A Conceptual Model of an Information Security Domain Knowledge Base

Nadine Barrett-Maitland
University of Technology Jamaica
nadinemland@yahoo.com

Kweku-Muata Osei-Bryson
Virginia Commonwealth University
KMOsei@vcu.edu

Gunjan Mansingh
University of the West Indies Mona
gunjan.mansingh@uwimona.edu.jm

Paper Category: Research Paper

ABSTRACT

*Information Security breaches and threats continue to grow worldwide. Securing information systems issues persist despite the development of several Information security standards. The low adoption rate of these security standards is one of the main contributing factors for this growing problem***.** *As emerging economies seek to be a part of the digital economy it is prudent that they make information security a priority. The lack of effective Information Security Strategies in developing countries has resulted in these countries facing the problem of becoming targets for cyber criminals. In this research we present a Conceptual Model and a design of an Information Security Domain Knowledge Base (InfoSec DKB) that can assist in developing and managing information security strategies. This design is based on a combination of decision making, security and auditing frameworks, namely concepts of the Value Focused Thinking (VFT) approach used in decision making, the Guidelines for Management of IT security (ISO/IEC 27001), Control Objectives for Information and Related Technologies (COBIT).*

Keywords:

Information Security, Security Standards, Conceptual Model, VFT, COBIT, ISO/IEC

1. INTRODUCTION

Securing Information Systems continues to be a challenge for organizations and governments worldwide. Developing effective information security is important for emerging economies as they seek to be a part of the “information rich” and digital economy. For the past 50 years the world has been undergoing a second Industrial Revolution and the gains made in this period is attributed to the advent of Information Technology (IT) which can be described as pervasive as it touches every aspect of our lives (Podgor, 2004). This is laudable, however these technological advancements brings with it new and serious risks and as a result it has transformed the world into a "very dangerous place" (Kritzinger & von Solms, 2010; Wegener, 2007). In today's information age the internet is becoming the "defining technology" and there is a growing dependence on information & communication technologies. Growth in the use of these services can be reflective of development, however this has also created new vulnerabilities (Podgor, 2004) (Gercke, 2011; Kshetri, 2006). Information security is a major issue for developing states as finding solutions for cyber-security has proven to be major problem in these regions (Gercke, 2011). According to (Ali, 2011) 96% of secured internet severs worldwide are located in the Organization for Economic Co-Operation and Development (OECD) countries and only 15% of the world population lives in these countries. As pointed out by (Salifu, 2008) developing countries suffer more from Internet crime than developed countries because of inadequate technological infrastructure. There is also a growing need for developing countries to develop anti-cybercrime strategies that are in line with international standards (Gercke, 2009). Failure to plan for information security could result in an information system paradox; where there is increased spending on information security measures yet there is an exponential increase in losses due to security breaches (Hovav, Andoh-Baidoo, & Dhillion, 2007). There is a low adoption rate of the present information security standards with the most widely adopted standard ISO 27001 ranging between 6%– 26% (Susanto12 et al., 2011, 2012) . This low implementation rate is attributed to; complexity, certification requirements, lack of resources, difficulty understanding and implementing, culture, the lack of trained information security personnel just to name a few (Von Solms, 2005; Susanto12 et al., 2011, 2012).

How can the implementation of an Information Security Domain Knowledge Base (InfoSec DKB) assist businesses and governments in developing states to craft their information security strategies? This study is part of a research program that aims to develop methods, models and other artifacts that support the strengthening of the management of information security particularly in developing countries through the knowledge of an information security domain knowledge base. In an earlier study (N. B. Maitland & Osei-Bryson, 2014) we presented a framework and process for facilitating the development of Information Security Strategies appropriate to developing countries. In this paper we present a Conceptual Data model of the InfoSec DKB.

Currently there is a paucity of research on the impact of information security breaches in developing countries, including the Caribbean region. Survey of literature reveals that approximately 85% of the world's population lives in developing states however they are not well represented in academic literature as most studies focus on developed countries (Ali, 2011; N. Maitland, Barclay, & Osei-Bryson; Sutton & Payne, 1993).

This paper is organized as follows: In section 2, we examine the literature on information security, including advantages and disadvantages of two of the most widely adopted information security standards – COBIT and ISO 27001 (Susanto12, Almunawar, & Tuan, 2011, 2012), and also discussion of the rate of adoption of these standards. In the subsequent sections the design steps for the development of the InfoSec DKB, the developed Conceptual Data model and the preliminary results followed by conclusion and future studies are presented.

2. CONCEPTUAL FOUNDATIONS

In this section we look at the benefits of knowledge management in building the proposed domain knowledge and also present frameworks that will be examined to build the proposed InfoSec DKB.

2.1.1 KNOWLEDGE MANAGEMENT

Knowledge management is the process of communicating tacit ("cognitive and technical elements") and explicit (articulated, codified and communicated") knowledge acquired and organized systematically so that it can be used more effectively and productively (Alavi & Leidner, 2001). Building organizations' "core" competence is tied up in identifying and managing important knowledge and making it available to the authorized user at the right time (Kwan & Balasubramanian, 2003; Rao, Mansingh, & Osei-Bryson, 2012). Process-related knowledge can be proactively delivered in its most correct form to the process performer and can be found in things such as documents, experts and help files just to name a few (Jung, Choi, & Song, 2007). Knowledge that is associated to a process and is "codifiable" can be broken down into rules or related courses of action and can result in accurate directions as it relates to procedures that should be followed (Turner & Makhija, 2006). This process- related knowledge is very important in building the proposed InfoSec DKB as codified knowledge will be taken from the ISO 270001 and the COBIT standards and will be distilled along with the VFT approach to produce a comprehensive and robust domain knowledgebase for information security.

