AUTHOR(S): NICHO, M.

TITLE: A process model for implementing information systems security governance.

YEAR: 2018

Publisher citation: NICHO, M. 2018. A process model for implementing information systems security governance. Information and computer security [online], 26(1), pages 10-38. Available from: https://doi.org/10.1108/ICS-07-2016-0061

OpenAIR citation: NICHO, M. 2018. A process model for implementing information systems security governance. Information and computer security, 26(1), pages 10-38. Held on OpenAIR [online]. Available from: https://openair.rgu.ac.uk/

A Process Model for Implementing Information Systems Security Governance

Mathew Nicho,

School of Computing and Digital Media, Robert Gordon University, United Kingdom

Abstract

Purpose

The frequent and increasingly potent cyber-attacks due to lack of an optimal mix of technical as well as non-technical IT controls, has led to increased adoption of security governance controls by organizations. The paper thus seeks to construct and empirically validate an information security governance process model through the Plan-Do-Check-Act cycle model of Deming

Design/methodology/approach

This descriptive research using an interpretive paradigm follows a qualitative methodology using expert interviews of five respondents working in the information security governance (ISG) domain in United Arab Emirates to validate the theoretical model.

Findings

Our findings suggest the primacy of the Plan-Do-Check-Act Deming cycle for initiating ISG through a risk-based approach assisted by industry-wide best practices in ISG. Regarding selection of ISG frameworks, respondents preferred to have ISO 27K supported by NIST as the core framework with other relevant ISG frameworks/standards forming the peripheral layer. The implementation focus of the ISG model is on mapping ISO 27 K/NIST IT controls relevant IT controls selected from ISG frameworks from a horizontal and vertical perspective. Respondents asserted the automation of measurement and control mechanism through automation to assist in the feedback loop of the PDCA cycle.

Originality/value

The validated model helps academics and practitioners gain insight into the methodology of the phased implementation of an information systems governance process through the PDCA model, as well as the positioning of ITG and ITG frameworks in ISG. Practitioners can glean valuable insights from the empirical section of the research where experts detail the success factors, the sequential steps, and justification of these factors in the ISG implementation process.

Key words: information security, governance, Deming cycle, ISO 27001, ISO 27002, COBIT

1. Introduction

Security governance is considered as the most appropriate method not only to gain control of security processes but also to guarantee alignment with business strategies (Rebollo, Mellado, Fernández-Medina, & Mouratidis, 2015). With increased cyber-attacks, and compliance failures, organizations are moving towards implementing security governance frameworks and standards. Hence, the problem of appropriate selection of adequate security controls and optimal risk treatment relies on international assurance standards (Rebollo et al., 2015). The current information security landscape is moving towards a more strategic approach, commonly referred to as information security governance (Dlamini, Eloff, & Eloff, 2007). Despite this approach, information security governance (ISG) is poorly understood, ill defined, and means multiple things to different people (Moulton & Coles, 2003). Considering the lack of empirical studies related to ISG methodology, the present study aims at complementing the body of literature on information security governance by developing, and empirically testing a theoretical model outlining the methodological process of ISG in an organization.

IT governance and IS security is a tightly knit concept. ISG is directly related to three research subjects namely IT governance, corporate governance and information security (Rebollo, Mellado, & Fernández-Medina, 2012). Both security and governance have in common the concepts of trust in an organization and its practices, data safeguards, and operations that rely not only on sound governance practices but also on good security (Wilson, 2007). IT management teams (representing the governance perspective) and IS security management teams are expected to implement the elements of good governance in conjunction (Whitman & Mattord, 2014). Thus, it has been argued that the protection of information as a valuable asset should not be left solely to the chief information officer of an organization, but should be treated as a governance issue (Abu-Musa, 2010). Since information security within an organization encompasses technical, as well as strategic and legal, concerns, information security needs to be addressed as a corporate governance responsibility involving risk management, reporting and accountability on the part of executive leadership and boards of directors (Posthumus & Solms, 2004). In light of this concept, our research will explore the methodological process of integrating and implementing IS security and IT governance into a process model within an organization.

The paper is structured as follows. Section two explores the different perspectives of ISG to bring out the major underlying concepts of ISG. This is followed by the presentation of the ISG process model (Section three). Section four justifies the research methodology, while section five and six provide the empirical validation of the model.

2. Information Security Governance: A Perspective from Literature

2.1 ISG Defined

The term 'information security governance' came from a briefing paper issued by the IT Governance Institute in 2001, which focused mainly on strategic alignment and direction (Williams, 2001). From an organizational perspective, ISG is a subset of enterprise governance that provides strategic direction, ensures that objectives are achieved, risks are managed appropriately, organizational resources are used responsibly, and the success or failure of the enterprise security program is monitored (IT Governance Institute, 2006). The building blocks of ISG have been stated as directives and control, risk, best practices, organization, and awareness (von Solms & von Solms, 2006).

ISG is defined as "the establishment and maintenance of the control environment to manage the risks relating to the confidentiality, integrity and availability of information and its supporting processes and systems" (Moulton & Coles, 2003, p. 581). ISG is considered an integral part of the enterprise governance that involves implementation of governance concepts and principles with regard to information security issues (Abu-Musa, 2010). ISG describes the process of how information security is addressed at an executive level (Posthumus & Solms, 2004), consisting of the leadership, organizational structures, and processes involved in the protection of information assets (Johnston & Hale, 2009). Hence, when properly implemented, ISG provides four basic outcomes; namely, strategic alignment, value delivery, risk management and performance measurement (Williams, 2001).

