with Knowledge Compression™ — **GSLC** Certification Security Leadership

SEC**566** Implementing and Auditing the Critical Security Controls – In-Depth — **GCCC** Certification Critical Security Controls

New to Cybersecurity?

SEC**301** Intro to Information Security — **GISF** Certification Information Security Fundamentals

Focus Job Roles

2 **You are** experienced in security, preparing for a specialized job role or focus

Security Monitoring & Detection

SEC**503** Intrusion Detection In-Depth — **GCIA** Certification Certified Intrusion Analyst

SEC**511** Continuous Monitoring and Security Operations — **GMON** Certification Continuous Monitoring

Penetration Testing & Vulnerability Analysis

SEC**560** Network Penetration Testing and Ethical Hacking — **GPEN** Certification Penetration Tester

SEC**542** Web App Penetration Testing and Ethical Hacking — **GWAPT** Certification Web Application Penetration Tester

Incident Response and Enterprise Forensics

FOR**508** Advanced Digital Forensics, Incident Response, and Threat Hunting — **GCFA** Certification Forensic Analyst

FOR**572** Advanced Network Forensics and Analysis — **GNFA** Certification Network Forensic Analyst

MGT**414** SANS Training Program for CISSP® Certification — **GISP** Certification Information Security Professional

Crucial Skills, Specialized Roles

SANS’ comprehensive course offerings enable professionals to deepen their technical skills in key practice areas. The courses also address other topics and audiences, such as security training for software developers, industrial control engineers, and non-technical personnel in management, legal, and audit.

3 **You are** a candidate for specialized or advanced training

Cyber Defense Operations

SEC**501**	Advanced Security Essentials – Enterprise Defender **GCED**
SEC**505**	Securing Windows and PowerShell Automation **GCWN**
SEC**506**	Securing Linux/Unix | **GCUX**
SEC**566**	Implementing and Auditing the Critical Security Controls – In-Depth | **GCCC**
SEC**579**	Virtualization and Software-Defined Security

Industrial Control Systems Security

ICS**410**	ICS/SCADA Security Essentials | **GICSP**
ICS**456**	Essentials for NERC Critical Infrastructure Protection
ICS**515**	ICS Active Defense and Incident Response | **GRID**

Penetration Testing & Ethical Hacking

SEC**550**	Active Defense, Offensive Countermeasures and Cyber Deception
SEC**561**	Immersive Hands-On Hacking Techniques
SEC**573**	Automating Information Security with Python | **GPYC**
SEC**575**	Mobile Device Security and Ethical Hacking | **GMOB**
SEC**617**	Wireless Ethical Hacking, Penetration Testing, and Defenses | **GAWN**
SEC**642**	Advanced Web App Penetration Testing, Ethical Hacking, and Exploitation Techniques
SEC**660**	Advanced Penetration Testing, Exploit Writing, and Ethical Hacking | **GXPN**
SEC**760**	Advanced Exploit Development for Penetration Testers

Digital Forensics and Incident Response

FOR**500**	(formerly FOR408) Windows Forensic Analysis | **GCFE**
FOR**518**	Mac Forensic Analysis
FOR**526**	Memory Forensics In-Depth
FOR**578**	Cyber Threat Intelligence **(Cert. Coming Soon)**
FOR**585**	Advanced Smartphone Forensics | **GASF**
FOR**610**	Reverse-Engineering Malware: Malware Analysis Tools and Techniques | **GREM**

Software Security

DEV**522**	Defending Web Applications Security Essentials **GWEB**
DEV**541**	Secure Coding in Java/JEE: Developing Defensible Applications | **GSSP-JAVA**
DEV**544**	Secure Coding in .NET: Developing Defensible Applications | **GSSP-.NET**