2.1.2 SECURITY FRAMEWORKS

As organizations and governments worldwide try to combat the evolving IS problem, several information security frameworks have been proposed as information security breaches continues to increase (Susanto12 et al., 2012) . Security governance guidelines such as control Objectives for information and related technology (COBIT), the Capacity Model for security (CMM-SEC), Guidelines for Management of IT security GMITS ISO/IEC 27001, BS7799, PCIDSS, COSO, ITIL, OPM3, PRINCE2, PMMM are all guidelines designed to help in IT governance with the primary goal being IS (Blum, 2006; Njenga & Brown, 2008; Susanto12 et al., 2012). Many of these standards are not well adopted for several reasons with the leading cause being complexity such as; difficulty of adoption with COBIT, ISO/IEC 27001, BS 7799, PCIDSS and ITIL leading the way (Susanto12 et al., 2012). The COBIT and ISO/IEC 27001 frameworks are the most widely adopted standards and will be presented below.

2.1.2.1 THE COBIT FRAMEWORK

The COBIT Framework is a well-researched and documented body of knowledge that is reflective of expert opinions. It is designed as a guide that businesses and organizations can use to manage their IT resources effectively (Charuenporn & Intakosum, 2012; Hojaji & Shirazi, 2010). The COBIT control objectives cover all aspects of the information “ecology” of an organization and are referred to as very “comprehensive” framework (Hojaji & Shirazi, 2010; Joseph Martin & CISA, 2003; Mamaghani, Samizadeh, & Saghafi, 2011). The COBIT framework is a set of 34 high-level control objectives in the management of information technology. The 4 main areas of focus are “planning and organizing”, “Acquisition & implementation”, delivery and support”, and “monitoring and evaluation” (Joseph Martin & CISA, 2003; Mamaghani et al., 2011). Adopting the COBIT framework will provide a well-defined and consistent framework that decision makers can use to reduce the communication gap between control requirements, technical issues and business risks (Lainhart IV, 2000; Salle &

Rosenthal, 2005). The weakness of the COBIT framework is that it focuses on what should exist and this makes it a less technical document but it can be difficult to implement (Joseph Martin & CISA, 2003; Salle & Rosenthal, 2005). While COBIT provides Key Goal Indicators and Key Performance Indicators for the processes it does not provide the details of how these should be implemented resulting in the need for a more detailed guideline for implementation (Salle & Rosenthal, 2005; Von Solms, 2005).

2.1.2.2 The ISO/IEC 27001 FRAMEWORK

The ISO (27001) is exclusively designed for IS management. As a result it is easier to implement and is more recognized by stakeholders and with a global reach of 80% it could be regarded as the IS management standards (ISMS) used for benchmarking (Susanto12 et al., 2011; Von Solms, 2005) . Researchers points out that while ISO/IEC 27001 was the most widely used security standard between 2008 and 2010 implementation of this standard ranged between 6% - 26% (Susanto12 et al., 2011, 2012). ISO is a more detailed standard when compared to COBIT. It states in clear terms how things must be done, it addresses IS at a lower level, it can be applied to any organization and, it is the preferred standard of technical persons (Susanto12 et al., 2012; Von Solms, 2005). One of the weaknesses of the ISO standard is that it is difficult to integrate into the wider framework of IT governance hence it is regarded as a ‘stand- alone’ standard (Von Solms, 2005) .

2.1.3 THE VALUE-FOCUSED THINKING

The Value-Focused Thinking (VFT) methodology of (Keeney, 1996) provides guidance on the formulation of objectives. According to Keeney (1996) the VFT approach leads to better decisions as it provides an avenue that brings together ‘critical resource’ and ‘hard thinking’ which is the core requirement in any decision making situation. VFT has been applied across a wide variety of domains including systems engineering (Boylan, Tollefson, Kwinn, & Guckert, 2006), security (Dhillon & Torkzadeh, 2006), project management (Barclay & Osei-Bryson, 2010) and Information security (N. B. Maitland & Osei-Bryson, 2014). Within the context of the VFT methodology, objectives are classified as being either a fundamental objective (FO) or a means-objective (MO), where each MO is an objective that is required in order to directly achieve its parent FO or another MO. Each leaf level MO may be considered to be a *Critical Success Factor (see Figure 1).*

The VFT process has several limitations that are relevant to our overall aim of facilitating the development Information System Security strategies (ISSs). The VFT process has several limitations that are relevant to our overall aim of facilitating the development of *ISS*s. Two of these are included in the focus of this paper:

- **Limitations in Human Ability to Recall**: It is well known that there are limitations on human short-term memory that can affect recall of relevant information both with regards to organizational and domain knowledge. This fact is important for the elicitation phase of the VFT process where the stakeholders are expected to identify all relevant objectives and to define them appropriately. This can affect even stakeholders who are ‘experts’ with respect to some dimensions of the relevant decision-making problem. This may lead to some experts being inappropriately impacted by *Informational Influence* (Huang & Wei, 2000), which is the acceptance of evidence from others as evidence about reality.