2.2 ISG Models

Research focusing on the different aspects of ISG has led to the proposal of various ISG models addressing particular aspects of information security governance. An ISG framework has been proposed for integrating information security into corporate governance (Posthumus & Solms, 2004) while Veiga and Eloff (2007) evaluated four approaches towards ISG to come up with a comprehensive framework providing a number of key components in the information security governance domain. These key components focus on IT governance, risk management, compliance, controls framework and standards, monitoring and feedback mechanisms, security awareness and culture, and IT services. From a control perspective, the ISG model based on the Direct–Control Cycle focuses upon the nature of control exerted by corporate management (von Solms & von Solms, 2006). Subsequently, dos Santos Moreira, Andréia Fondazzi Martimiano, José dos Santos Brandão, and César Bernardes (2008) proposed an ISG framework , which organize ISG into three levels namely, the operational, tactical and strategic levels to assist managers in identifying the security best practices to be followed at each level. From a cloud perspective, an ISG process model related to the cloud service life cycle has been proposed considering control and the security risk (Rebollo et al., 2015). While the above models and frameworks have provided the objective, the needed conceptual framework and building blocks for ISG, a methodological approach to implementing ISG in an organization is lacking in the literature.

In this respect, our model follows the 'theory of design and action', which says 'how to do' something by discussing the methodologies and tools used in the development of information systems (Gregor, 2002). This leads to our exploratory research question: How does organization implement the conceptual components of 'IT governance' and 'security' for information security governance? Since the research question incorporates 'process' of 'security' and 'governance', we analyze these three concepts to get insights into current practices of IS process implementation and understand the role of 'governance' in IS security.

Evaluating the above ISG definitions, models, and the ISG building blocks, the major ISG themes cited by researchers can be categorized as the cyclical process of ISG, risk management, ITG frameworks for selecting and integrating appropriate IT controls, monitoring and measurement, including feedback, a security culture via training, and best practices.

2.3 Cyclical Process of IS Security

Security management must integrate security and controls across the strategic, tactical, and operational levels within the organization, as well as view IS security from a life cycle perspective (Choobineh, Anderson, & Grimaila, 2010). The dynamic nature of information security prevents any fixed boundaries because the different dimensions of IS security must work together to create a secure environment (Solms, 2001) thus supporting a continuous improvement cyclical process. This cyclical method is the cornerstone of the ISO 27001 (2005) which proposes an approach to continuous improvement through a process of establishing, implementing, operating, monitoring, reviewing, maintaining and improving the organization's information security management system (ISO, 2011; Veiga & Eloff, 2007). The 2005 version of the ISO 27000 standards heavily employ the Plan-Do-Check-Act model (PDCA) to structure IT processes (Nicho & Avinash, 2012; Nor Aza & Normaziah, 2012), and reflects the principles set out in the OECG guidelines. However, the 2013 version places more emphasis on measuring and evaluating the performance of an organization's information security management system (ISMS) (International Standards Organization, 2013).

Thus, our research looks at the ISG implementation process through the lens of the PDCA cycle of Edward Deming, incorporating the models, frameworks and standards used in the security and governance implementation process. This leads to the first proposition – ***the ISG implementation process follows the Plan-Do-Check-Act Cycle.*** The planning stage of security management starts with an assessment of risks, followed by the stages: definition of policy, delineation of requirements, establishment of control, environmental monitoring, and final risk assessment (Choobineh et al., 2010). Information security risk management being a continuous management process (Wu, Guo, Lin, & Li, 2015), the security risks and requirements must be clearly understood before proper security mechanisms can be identified and designed (Yadav, 2010).

2.4 Risk Assessment

A risk-based approach in managing information security has been an accepted method in a security program, since increasing dependence on information networks for business operations has focused managerial attention on managing risks posed by the possible failure of these networks (Chen, Kataria, & Krishnan, 2011). Most IT audits are conducted using a "risk-based" approach, where potential risks are identified and prioritized, control mechanisms are assessed, and the controls tested (Merhout & Havelka, 2008). Hence, managers should initiate a theory-based security program that includes the use of a security risk planning model, education in security awareness, and a counter measure matrix analysis (Straub & Welke, 1998). This directs our research to its second proposition – ***ISG is initiated using a risk-based approach***. Since, determining the effective management of risk is part of IT governance (Solms, 2005), the IT governance structure must be designed so that IT adds value to the business and IT risks are mitigated (Mishra & Weistroffer, 2007).

2.5 Relevance of Governance in IS Security

Security and governance controls play a critical role in risk prevention, as 97% of the breaches were avoidable through simple or intermediate controls (Verizon, 2012). Hence, implementing security mechanisms alone is not sufficient to prevent data breaches, as technical and non-technical controls, supplemented with best practices in information security and governance, are required to provide optimized, rather than adequate protection. Subsequently, the high incidence of security breaches in organizations could be attributed to the organization's inability to adequately focus on non-technical issues in information systems security, namely policies, procedures, practices, and strategies that, organizations normally put in place to minimize threats (Dhillon & Backhouse:, 2001; Ifinedo, 2009; Straub & Welke, 1998).

The management of information security is primarily concerned with strategic, tactical, and operational issues surrounding the planning, analysis, design, implementation and maintenance of the IS security program (Choobineh, Dhillon, Grimaila, & Rees, 2007). In this respect, the effective and efficient utilization of information technology requires the alignment of IT strategies with business strategies (Luftman & Brier, 1999; Luftman, Lewis, & Oldach, 1993). Accordingly, the strategic alignment of IT goals with organizational goals is the prime objective of IT governance. Subsequently, an effective implementation of information security involves using a strategic mix of: IT governance frameworks (which align the IT goals with the organizational goals), IT service management (which maintains efficient and effective continuity of operations), and compliance with relevant security standards, policies and programs. Thus, our third proposition states – ***the ISG implementation involves the selection of appropriate ISG frameworks and standards.*** In light of this proposition, it is imperative to look at ITG frameworks, IS security frameworks and standards, in the ISG domain.