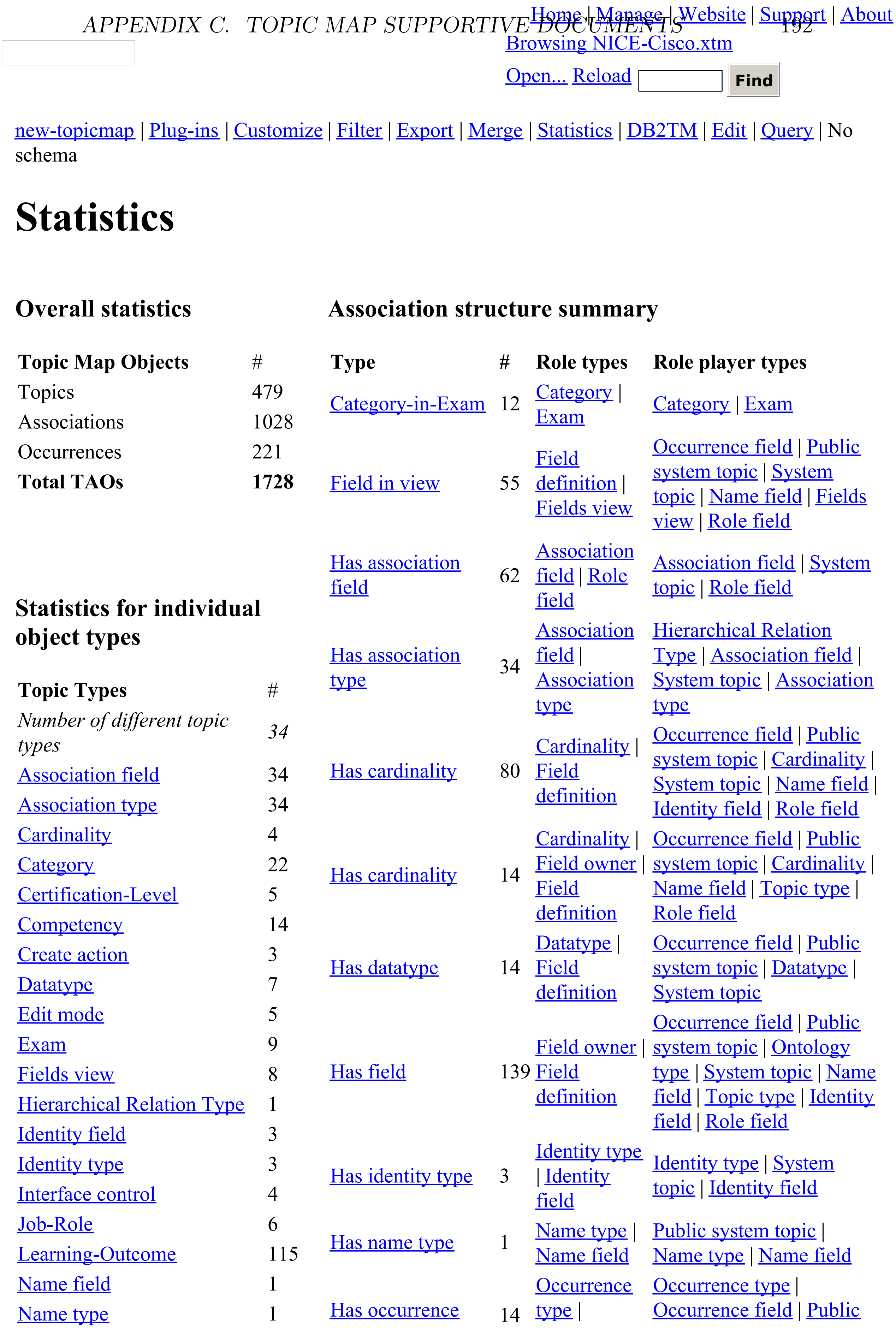
Management

MGT**514**	IT Security Strategic Planning, Policy, and Leadership | **GSTRT**
MGT**517**	Managing Security Operations: Detection, Response, and Intelligence
MGT**525**	IT Project Management, Effective Communication, and PMP® Exam Prep | **GCPM**

Audit | Legal

AUD**507**	Auditing & Monitoring Networks, Perimeters, and Systems | **GSNA**
SEC**566**	Implementing and Auditing the Critical Security Controls – In-Depth | **GCCC**
LEG**523**	Law of Data Security and Investigations | **GLEG**

PMP® is a registered trademark of the Project Management Institute, Inc.