- **Need to Support Group Decision Making**: The VFT process typically involves multiple stakeholders who may have different values and opinions both with regards to which objectives are relevant, relationships between the objectives, and the relative importance of each FO. There is thus the need for a process to provide decision guidance to empower group members to successfully face the challenge of consensus building (Bryson, 1996; Potter, Gordon, & Hamer, 2004).

3. RESEARCH METHODOLOGY

A design science approach was used in the creation and evaluation of this research model for the proposed InfoSec DKB and preliminary results with the intent to conduct subsequent evaluation in future research. The design science approach applied for this study is based on work presented by (Hevner, 2007). The design science paradigm seeks to create innovative designs that define the technical capabilities, practices and ideas and use them to solve problems (von Alan, March, Park, & Ram, 2004). Design science is a technology-oriented paradigm that has its foundation in the sciences and engineering. The generally accepted activities in design science are: Build and evaluate (Nugrahanto & Morrison, 2008; von Alan et al., 2004) where build looks at the development of an artifact to meet specific requirements and Evaluate is concerned with how well they achieve the intended purpose and contribute to knowledge. Design science brings together technology-based artifacts that can be classified as instantiations constructs, methods or models (Golding & Donaldson, 2009). An artifact was produced; in this case a model evaluating the knowledge base and a conceptual model is represented using an Entity-Relationship model. This research project that follows the guidelines for design science presented in Hevner et al. (2004). Table 1 provides a description of these guidelines and corresponding activity for this research project.

Table 1: Outline of the Design Science Methodology

Guideline	**Activity of this Research Project**
Design as an Artifact	Development of a the *Conceptual Data Model (CDM)of the SDKB*
Problem Relevance	The importance & relevance of the research problem was established in earlier sections of the proposal.
Design Evaluation	For this stage of the research program, the *Conceptual Data Model of the Information Security DKB* was presented (Hevner et al., 2004).
Research Contribution	Definition and illustration of an appropriate *Conceptual Data Model of the Information Security DKB.*
Research Rigor	Utilization of established techniques to define the *Conceptual Data Model of the Information Security DKB* that is consistent with the previously proposed *Hybrid VFT/Delphi Framework* (Maitland & Osei-Bryson, 2014), and the justification of this ‘solution’ framework.
Design as a Search Process	Research on security frameworks, value focused thinking, knowledge management, and other relevant literature in order to identify appropriate techniques & other results that could be used to inform the design of the

	Conceptual Data Model of the Information Security DKB
Communication of Research	Presentation of results to the research community in the form of conference and journal papers

In this study we developed a Conceptual Model that brings together the two most widely adopted security frameworks / standards: COBIT and the ISO 27001, and the Value Focused Technique that will be distilled to build the InfoSec DKB. In table 2 below we describe the application of the Design Science process used in developing this model and the specific steps that we used to develop our Conceptual Data Model: see Figure 2

Table 2: Application of the Design Science process

Step	Action	Example of Results
1a	Review papers on VFT methodology	Literature review
1b	Review existing VFT models for the IS Security	Literature review
1c	Identify Concepts of a VFT Model	○ Objective: Fundamental (FO), Means (MO) ○ Attributes (e.g. Direction, Decision Context)
1d	Identify Relationships in a VFT Model	○ MO ***Leads_To*** FO (M:M) ○ MO ***Consists_Of*** MO (M:M) See Figure 1
2a	Review existing IS Security Frameworks	
2b	Identify Concepts of IS Security Frameworks	○ Information Security Goal, Process
2c	Identify Relationships in IS Security	○ Process **Is_Required_For** Information Security Goal

	Frameworks	
3	Identify Relationships between Concepts of a VFT Model & Concepts of IS Security Frameworks	○ Information Security Goal ***Is_Equivalent_To*** Fundamental Objective (FO)
4a	Develop Conceptual Data Model (CDM) based on Results from Steps 1a – 3.	See Figure 2 & Table 3
4b		
5a	Develop Relational Data Model (RDM) based on CDM	
5b	Do initial population of the RDM based on data in existing VFT diagrams & IS Security Frameworks	
5c	Run Proof-of-Concept Queries against RDM model	See Table 4

4. FINDINGS

In this section we present conceptual models for the VFT technique, the conceptual model developed for the proposed InfoSec DKB and some preliminary results from SQL that was executed on the initial data inputted from the COBIT and ISO27001 frameworks and the VFT network for Information Security. Figure 1 represents a conceptual model of the VFT. Within the VFT methodology, objectives are placed in two categories: Fundamental objective (FO) or means-objective (MO). Each MO can either be an objective that is required for the achievement of its parent FO or an objective that achieves another MO.