2.6 Governance Aspect of Security (Internal controls – technical and non-technical)

A global survey on control frameworks used in enterprise governance of IT revealed that, 28% use ITIL/ISO 20000, 21.1% use ISO 27000-related security frameworks, 15.1% use Six Sigma, 12.9% use COBIT, 12.7% use PMI/PMBOK, and 12% use the RiskIT framework of Information Systems Audit and Control Association (ISACA) along with other frameworks (ISACA, 2011). Similarly, another survey of security professionals focused on North America revealed that 72% of North American organizations with 1,000 or more employees have implemented one or more formal IT best-practice control and process models (Turner, Oltsik, & McKnight, 2009). Among these, the most widely used commercial IT control frameworks were ITIL, ISO 27002 and COBIT, which provide optimal security management. Furthermore, ISO/IEC 27002, COBIT, ISO 20000, and ITIL are the most applicable and common standards to manage and maintain IT services (Sahibudin, Sharifi, & Ayat, 2008).

The overlap of different frameworks and standards leads to mapping between IT governance and security domains as in the case of PCI DSS, which employs IT security best practices such as ISO 27002 and COBIT (Laredo, 2009). Likewise, there are 70 technical controls shared between ISO 27000 and PCI DSS (Gikas, 2010). While, governance is considered a key factor in the setting of standards, success is more likely if the governance structure includes all the various network domains. Hence, the standards themselves (e.g. ISO 27 K, PCI DSS, ISO 20000) need to be effective, yet flexible enough to satisfy these competitive interests (Sullivan, 2010). In this regard, (Solms, 2005) stated that the components of ISG must work together to ensure that the confidentiality, integrity and availability (CIA) of the company's electronic assets are maintained at all times'. This leads to our fourth proposition – ***ISG implementation process involves the mapping, integration, and implementation of relevant IT frameworks, and standards.*** Since, the measurement of IS success is important for assessing the effectiveness of IS (Gorla & Somers, 2014), a measurement and feedback mechanism with pre-defined metrics ensures monitoring and control.

2.7 Measurement and Feedback in ISG

Information systems should be measured like any other part of a business (Singleton, McLean, & Altman, 1988). In fact, measurement of IS success is one of the most enduring research topics in the IS field (Markus, Tanis, Petrie, & Tanis, 2000), and is critical for the understanding about the value and efficacy of information systems (DeLone & McLean, 2003). Accordingly, there is a need for systematic techniques with which to obtain quantitative evidence of the operational systems' security performance (Savola, 2013). In this respect, implementing an IS security governance model has to be viewed as a proactive and holistic approach that aligns security mechanisms, procedures and metrics (measurement) with governance principles, business drivers and enterprise strategic objectives (Spremić, 2013). Thus, securing information depends not only on the ability to compare, contrast, and make quantifiable statements about system security (Wang & Wulf, 1997), but require a risk-management approach with dependable, quantifiable metrics (Geer Jr, Hoo, & Jaquith, 2003), with the desired results to be achieved by implementing control procedures for the processes. Furthermore, different kinds of metrics, such as key performance indicators (KPI), key goal indicators (KGI), and critical success factors (CSF), are suggested in order to monitor the general goodness of each process of IT governance (Simonsson, Johnson, & Wijkstrom, 2007). This directs us to the fifth proposition – ***the check phase of the ISG process involves the monitoring and measurement of IT controls, using key performance indicators, key goal indicators and matrices***.

The 'Act' phase of the PDCA cycle involves taking corrective and preventive actions based on the results of the internal ISMS audit and management review (or other relevant information), to achieve continual improvement of the ISMS (Mataracioglu & Ozkan, 2011). The ISG controls implemented have to be scrutinized in a periodic fashion, using feedback loops to incorporate revisions, which, in turn create a solid IS security governance structure (Mishra & Dhillon, 2006). Moreover, management needs feedback on what is happening in the company in terms of information security to have a proper corporate and information security governance framework in place (Kruger & Kearney, 2006). Thus, our sixth proposition is stated as – ***a feedback loop in the ISG process ensures timely corrective actions***. Since the feedback loop involves communicating deviations and corrections to the cycle, an effective information security program cannot be implemented without implementing an employee-awareness training program to address the policy, procedures, and tools (Peltier, 2005).

2.8 Information Security Awareness and Best Practices

End users at the workplace are said to be “the weakest link” in IS security (Guo, Yuan, Archer, & Connelly, 2011; Paans & Herschberg, 1987). In this respect, a holistic information security management approach emphasizes the importance of taking account of the “human” element when ensuring information security throughout the organization (Flores, Antonsen, & Ekstedt, 2014). The term “information security awareness”' refer to a state where users within an organization are aware of, and ideally, are committed to, the organization’s security mission (Siponen, 2000). Information security awareness programs need to be implemented in organizations, while those already in existence need to be expanded (Thomson & R. von Solms, 1998) thus ensuring a continuous and dynamic approach. This creates an information security culture, which is considered as the set of information security characteristics that the organization values (Gebrasilase & Lessa, 2011). Researchers have proposed the importance of establishing an information-security-aware culture to minimize risks to information (Niekerk & Solms, 2010; Veiga & Eloff, 2010). An information security culture provides a guide and structure to human behavior to prevent risks to the security of information assets (Al Hogail, 2015). This includes the relevance of inculcating a security culture in the organization through training, since effective user security awareness training can greatly enhance the information assurance posture of an organization (Cone, Irvine, Thompson, & Nguyen, 2007). This leads to our seventh proposition – ***information security awareness programs ensure successful implementation of ISG.***

An appropriate method to establish information security is to engineer an array of interlocking best practices, from a commonly accepted model of best practice (Kohnke & Shoemaker, 2015). Subsequently, effective information security management requires identifying the critical success factors (CSF) of implementation, and ensuring the proper management of information security (Torres, Sarriegi, Santos, & Serrano, 2006). Since, CSFs and best practices (BPs) enhance the successful implementation of IT governance frameworks, these have been proposed for IT governance implementation (Grembergen & Haes, 2009) and ITIL (Iden & Langeland, 2010; Pederson, Kraemmergaard, Lynge, & Schou, 2010; Tan, Cater-Steel, & Toleman, 2009). Since studies on CSFs in the ISG domain are lacking, we can replicate the CSFs and BPs of IT governance in IS security, due to the overlap between the two. Thus, we arrive at our eighth proposition – ***following best practices in the stages of the ISG implementation process cycle ensure a secure environment.***