Home | Manage | Website | Support | About
Browsing NICE-Cisco.xtm
Open... Reload Find

new-topicmap | Plug-ins | Customize | Filter | Export | Merge | Statistics | DB2TM | Edit | Query | No schema

Statistics

Overall statistics

Topic Map Objects	#
Topics	479
Associations	1028
Occurrences	221
Total TAOs	**1728**

Statistics for individual object types

Topic Types	#
Number of different topic types	*34*
Association field	34
Association type	34
Cardinality	4
Category	22
Certification-Level	5
Competency	14
Create action	3
Datatype	7
Edit mode	5
Exam	9
Fields view	8
Hierarchical Relation Type	1
Identity field	3
Identity type	3
Interface control	4
Job-Role	6
Learning-Outcome	115
Name field	1
Name type	1

Association structure summary

Type	#	Role types	Role player types
Category-in-Exam	12	Category | Exam	Category | Exam
Field in view	55	Field definition | Fields view	Occurrence field | Public system topic | System topic | Name field | Fields view | Role field
Has association field	62	Association field | Role field	Association field | System topic | Role field
Has association type	34	Association field | Association type	Hierarchical Relation Type | Association field | System topic | Association type
Has cardinality	80	Cardinality | Field definition	Occurrence field | Public system topic | Cardinality | System topic | Name field | Identity field | Role field
Has cardinality	14	Cardinality | Field owner | Field definition	Occurrence field | Public system topic | Cardinality | Name field | Topic type | Role field
Has datatype	14	Datatype | Field definition	Occurrence field | Public system topic | Datatype | System topic
Has field	139	Field owner | Field definition	Occurrence field | Public system topic | Ontology type | System topic | Name field | Topic type | Identity field | Role field
Has identity type	3	Identity type | Identity field	Identity type | System topic | Identity field
Has name type	1	Name type | Name field	Public system topic | Name type | Name field
Has occurrence	14	Occurrence type |	Occurrence type | Occurrence field | Public

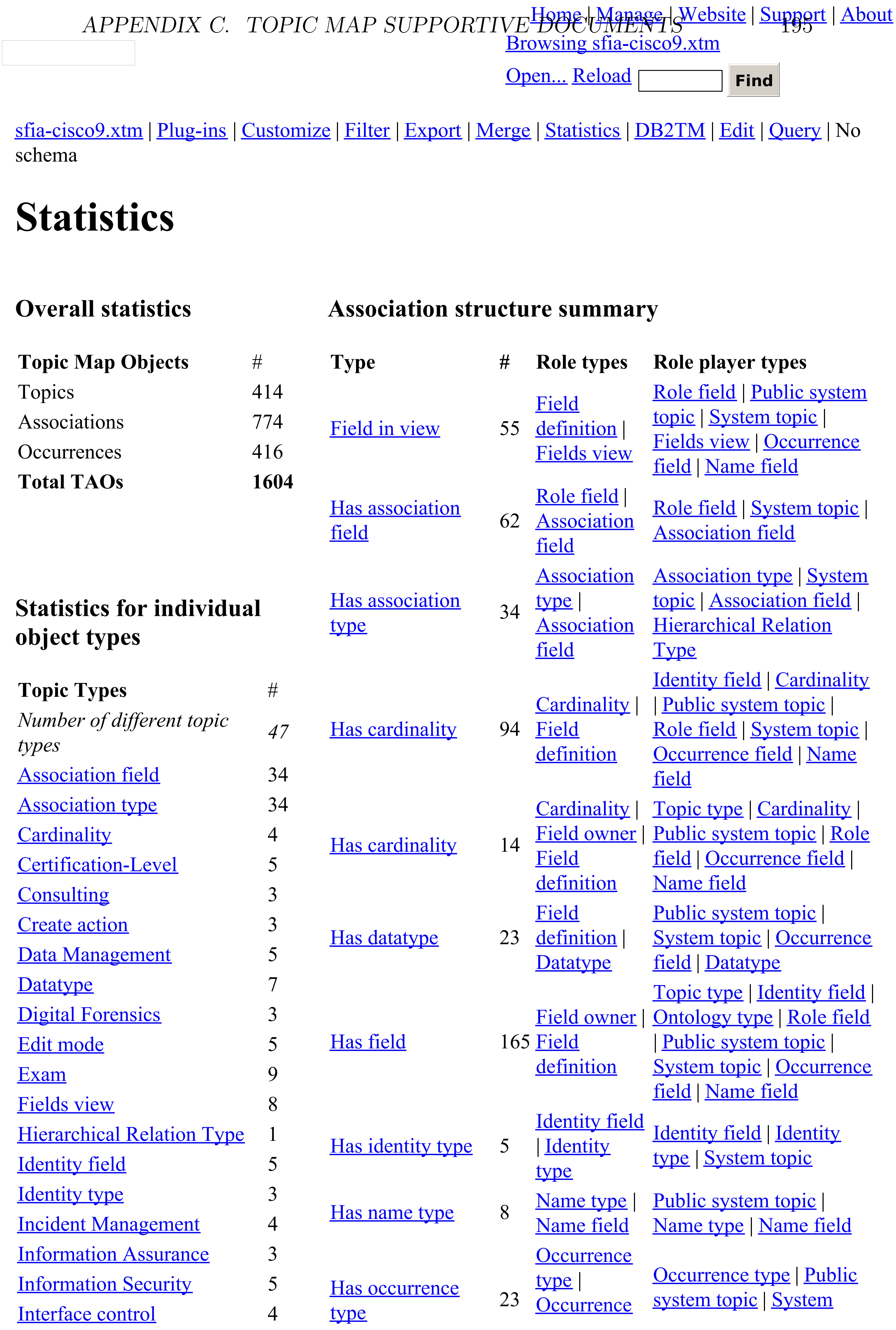
Occurrence field	14
Occurrence type	17
Ontology	2
Ontology type	5
Public system topic	33
Role field	62
Role type	5
Subordinate Role Type	1
Superordinate Role Type	1
System topic	168
Taxonomy-Level	6
Technology	55
Topic map	1
Topic type	35
View mode	4