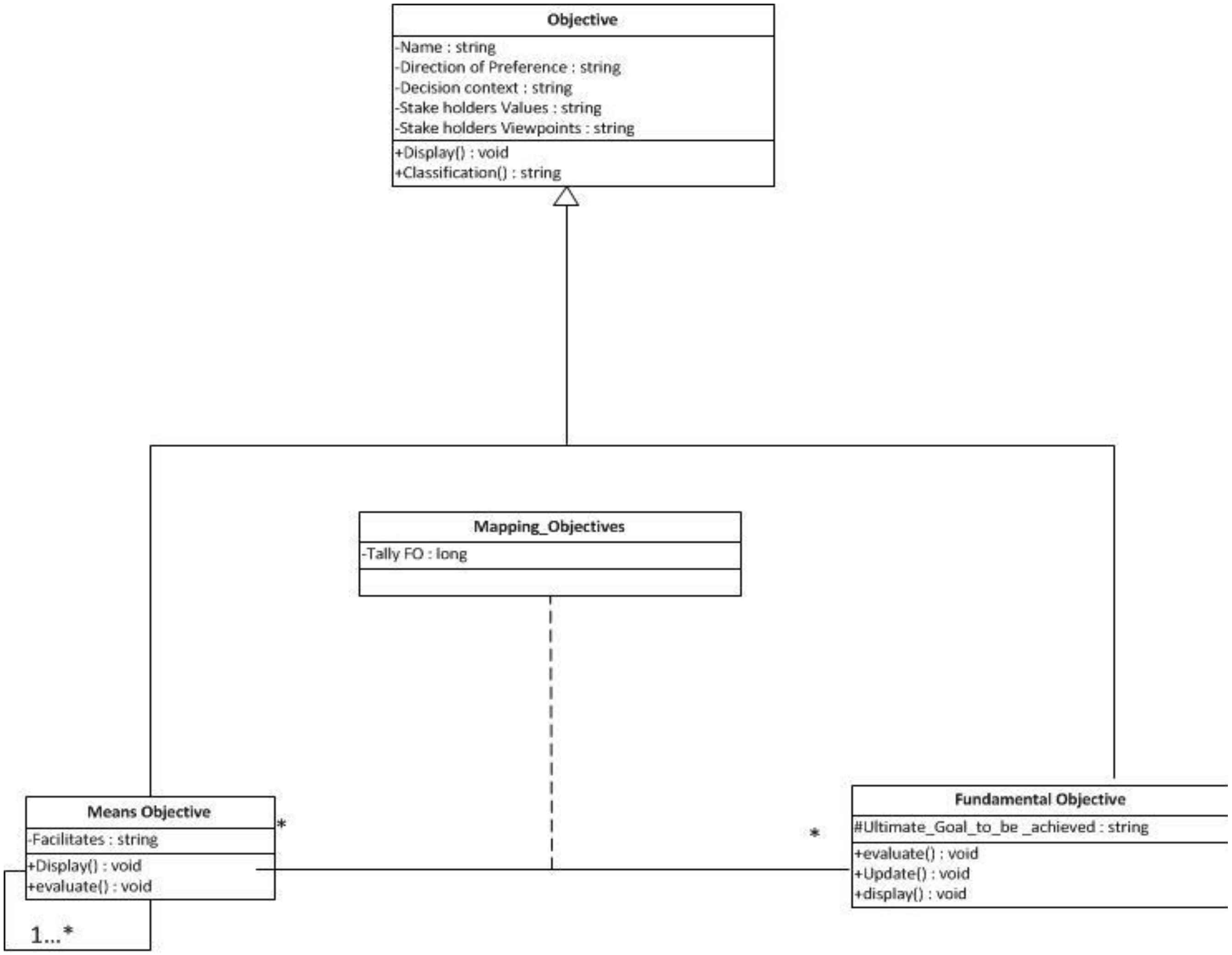


Figure 1: A conceptual data model of the VFT technique

Figure 3 is a Conceptual Data Model that connects concepts of information security frameworks (such as COBIT and ISO/IEC 27001) with concepts of the VFT model. along with the application of the VFT technique used in identifying decision makers " wish list" for information security in ICT (Drevin, Kruger, & Steyn, 2007; Susanto12 et al., 2012). The COBIT framework provides a well-defined and consistent framework that decision makers can use to reduce the communication gap between control requirements, technical issues and business risks (Lainhart IV, 2000; Salle & Rosenthal, 2005). ISO is a more detailed standard when compared to COBIT as it states in clear terms how things must be done as its addresses information security at a lower level, it can be applied to any organization and, it is the preferred standard of technical persons (Susanto12 et al., 2012; Von Solms, 2005). The VFT provides a medium for identifying values that are important for decision makers in a specific decision context.

In this research we focus on Delivery and support Domain (DS) of the COBIT framework that is aimed at the security and Support of IT systems in organizations. The relational Model presented in Figure 3 is a representation of how various tasks are integrated by the COBIT and ISO/IEC 27001 Frameworks to ensure information security in organizations. The COBIT Framework *Information Criteria/Information Security Goals* are Effectiveness, Efficiency, Confidentiality, Integrity, Availability, Compliance and Reliability, with Confidentiality, Integrity and Availability the main Information Criteria required for Information Security. Each *Domain* in the COBIT framework consists of various processes that are required to achieve the desired Information Criteria /Information Security Goal (ISG). A level of priority is also assigned to each *Process* to indicate the importance of the Process in achieving that Information Criteria. The *Information Technology Resources* are People, Information, Technology, application, Facilities. These Information Technology Resources are selected based on the relevance to the process involved in achieving the desired Information Criteria.