3. IS Security Governance (ISG) Process Model

Based on the analysis of extant literature on IT governance and security, our proposed IS security governance model incorporates the following activities:

1. Implementing ISG through the Plan Do Check Act cycle;
2. Viewing IT governance security from a risk-based perspective;
3. Selecting relevant IS security and governance frameworks (technical as well as non-technical);
4. Mapping relevant IT controls upon ISG frameworks and standards;

5. Implementing a measurement framework for tracking and monitoring IS security governance entities, using quantifiable metrics;
6. A feedback loop that receives outputs from the Check phase, and provides corrective actions;
7. Making sure that the people involved in the ISG framework share a security culture through continuous, multi-level, optimally-crafted, technical and non-technical training; and
8. Use industry best practices to implement ISG at each stage of the PDCA cycle.

The proposed ISG implementation process model (Figure 1) based on the above eight propositions illustrates the significance of effectively managing the ISG implementation process. In this respect, the PDCA cycle has been proposed as the framework on which the various entities are incorporated within the process model. While a risk-based approach to ISG has been emphasized as the first step, researchers have pointed out the significance of selecting relevant IT governance and security frameworks/standards to get the ISG implementation process moving in the initial two phases (of PDCA). Subsequently, the values obtained through the monitoring the performance of IT controls (in the subsequent phases) serve as a feedback mechanism for continuous improvement. To validate the model, we follow a qualitative interpretive methodology.

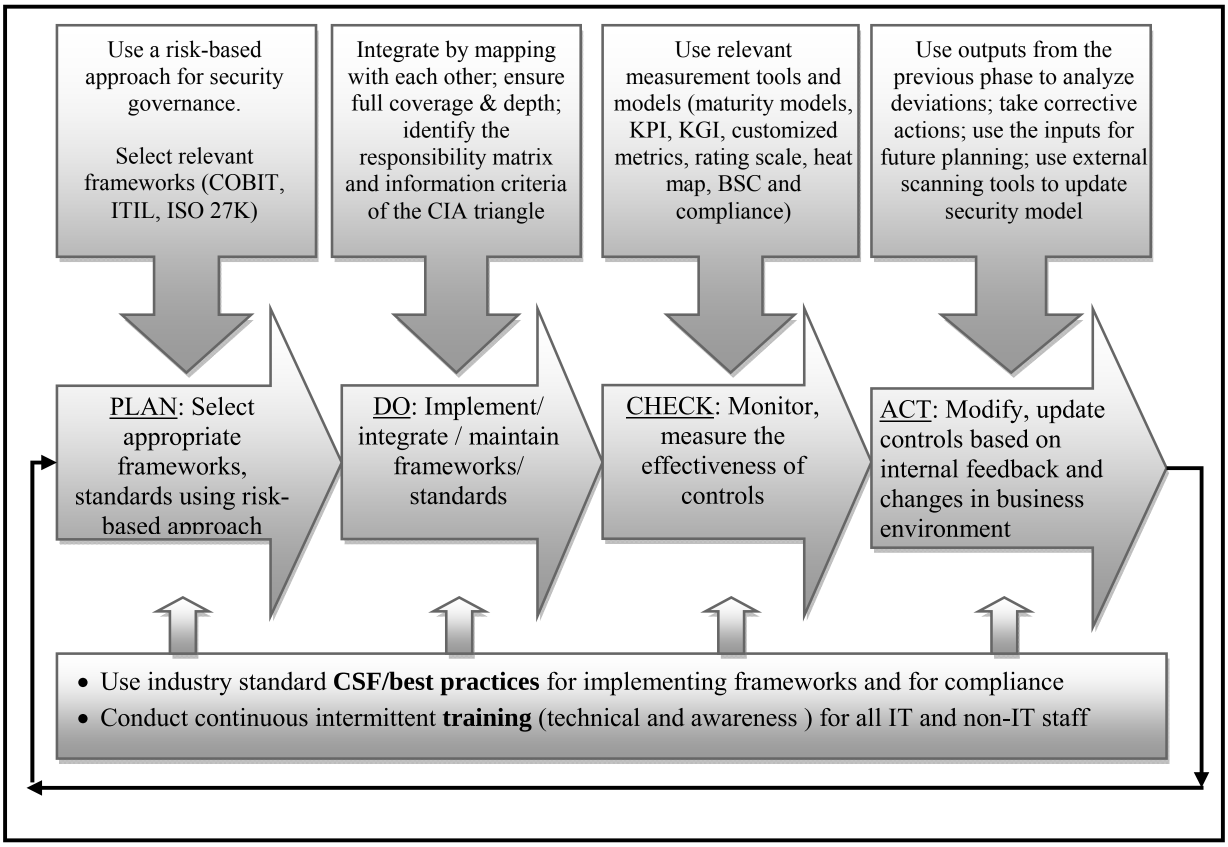

Use a risk-based approach for security governance.
Select relevant frameworks (COBIT, ITIL, ISO 27K)
Integrate by mapping with each other; ensure full coverage & depth; identify the responsibility matrix and information criteria of the CIA triangle
Use relevant measurement tools and models (maturity models, KPI, KGI, customized metrics, rating scale, heat map, BSC and compliance)
Use outputs from the previous phase to analyze deviations; take corrective actions; use the inputs for future planning; use external scanning tools to update security model
PLAN: Select appropriate frameworks, standards using risk-based approach
DO: Implement/ integrate / maintain frameworks/ standards
CHECK: Monitor, measure the effectiveness of controls
ACT: Modify, update controls based on internal feedback and changes in business environment
• Use industry standard CSF/best practices for implementing frameworks and for compliance
• Conduct continuous intermittent training (technical and awareness) for all IT and non-IT staff

Figure 1. ISG implementation process model (Adapted from Nicho (2012))