Association Types	#
Number of different association types	*26*
Category-in-Exam	12
exam-for-certification	10
Field in view	55
Has association field	62
Has association type	34
Has cardinality	94
Has datatype	14
Has field	139
Has identity type	3
Has name type	1
Has occurrence type	14
Has role type	62
Is abstract	1
Is embedded view	5
Is hidden type	10
Is hidden view	1
job-competencies	6
Learning-Outcome-in-Category	114
lower-competencies	58
Superclass/subclass	5
Taxonomy-Level	113
Technology-type	128
Use edit mode	12
Use interface control	62
Use value view	7

type		Occurrence field	system topic | System topic
Has role type	62	Role type | Role field	Role type | Ontology type | System topic | Topic type | Subordinate Role Type | Role field | Superordinate Role Type
Is abstract	1	Topic type	System topic | Topic type
Is embedded view	5	Fields view	System topic | Fields view
Is hidden type	10	Ontology type	Occurrence type | Hierarchical Relation Type | System topic | Association type
Is hidden view	1	Fields view	System topic | Fields view
Learning-Outcome-in-Category	114	Learning-Outcome | Category	Learning-Outcome | Category
Superclass/subclass	5	Subclass | Superclass	System topic | Topic type
Taxonomy-Level	113	Taxonomy-Level | Learning-Outcome	Learning-Outcome | Taxonomy-Level
Technology-type	128	Learning-Outcome | Technology	Technology | Learning-Outcome
Use View mode	6	View mode | Field definition | Fields view	View mode | Public system topic | System topic | Fields view | Role field
Use edit mode	12	Edit mode | Field definition	Edit mode | Public system topic | System topic | Role field
Use interface control	62	Interface control | Field definition	Public system topic | System topic | Interface control | Role field
Use value view	7	Parent view | Child view | Field definition	Public system topic | System topic | Fields view | Role field
exam-for-certification	10	Certification-Level | Exam	Certification-Level | Exam
job-competencies	6	Job-Role | Competency	Job-Role | Competency
lower-competencies	58	Learning-Outcome | Competency	Learning-Outcome | Competency

Use View mode	6

Occurrence Types	#
Number of different occurrence types	*11*
Datatype locator	7
Description	11
Field order	173
Height	6
Maximum cardinality	2
Minimum cardinality	4
Ontology Version	1
Players query	3
Players types query	2
taxonomy-rank	6
Width	6



Home | Manage | Website | Support | About

Browsing sfia-cisco9.xtm

Open... Reload Find

sfia-cisco9.xtm | Plug-ins | Customize | Filter | Export | Merge | Statistics | DB2TM | Edit | Query | No schema

Statistics

Overall statistics

Topic Map Objects	#
Topics	414
Associations	774
Occurrences	416
Total TAOs	**1604**

Statistics for individual object types

Topic Types	#
Number of different topic types	*47*
Association field	34
Association type	34
Cardinality	4
Certification-Level	5
Consulting	3
Create action	3
Data Management	5
Datatype	7
Digital Forensics	3
Edit mode	5
Exam	9
Fields view	8
Hierarchical Relation Type	1
Identity field	5
Identity type	3
Incident Management	4
Information Assurance	3
Information Security	5
Interface control	4