The ISO/IEC 27001 framework as mentioned in section 2.1.4 is a more detailed standard when compared to COBIT. The ISO/IEC 27001 standard states in clear terms the step-by-step procedures that are required when addressing Information Security at a lower level. The ISO/ IEC 27001 standard/ framework also identifies Integrity, Availability and Confidentiality as the main requirements for Information Security. The processes that are primarily involved in Information Security in both frameworks are merged in Figure 3.

The Conceptual Model in Figure 2 represents the frameworks that are combined and used in this study. The equivalent factors as it relates to IS security in the frameworks and the fundamental objectives of the VFT approach were identified.

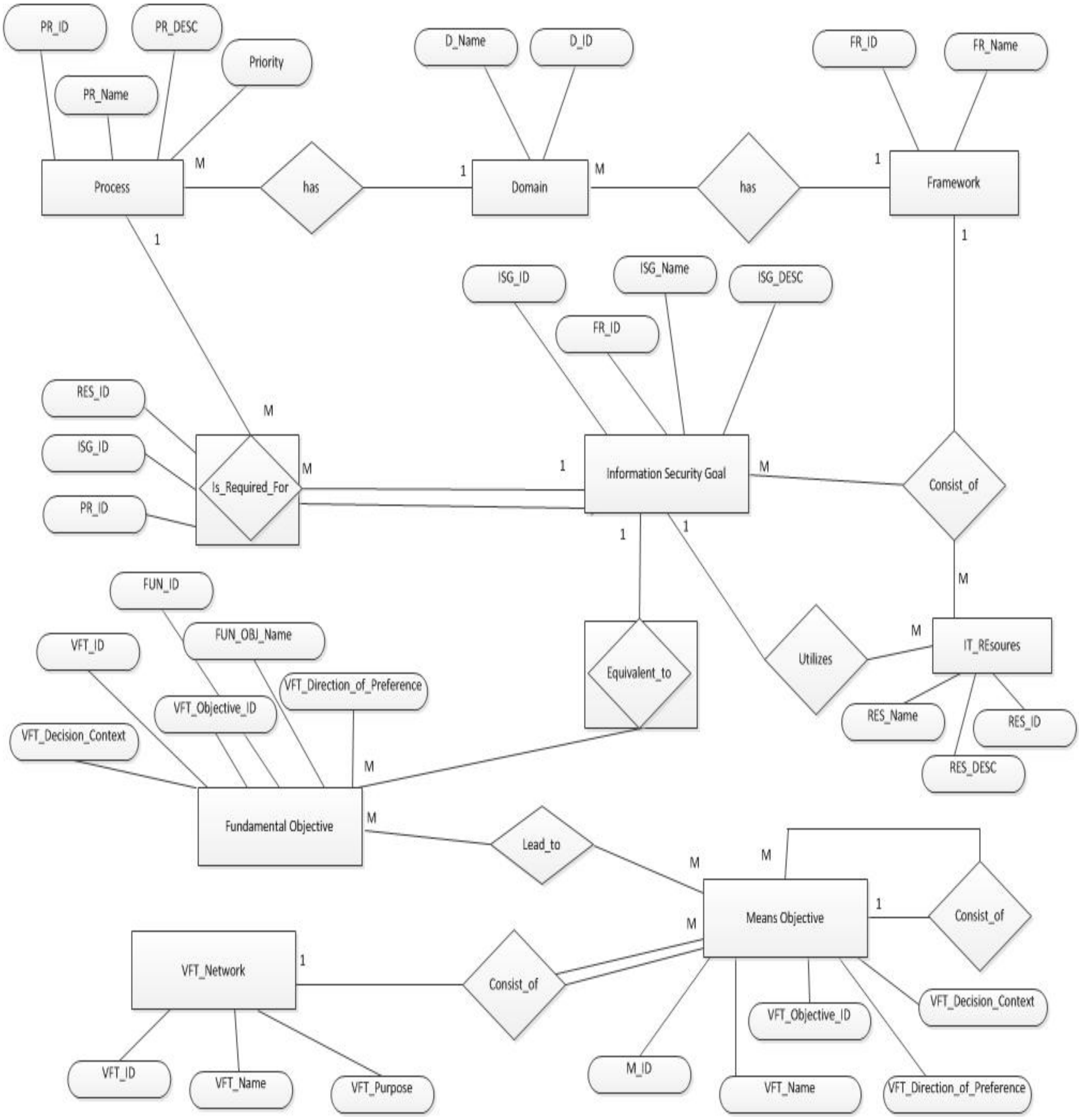


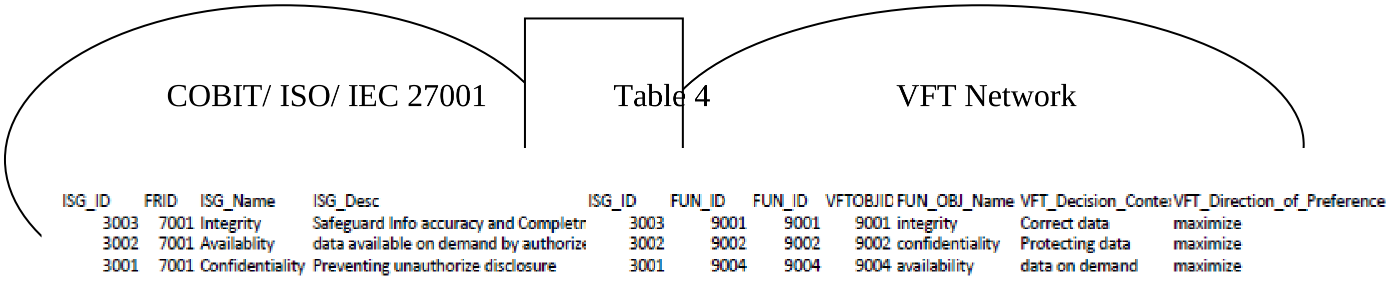
Table 3: Sample Metadata of Conceptual Data Model