3.1 Research Method

The nature of the descriptive research question led us to conduct our study using qualitative methods. Qualitative research is concerned with understanding social phenomena from the actors' perspectives through participation in the life of those actors (Firestone, 1987). The actor in this research being the ‘expert’ to validate the model, the expert interview method was employed, as it is a method of qualitative empirical research designed to explore expert knowledge (Meuser & Nagel, 2009). It not only provides researchers control over the dimensions that are central to the comparative research, but also bridges the divide between case studies and the comparison of a large number of countries based on more general and publicly available data (Dorussen, Lenz, & Blavoukos, 2005). Thus, it was decided to interview managers (see interview schedule in Appendix 1) working in the information security and governance domain in United Arab Emirates (UAE), who had expertise in implementing multiple frameworks and standards, and who were members of professional security and/or governance associations. A semi-structured interview method was selected as it offers the merit of using a list of predetermined themes as in a structured interview, while ensuring adequate flexibility to enable the interviewee to talk freely about any topic raised during the interview (Wahyuni, 2012). Being a theory driven approach, the questions in the interview schedule were derived from the propositions (see Appendix 2), which further aligns with the pre-determined coding themes (Appendix 3) which follow the PDCA process model (Appendix 4).

The respondents were contacted through UAE chapter of Information Systems Audit and Control Association (ISACA) of which the author is also a member. Among over 1400 members in the chapter, 37 members were identified fitting the ‘respondent’s profile’, of which five consented to this research. The responses were digitally recorded, transcribed verbatim, and imported into NVIVO (a qualitative analysis software), where three coding techniques (Urquhart, 2001) were used to arrive at the final code categories. Initially, the deductive (theory-driven) approach was used to aggregate information into pre-defined themes (codes). Secondly, open coding was used to identify emergent sub themes inside the pre-defined themes. This was an iterative process whereby the transcripts were read repeatedly to allocate identified texts to respective codes/sub-codes. Finally, axial coding was used to group categories and subcategories (Urquhart, 2001), as well as identify relationships among the pre-defined and emergent themes.

4. Analysis of the Process Model

Five respondents from five organizations in three sectors within the industry – namely, the financial, media and the information technology sevices sectors – who directly manage the information security and governance domain were selected for the interview (Table 1). The five criteria which were used to select the respondents were: organizational size (minumum of 1000 employees), number of years of experience within the industry (minimum of ten years), having a security and governance role within their IT department, industry-relevant certifications in the ISG domain, and experience implemeting at least three frameworks in security and governance.

Table 1. Profiles of the respondents

Month and year of interview	Position/ title	Experience in ITG & security	Industry	Professional IT security, governance, and IT operations certifications/associations

March 2014	IT Manager	24 years	Media	ISO 27000, ISO 20000 & ISO22301 Certified Lead Auditor; Certified Ethical Hacker (CEH);
				Control Objectives for Information and Related Technology (COBIT 4.1) Foundation; Certified in the Governance of Enterprise IT (CGEIT); Information Technology Infrastructure Library (ITIL) Expert; Certified ITIL V2;
				Cloud Computing Associate; The Open Group Architecture Framework (TOGAF 9.1) Certified Professional; Microsoft Certified Technology Specialist (MCTS); Cisco Certified Network Associate (CCNA); Microsoft Certified Solutions Expert (MCSE); Microsoft Certified Desktop Support Technician (MCDST); Dubai Government Excellency Program Certified Auditor.

June 2014	Director - Strategic Security Consulting	14 years	IT GRC and Security service provider	Certified Information Security Manager (CISM);
				CGEIT; Certified Information Systems Auditor (CISA); British Standards Institution Certified BS7799 Lead Auditor;
				Certified Microsoft Operations Framework (MOF).

August 2014	IT Strategy Manager	37 years	Banking	ISO 27001:2005 Lead Auditor (UK); CISM; Certified in Risk and Information Systems Control (CRISC);
				Charted Information Technology Professional, UK (CITP); COBIT 4.1 Foundation; International Register of Certified Auditors (IRCQ) QMS Internal Auditor for ISO 9001:2000 UK; ITIL Foundation Certification in IT – Service Management itSMF;
				TOGAF 9.1 Certified.

December 2014	Senior Consultant (Security & Trust)	13 years	IT security, IT governance, and cloud services	Certified Information Systems Security Professional (CISSP); CISM; Certified Penetration Testing Engineer (CPTE); CISA; ITIL – Foundation.

March 2015	Director and CEO	35 years	IT governance, risk and compliance (GRC), IS security, and digital forensics consulting and training	CISSP; CISM; CEH; Comptia Security+; Computer Hacking Forensic Investigator (CHFI); Certified Forensic Investigation Professional (CFIP);
				Institute of Chartered Accountants in England & Wales (FCA); CISA;
				PhD; Certified Software Quality Professional (CSQP); Former global chair of two international security associations.

In the initial phase, the model and interview schedule were sent by email to the prospective respondents. Thereafter, appointments were made to meet the respondents at their respective offices to get feedback regarding the model. The interviews were transcribed, validated through subsequent telephonic interviews, and imported to NVIVO 10, a qualitative analysis software used by qualitative researchers. The analysis follows the guidelines of Whittaker (2006) which aligns with the three coding techniques identified in section 3.1. In this regard, the interview data was coded into pre-defined themes (Appendix 4) where the transcribed text was systematically examined to identify the key concepts. Subsequently, the data was grouped into similar categories, and searched for relationships between a category and its concepts for further sub categorization. Care was taken to elicit as broad an answer as possible from the respondents, but at the same time, keeping within the interview schedule. This was to ensure that the respondent did not limit his response to the researcher's question, but rather, gave as broad a view as possible within the time provided.

After going through the transcribed interviews several times, two major themes that emerged were: (1) the ISG process and (2) discussion focusing on the eight propositions of the model. Due to the qualitative nature of the responses, there was a great deal of overlap between the two major theme nodes, and as such, care has been taken to separate them as clearly as possible into nine pre-defined first-level nodes (see Appendix 4). In the following section, we will analyze and discuss the ISG process (4.1), focusing on the PDCA cycle, followed by a discussion of the eight propositions (5).