Association structure summary

Type	#	Role types	Role player types
Field in view	55	Field definition | Fields view	Role field | Public system topic | System topic | Fields view | Occurrence field | Name field
Has association field	62	Role field | Association field	Role field | System topic | Association field
Has association type	34	Association type | Association field	Association type | System topic | Association field | Hierarchical Relation Type
Has cardinality	94	Cardinality | Field definition	Identity field | Cardinality | Public system topic | Role field | System topic | Occurrence field | Name field
Has cardinality	14	Cardinality | Field owner | Field definition	Topic type | Cardinality | Public system topic | Role field | Occurrence field | Name field
Has datatype	23	Field definition | Datatype	Public system topic | System topic | Occurrence field | Datatype
Has field	165	Field owner | Field definition	Topic type | Identity field | Ontology type | Role field | Public system topic | System topic | Occurrence field | Name field
Has identity type	5	Identity field | Identity type	Identity field | Identity type | System topic
Has name type	8	Name type | Name field	Public system topic | Name type | Name field
Has occurrence type	23	Occurrence type | Occurrence	Occurrence type | Public system topic | System

IT Management	3
Job Role	3
Name field	8
Name type	8
Network Design	2
Network Planning	2
Occurrence field	23
Occurrence type	24
Ontology	2
Ontology type	5
Penetration Testing	3
Problem Management	3
Public system topic	33
Research	5
Role field	62
Role type	6
Security Administration	6
SFIA levels	7
Subordinate Role Type	1
Superordinate Role Type	1
System Software	3
System topic	168
Systems Installation	5
Technical Specialism	3
Technology	38
Topic map	1
Topic type	49
View mode	4

Association Types	#
Number of different association types	*26*
competency-certification	3
competency-level	58
competency-technology	15
exam-certification	10
Field in view	55
Has association field	62
Has association type	34
Has cardinality	108
Has datatype	23
Has field	165
Has identity type	5
Has name type	8

		field	topic | Occurrence field
Has role type	62	Role field | Role type	Superordinate Role Type | Ontology type | Topic type | Role field | System topic | Subordinate Role Type | Role type
Is abstract	1	Topic type	Topic type | System topic
Is embedded view	5	Fields view	System topic | Fields view
Is hidden type	10	Ontology type	Association type | Occurrence type | System topic | Hierarchical Relation Type
Is hidden view	1	Fields view	System topic | Fields view
Superclass/subclass	21	Superclass | Subclass	Topic type | System topic
Use View mode	6	View mode | Field definition | Fields view	View mode | Role field | Public system topic | System topic | Fields view
Use edit mode	12	Field definition | Edit mode	Role field | Public system topic | System topic | Edit mode
Use interface control	62	Field definition | Interface control	Role field | Public system topic | System topic | Interface control
Use value view	7	Field definition | Parent view | Child view	Public system topic | Role field | System topic | Fields view
competency-certification	3	Competency | Certification-Level	Incident Management | Network Design | Certification-Level
competency-level	58	Competency | SFIA levels	Data Management | Incident Management | Network Design | Research | SFIA levels | Consulting | Network Planning | Digital Forensics | Security Administration | Information Assurance | Systems Installation | Penetration Testing | Information Security | System Software | Problem Management | Technical Specialism | IT Management
			Technology | Incident

Has occurrence type	23
Has role type	62
Is abstract	1
Is embedded view	5
Is hidden type	10
Is hidden view	1
job-competency	8
sfia-cisco-level	8
Superclass/subclass	21
technology-exam	2
Use edit mode	12
Use interface control	62
Use value view	7
Use View mode	6

competency-technology	15	Technology | Competency	Management | Network Design
exam-certification	10	Exam | Certification-Level	Exam | Certification-Level
job-competency	8	Competency | Job Role	Security Administration | Information Security | Problem Management | Job Role | Incident Management | Network Design
sfia-cisco-level	8	SFIA levels | Certification-Level	Certification-Level | SFIA levels
technology-exam	2	Exam | Technology	Exam | Technology

Occurrence Types	#
Number of different occurrence types	*18*
autonomy	7
business-skill	7
complexity	7
Datatype locator	7
Description	90
exam-number	8
Field order	240
Height	11
influence	7
lower-level-competencies	1
Maximum cardinality	2
Minimum cardinality	4
Ontology Version	1
Players query	3
Players types query	2
sfia-rank	7
website	1
Width	11