Entities and Relationships	**Type**	**Meta Data for each Concept**
Information security goal	Entity	Ensuring integrity of organization data/information
Process	Entity	Define and manage service levels; Manage third-party services; Manage performance capacity; Ensure continuous service, Identify and allocate cost; Educate and train users; Manage service desk incidents; Manage the configuration; Manage problems; Manage operations; Manage physical environment
Framework	Entity	This is the value for the framework entity that provides the expert know-how and the step-by-step guide for implementing the requirements in the InfoSec DKB
Is_Required_For	Relationship	This relationship brings together the processes that are required to achieve the desired information security goal.
Domain	Entity	The domain is a process model that is organized based on a system life cycle approach. There are four primary domains: Plan and Organize; Acquire and Implement; Delivery and Support; and Monitor and Evaluate. The focus of this study is Delivery and Support
IT_Resources	Entity	*People*: Persons authorized to use file resources (Copy, Write, Change, Overwrite) *Data*: Information to be protected *Technology*: Mechanisms and procedures used to identify authorize users(subjects) of objects ,files/data on the system; Identify systems and sub-systems that are

		authorized to share or exchange information (user programs) modify. *Application*: Used printed audit reports, request etc. *Facilities*: Location of sub-system involved in the process: How secure are these facilities**:** What are the required protocols to access them etc.
Mean Objectives	Entity	These are objectives that if achieved can result in ascertaining the desired output. Means objectives can be in one or more parent child relationships. An example as used in the VFT modeled in this research: Maximize information → Maximize effective use of passwords →Maximize logical access control →Minimize tampering with systems these are all means objective and they are in a parent child relationship that lead to achieving the desired fundamental objective (Maximize integrity of data).
Fundamental Objective	Entity	Fundamental objectives are referred to as the reason for the problem under consideration. These are the decision makers goal “wish list” the desired output in this instance Maximize Integrity of data.
Equivalent _to	Relationship	This evaluates the fundamental objectives and the information security goals and display the equivalent values.

Below are the results derived from the system query language (SQL) statement that was executed to derive the equivalent factors as it relates to the main information security goals / fundamental objectives required for information security that was derived by the COBIT and the ISO 27005 framework and VFT assessment of ICT security awareness done by (Drevin et al., 2007). Table 4 displays the results of the evaluation of the COBIT and ISO/IEC 27001 security standards and the selected VFT for ICT security network used in this study. The result of this evaluation identified availability, confidentiality and integrity as the factors that were equivalent for information security in all three standards. Therefore the implementation of this InfoSec DKB could assist businesses and governments in developing templates to craft their information security strategies as the core requirements for information security are the same across all three standards. This would eliminate the need for expensive certifications, reduce ambiguities and complex implementation requirements.

Equivalent Security Goals


COBIT/ ISO/ IEC 27001
Table 4
VFT Network

ISG_ID	FRID	ISG_Name	ISG_Desc	ISG_ID	FUN_ID	FUN_ID	VFTOBJID	FUN_OBJ_Name	VFT_Decision_Conte	VFT_Direction_of_Preference
3003	7001	Integrity	Safeguard Info accuracy and Completr	3003	9001	9001	9001	integrity	Correct data	maximize
3002	7001	Availablity	data available on demand by authoriz	3002	9002	9002	9002	confidentiality	Protecting data	maximize
3001	7001	Confidentiality	Preventing unauthorize disclosure	3001	9004	9004	9004	availability	data on demand	maximize

Preliminary Evaluation of the CDM Artifact

Maes & Poels (2006) presented an assessment framework based on Seddon’s re-specified Information Systems Success model (Seddon, 1997) which acknowledges quality as an antecedent to system success. This model identified four interconnected categories as necessary to assess the quality of an artifact:

- *Perceived Semantic Quality* describes the correspondence between the information that users think the model contains and the information that users think the model should contain, based upon their knowledge of the problem domain (Krogstie et al., 1995). Thus, the users or participants can view the semantic quality of the model as how valid and complete it is with respect to (their perception of) the problem domain.

- *Perceived Usefulness* relates to "the degree to which a person believes that using a particular system has enhanced his or her job performance" (Davis 1989).
- *User Satisfaction* (US) is a subjective evaluation of the various consequences evaluated on a pleasant-unpleasant continuum (Seddon 1997).
- *Perceived Ease of Use* refers to "the degree to which a person believes that using a system would be free of effort" (Davis, 1989) or perceived as being difficult to use (Moore & Benbasat, 1991).

Below we present the results of the use of an Informed Argument approach to conduct a preliminary evaluation of our proposed Information Security Conceptual Data Model based on the Maes & Poels (2006) framework.