4.1 ISG Process

The ISG process follows the PDCA cycle with the 'Plan' phase, which takes considerable time and effort, followed by the 'Do', 'Check' and 'Act' phases. According to the respondents, the duration of a cycle, from the initial 'Plan' phase to the starting of the second cycle, depends on (1) the security maturity level within the organization, (2) whether the organizational structure is conducive to governance, and (3) the IT risks appreciation of the organization. While unanimously affirming that overarching role of the PDCA cycle in the ISG process, two respondents suggested initiating ISG using the PDCA methodology with simple and manageable scope and gradually increasing the scope in subsequent cycles based on preceding feedback.

4.1.1 Plan

The best practice in this phase has been given as a sequential ISMS process (managerial decisions, risk assessment, establish processes/frameworks, and plan for subsequent phases) involving the ISG entities namely people, process and technology (Figure 2). This time and labor-intensive phase involves a two-dimensional matrix (Figure 3) of ISMS and respective ISG processes (see appendix 5 for the coding source). The major activity during this phase is to establish ISMS, including people, processes and IT systems, by applying a risk-management process where people play a major role during the Plan phase followed by processes and to some extent, technology.

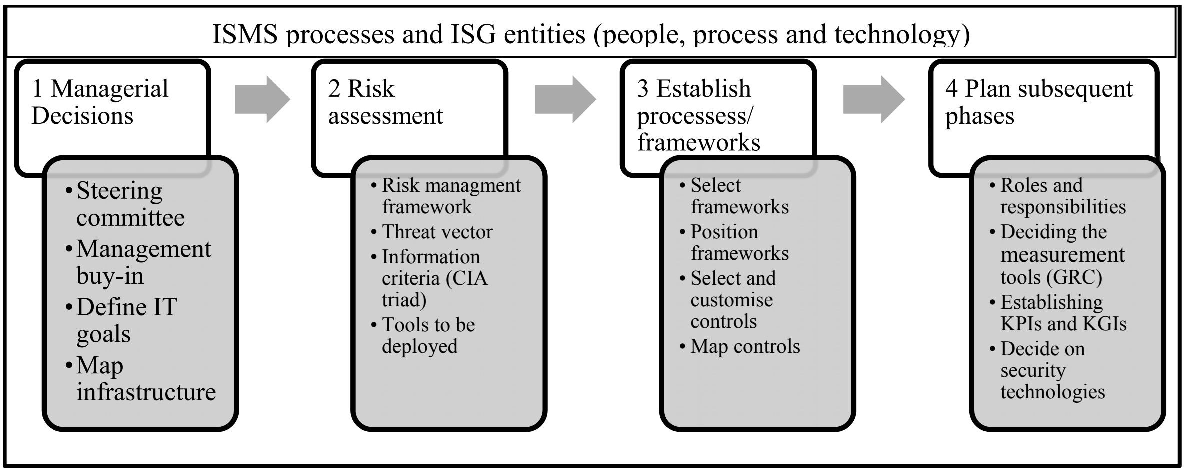

ISMS processes and ISG entities (people, process and technology)
1 Managerial Decisions
• Steering committee
• Management buy-in
• Define IT goals
• Map infrastructure
2 Risk assessment
• Risk managment framework
• Threat vector
• Information criteria (CIA triad)
• Tools to be deployed
3 Establish processess/ frameworks
• Select frameworks
• Position frameworks
• Select and customise controls
• Map controls
4 Plan subsequent phases
• Roles and responsibilities
• Deciding the measurement tools (GRC)
• Establishing KPIs and KGIs
• Decide on security technologies