Table 5

Category	**Activity**
Perceived Semantic Quality	Hybrid VFT/Delphi aims to provide knowledge base support for the elicitation phase of the VFT process. Given that the CDM is based on knowledge/information expressed in established existing IS Security frameworks & previously proposed IS Security Domain VFT models which have been linked then the corresponding InfoSec DKB should contain should contain *the information that users think* it *should contain*'.
Perceived Usefulness	Given that the CDM is based on knowledge/information expressed in established existing IS Security frameworks & previously proposed IS Security Domain VFT models which have been linked in a manner that allows for querying the corresponding SDKB, then use of the SDKB should result in improved performance by stakeholder in using a VFT based process to develop IS Security Strategies & Policies.
User	Given that stakeholders may be at different levels of knowledge and

Satisfaction	competence with regards to Information Systems security, and limitations on human's ability to recall all relevant information, then stakeholders should be satisfied to have access to relevant information that would be contained in the SDKB which is based on the CDM
Perceived Ease of Use	The stakeholders would not be interacting directly with the SDKB/CDM but rather through software facilities including that provided by the RDBMS.

CONCLUSION AND FUTURE WORKS

In this paper we used design science methodology to build and evaluate a conceptual model for strengthening information security in developing states as they seek to protect their systems from Internet "rogues". This brings together the ISO, COBIT security guidelines and the VFT means-end-network for information security. We have discovered that the ISO and COBIT standards are the most widely adopted standards with ISO/IEC 27001 the leading standard with an adoption rate between 6% - 26% (Susanto12 et al., 2011, 2012). This low rate of adoption of information security standards is attributed to the complexity and difficulty experienced in implementing these standards (Susanto12 et al., 12). These standards are predominantly auditing standards, however developing countries need to build information security into their systems from the onset and should be viewed as a functional requirement rather than a non-functional requirement (Busby-Earle & France, 2013; Gercke, 2009, 2011). We have proposed a conceptual framework for an information security DKB that aims to assist developing countries in strengthening and managing information security. Preliminary results reveal that these are equivalent frameworks; hence the strengths of each can combined to produce a more robust framework. Future components of this research program will involve the development of a software system that will implement this *framework*, followed by the evaluation of the system. We anticipate that the next steps will include the population and testing of the Information Security Domain Knowledge Base (InfoSec DKB) and a software tool for accessing this Knowledge Base.

References

Alavi, M., & Leidner, D. E. (2001). Review: Knowledge management and knowledge management systems: Conceptual foundations and research issues. *Mis Quarterly*, 107-136.

Ali, A. H. (2011). Power of Social Media in Developing Nations: New Tools for Closing the Global Digital Divide and Beyond, The. *Harv. Hum. Rts. J., 24*, 185.

Barclay, C., & Osei-Bryson, K.-M. (2010). Project performance development framework: An approach for developing performance criteria & measures for information systems (IS) projects. *International Journal of Production Economics, 124*(1), 272-292.

Blum, D. (2006). Making Business Sense of Information Security. *Security and Risk Man*.

Boylan, G. L., Tollefson, M. E. S., Kwinn, L. C. M. J., & Guckert, R. R. (2006). Using value-focused thinking to select a simulation tool for the acquisition of infantry soldier systems. *Systems engineering, 9*(3), 199-212.

Bryson, N. (1996). Group decision-making and the analytic hierarchy process: Exploring the consensus-relevant information content. *Computers & Operations Research, 23*(1), 27-35.

Busby-Earle, C. C., & France, R. B. (2013). Analysing Requirements to Detect Latent Security Vulnerabilities.

Charuenporn, P., & Intakosum, S. (2012). Qos-Security Metrics Based on ITIL and COBIT Standard for Measurement Web Services. *J. UCS, 18*(6), 775-797.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS quarterly*, 319-340.

Denning, D. E. R. (1999). *Information warfare and security* (Vol. 4): Addison-Wesley Reading MA.

Dhillon, G., & Torkzadeh, G. (2006). Value-focused assessment of information system security in organizations. *Information Systems Journal, 16*(3), 293-314.

Drevin, L., Kruger, H. A., & Steyn, T. (2007). Value-focused assessment of ICT security awareness in an academic environment. *Computers & Security, 26*(1), 36-43.

Gercke, M. (2009). Understanding cybercrime: a guide for developing countries. *International Telecommunication Union (Draft), 89*, 93.

Gercke, M. (2011). Understanding Cybercrime. A Guide for Developing Countries. *International Telecommunication Union (Draft), 89*, 93.

Golding, P., & Donaldson, O. (2009). A design science approach for creating mobile applications. *ICIS 2009 Proceedings*, 165.

Hevner, A. R. (2007). A three cycle view of design science research. *Scandinavian journal of information systems, 19*(2), 4.

Hojaji, F., & Shirazi, M. R. A. (2010). *A comprehensive SOA governance framework based on COBIT.* Paper presented at the Services (SERVICES-1), 2010 6th World Congress on.

Hovav, A., Andoh-Baidoo, F. K., & Dhillion, G. (2007). *Classification of security breaches and their impact on the market value of firms.* Paper presented at the Proceedings of the Sixth Annual Security Conference, Las Vegas.