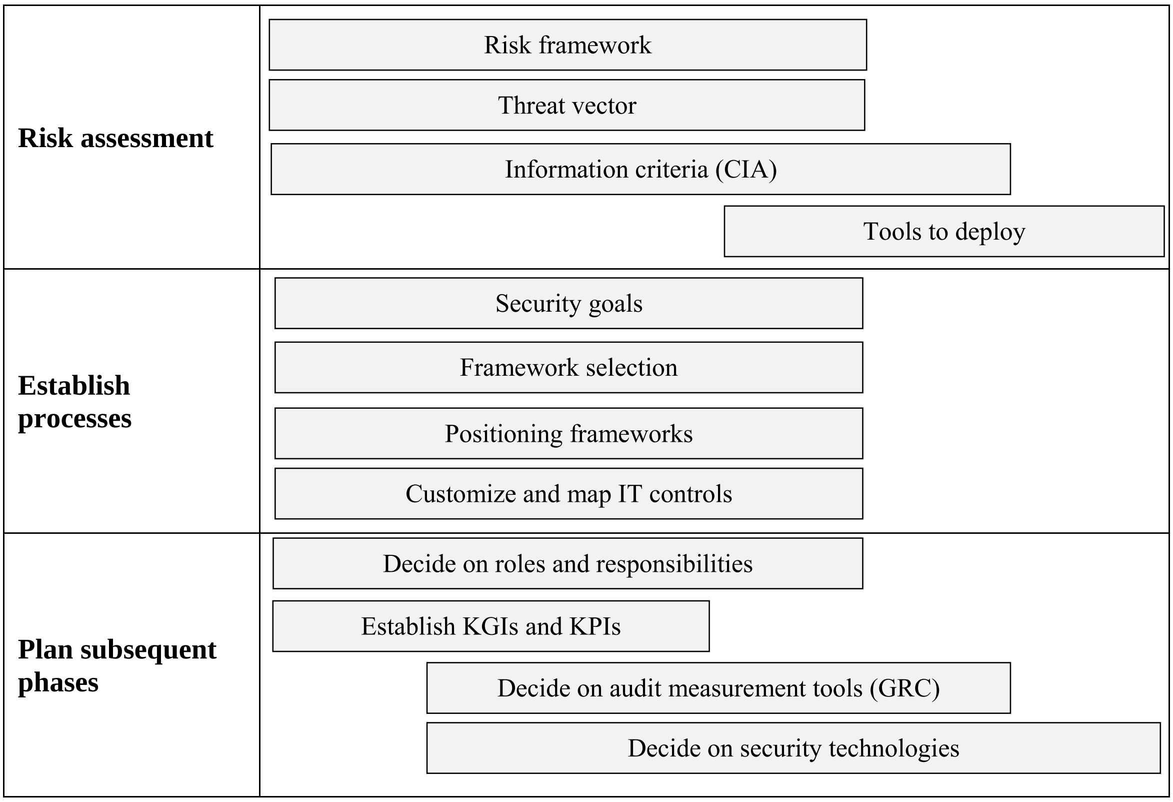
Figure 2. Plan stage of the ISG process

4.1.1.1 Managerial Decisions

The initial steps in the planning process include setting up an ISG structure with a steering committee, achieving management buy-in, defining the IT goals, followed by the technical objective of mapping the information system infrastructure to the security program infrastructure. Respondents affirmed the critical need for high-level representations from IT and business to ensure 'prompt and agreeable' decisions. Hence, one of the requirements for ISG, is the establishment of a security steering committee with people from IT security as well as IT governance, as part of the ISMS. In this regard, a balanced representation from different business and ISG domains ensures alignment of IT goals with business goals. With regard to the business goal of 'accessibility' and the IT goal of 'security', the IT Manager illustrates the need for a 'balanced approach':

> "…most important because if you leave it to the security guys, they would argue against any accessibility, citing security reasons, while at the same time if you leave it to the service desk or the IT service management they want everybody to have full access to keep the customer happy. So, you need to have a balanced approach."

	People	**Processes**	**Technology**
Managerial decisions	Steering committee		
	Management buy in		
	Define IT goals		
		Map infrastructure	



Risk assessment	Risk framework Threat vector Information criteria (CIA) Tools to deploy
Establish processes	Security goals Framework selection Positioning frameworks Customize and map IT controls
Plan subsequent phases	Decide on roles and responsibilities Establish KGIs and KPIs Decide on audit measurement tools (GRC) Decide on security technologies

Figure 3. People, processes and technology matrix of the ISG 'Plan' phase

The IT Manager and the IT Strategy Manager suggested the best practice of employing risk assessment as a tool to convince management to release the funds for ISG. Appropriate ISG decision-making process involves 'management buy in', the involvement of different levels of management and functional areas, and the extent of investments in people, process and technology tools. In this regard, ISO 27 K standards (use of committees responsible for managing security) is useful:

> "… (the use of committees) actually release a lot of pain from the security administrator because they can justify their investment and we get direct support from the higher management due to participation in the committees. So, they start looking at our risk assessment and at our penetration testing results" (IT Manager).

The next step is aligning the IT goals in relation to business goals, mapped from the highest level down to operational goals incorporating the 'KPIs and KGIs'.The defined IT goals are mapped onto IS security goals encompassing the governance aspect as well. Finally, the information system infrastructure is mapped into the security program infrastructure, which clarifies "the scope, the allocation of personnel, roles and responsibilities, identifying the assets that need to be protected, the technical as well as non-technical mechanisms required to protect these assets." The assets "can be services, hardware, software, information that an organization needs to safeguard." This sets the stage for "risk assessment of all those assets against the identified potent threats" culminating in a risk statement plan.

4.1.1.2 Risk Assessment:

In the initial stage of ISG, there is a need to establish a risk-management framework because "before even selecting anything in 'Plan', the risk comes first where you have to define the risk." All the respondents were unanimous in stating the role of risk assessment as the first step in ISG running in parallel to the managerial decisions. They stated, "it is imperative to understand the attack surface" as well as the "threat vector," to "define the security plan which is the product of the risk plan." Hence, once the attack surface is known, then the organization needs to look at the threat vectors, which subsequently, "helps in calculating the risk." Along with the concept of risk assessment, "time-based security assessment or time-based risk assessment, along with cost benefit analysis is important" to "assess the value of counter measures." Risk assessment is a continuous cycle in the ISG process due to the dynamic nature of risk. According to the Director - Strategic Security Consulting,

> "…the controls require upgradation, where you have to deploy new controls, because once you do your risk assessment, you find out that there are new risks, and new threats to your assets. Then you will have to implement or improve your new or existing controls and start the process again."

Since, according to the Senior Consultant (Security & Trust) risk "drives the future phases," he suggested the use of the RiskIT framework, which also complements COBIT. Thus, he states,

> "Risk assessment is the heart of any security program. The more effective the risk assessment, the more effective the security program will be. So the first thing you need to establish is your risk management framework, which assesses the risk; and any decision, has to be risk assessed."

A risk statement plan assists in identifying relevant "technical controls and security automation tools" for mitigating risk. Moreover, the identified assets (in the risk assessment plan) and their corresponding risks are mapped to the appropriate information criteria of the CIA triangle. An advantage of a risk-management approach in ISG is not only to facilitate management's understanding of risk, but also to ensure adequate budgetary allocation to mitigate the risk. Hence:

> "…the advantage here is that, instead of the system administrator or security administrator begging to the management to enhance the security system, it is the other way round, where the business understands exactly what they want to do, evaluate, approve and monitor the budget" (IT Manager).

Thus, justification of the organization's risk plan to the management is important since security governance implementation involves the use of "very expensive tools, and you need to justify your requirement; otherwise they (management) will not release the budget for security governance" (IT Manager).

4.1.1.3 Establish Processes

This sub phase consists of deciding on the type of frameworks and standards to deploy, grouping and positioning frameworks, selection of appropriate controls, customizing, and mapping.

Categorizing Frameworks

Respondents identified relevant frameworks in ISG as ISO 27001, ISO 27002, ISO 27018, Risk IT framework[1], National Institute of Standards and Technology (NIST) database and standards on information security, Val IT[2], Control Objectives for Information and Related Technology (COBIT[3]), ISO 20000, Information Technology Infrastructure Library (ITIL), Open Group Architecture Framework (TOGAF), and Payment Card Industry Data Security Standard (PCI DSS).