Huang, W. W., & Wei, K.-K. (2000). An empirical investigation of the effects of group support systems (GSS) and task type on group interactions from an influence perspective. *Journal of Management Information Systems, 17*(2), 181-206.

Joseph Martin, C., & CISA, C. (2003). CobiT: A Tool to manage information ecology. *Information Systems Control Journal, 3*, 37-39.

Jung, J., Choi, I., & Song, M. (2007). An integration architecture for knowledge management systems and business process management systems. *Computers in industry, 58*(1), 21-34.

Keeney, R. L. (1994). Creativity in decision making with value-focused thinking. *Sloan Management Review, 35*, 33-33.

Keeney, R. L. (1996). Value-focused thinking: Identifying decision opportunities and creating alternatives. *European Journal of Operational Research, 92*(3), 537-549.

Kritzinger, E., & von Solms, S. H. (2010). Cyber security for home users: A new way of protection through awareness enforcement. *Computers & Security, 29*(8), 840-847.

Krogstie, J., Lindland, O. I., & Sindre, G. (1995, January). Towards a deeper understanding of quality in requirements engineering. In *Advanced Information Systems Engineering* (pp. 82-95). Springer Berlin Heidelberg.

Kshetri, N. (2006). The simple economics of cybercrimes. *Security & Privacy, IEEE, 4*(1), 33-39.

Kwan, M. M., & Balasubramanian, P. (2003). KnowledgeScope: managing knowledge in context. *Decision Support Systems, 35*(4), 467-486.

Lainhart IV, J. W. (2000). COBIT™: A methodology for managing and controlling information and information technology risks and vulnerabilities. *Journal of Information Systems, 14*(s-1), 21-25.

Maes, A., & Poels, G. (2006). Evaluating quality of conceptual models based on user perceptions. In *Conceptual Modeling-ER 2006* (pp. 54-67). Springer Berlin Heidelberg.

Maitland, N., Barclay, C., & Osei-Bryson, K.-M. A Value Focused Thinking (VFT) Analysis to Understanding Users' Privacy and Security Dynamics in Social Networking Services.

Maitland, N. B., & Osei-Bryson, K.-M. (2014). Hybrid VFT/Delphi Method to Facilitate the Development of Information Security Strategies in Developing Countries.

Mamaghani, N. D., Samizadeh, R., & Saghafi, F. (2011). Developing a Combined Framework for Evaluating IT Projects based on IT-BSC and COBIT. *International Journal of Digital Content Technology and its Applications, 5*(5), 10-22.

Moore, G. C., & Benbasat, I. (1991). Development of an instrument to measure the perceptions of adopting an information technology innovation. *Information systems research, 2*(3), 192-222.

Njenga, K., & Brown, I. (2008). *Collective Improvisation: Complementing Information Security Frameworks with Self-Policing.* Paper presented at the ISSA.

Nugrahanto, S., & Morrison, I. (2008). A Design Science Approach to Modelling and Facilitating Clinical Workflow and Decision Making.

Podgor, E. S. (2004). Cybercrime: National, Transnational, or International. *Wayne L. Rev., 50*, 97.

Potter, M., Gordon, S., & Hamer, P. (2004). The nominal group technique: a useful consensus methodology in physiotherapy research. *New Zealand Journal of Physiotherapy, 32*, 126-130.

Rao, L., Mansingh, G., & Osei-Bryson, K.-M. (2012). Building ontology based knowledge maps to assist business process re-engineering. *Decision Support Systems, 52*(3), 577-589.

Ritchey, R. W., & Ammann, P. (2000). *Using model checking to analyze network vulnerabilities.* Paper presented at the Security and Privacy, 2000. S&P 2000. Proceedings. 2000 IEEE Symposium on.

Salifu, A. (2008). The impact of internet crime on development. *Journal of Financial Crime, 15*(4), 432-443.

Salle, M., & Rosenthal, S. (2005). *Formulating and Implementing an HP IT program strategy using CobiT and HP ITSM.* Paper presented at the System Sciences, 2005. HICSS'05. Proceedings of the 38th Annual Hawaii International Conference on.

Seddon, J. (1997). Ten arguments against ISO 9000. *Managing Service Quality: An International Journal, 7*(4), 162-168.

Susanto12, H., Almunawar, M. N., & Tuan, Y. C. (2011). Information security management system standards: A comparative study of the big five.

Susanto12, H., Almunawar, M. N., & Tuan, Y. C. (2012). Information security challenge and breaches: novelty approach on measuring ISO 27001 readiness level. *International Journal of Engineering and Technology, 2*(1).

Susanto, H., & Almunawar, M. N. (2012). Information Security Awareness Within Business Environment: An IT Review. *Available at SSRN 2150821*.

Sutton, P., & Payne, A. (1993). Lilliput under threat: the security problems of small island and enclave developing states. *Political Studies, 41*(4), 579-593.

Turner, K. L., & Makhija, M. V. (2006). The role of organizational controls in managing knowledge. *Academy of Management Review, 31*(1), 197-217.

von Alan, R. H., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *Mis Quarterly, 28*(1), 75-105.

Von Solms, B. (2005). Information Security governance: COBIT or ISO 17799 or both? *Computers & Security*, *24*(2), 99-104.

Wegener, H. (2007). *Harnessing the perils in cyberspace: who is in charge?‖*. Paper presented at the Disarmament Forum.