The respondents stated the need "to differentiate between controls, framework and best practices" as well as the need to "tailor the frameworks to fit the business and the organization." Based on the responses, IT security governance and standards fall under three partially overlapping categories; namely, governance frameworks, process frameworks, and management frameworks (see Figure 4). Governance frameworks are the driving factors which specify how to govern the organization. The drivers for the governance framework are corporate objectives, regulatory requirements, and SWOT analysis. Process frameworks are those that provide the processes to govern and manage information systems; namely, ITIL, ITSM, and ISMS, while the relevant management frameworks are standards, which a business has to get certified in and/or comply with; namely, ISO 27000, ISO 20000, ISO 9000, and PCI DSS.

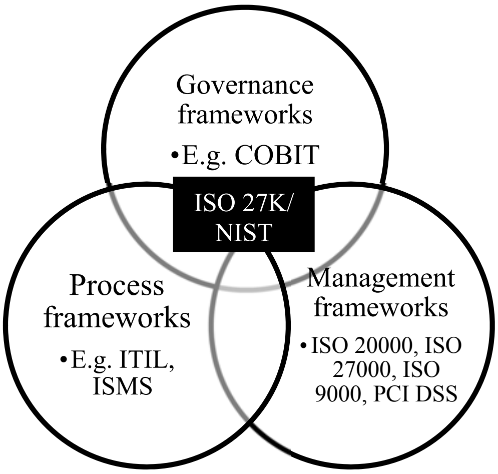


Figure 4. Positioning of framework in the 'Plan' stage of the ISG process

In a security governance model, all the respondents stated the need to have IT controls focused on two standards, namely ISO 27K and the NIST 800 series, with the three framework categories forming the peripheral layer, forming an IS governance system involving the management and

[1] COBIT 5 released in 2012 consolidates and integrates COBIT 4.1, Val IT 2.0 and Risk IT frameworks

[2] ibid

[3] The respondent refers to COBIT 4.1

business. Regarding ISO 27000, respondents unanimously stated the creation of a security management system, to have ‘across-the-board value.’ They recommended organizations to use ISO 27001 since it is considered as the most comprehensive standard focused on security unlike frameworks such as COBIT, which moderately encompasses security from a governance perspective. The inclusion of relevant IT governance controls, implementation guidelines, control objectives for 11 domains, support guidelines for risk management, and guidelines for creating ISMS provide the impetus for deploying relevant ISO 27 K series controls within an ISG model.

Integrating NIST with ISO 27002 has been cited by respondents as the best practice for ISG implementation, principally due to the presence of ‘how to’ guidelines in NIST as well as its technical security focus from a governance perspective. Other relevant drivers include providing a pathway to governance risk and compliance (GRC), technical configurations for IT control implementations, the free availability of NIST (unlike ISO standards) standard, and its global nature.

Regarding the role of the governance framework COBIT in ISG, all the respondents were of the opinion that it helps security from a governance perspective, aligns IT with business, enhance IT strategy and objectives, and support the governance aspect of security. From an IS security perspective, “COBIT assists the IS security personnel to communicate to the management in a language that they are able to understand” (IT Manager). In ISG, COBIT and ITIL have a limited role, where COBIT supports it from a high-level governance perspective while, ITIL supports IS security at the operational level. However, ITIL has limited role in ISG since ITIL’s corresponding management framework “ISO 20000 has a limited impact as it covers only a small aspect of security from a service management perspective” (Director - Strategic Security Consulting). Enterprise architecture is a critical component of the ISG framework since integration of different frameworks and standards requires a framework (TOGAF 9.1). PCI DSS has only optional value to ISG due to its selective application within the financial sector.

Control selection and mapping: This is considered as a continuous process due to the dynamic nature of risks, and threats to the organization’s assets, which require the organization to implement new controls or modify existing controls. Since, controls are selected from different standards and frameworks, the IT manager advised to undertake the selection of IT control process from a business case perspective.

4.1.1.4 Planning subsequent phases

This sub-phase consists of allocating roles and responsibilities, deciding on the governance and audit measurement tools, establishing KPIs and KGIs, and deciding on the security technologies to aid in automation. Some of the questions (that highlights the relevance of measurement tools) raised by the Senior Consultant -Security & Trust are stated as:

> "How are you going to audit it? How you are going to assess it? What is the frequency of assessment? Is it once a year or twice a year? What tools are you are going to use? Is it external auditing, internal auditing, or a combination of both? These are the questions you are going to define in the 'Plan' phase…, again, these questions depend on the organizational assets and business plan."

Respondents unanimously highlighted the role of planning stage wherein each activity during the ISG process is pre-defined, and positioned. This also includes decisions on training, the role of consultants, and the audience for the periodic reports generated through internal and external audits.

4.1.2 'Do' phase

The overarching activity during this phase is the implementation of IT controls. In this regard, this phase is typically about execution (IT controls), where implementing an IT project (as a requirement of IT controls implementation) is not only deploying a tool in place but also encompasses activities like resource training, user training, hardware provisioning, and the initiation of monitoring/measuring the performance (see appendix – 6). Accordingly, this phase:

> "Sets up boundaries or rules on how [the organization is] going to implement it (the plan). Once you have implemented your controls in the form of configuration, in the form of policies, procedures, in the form of tools, you will come to know which hardware/software devices to deploy. For example, once these controls are implemented, you can develop matrices, matrices for your controls, and tools to assess the effectiveness of these controls. Only after its deployment, you can start measuring their performance" (Senior Consultant -Security & Trust).

The Senior Consultant - Security & Trust illustrates the deployment of controls through the deployment of firewalls. He states

> "While implementing a firewall policy, people have to clearly define the policy in terms of configuration, the source of this configuration – whether it came from the industry best practices or [was] customized. And since best practices come from best practices, it should be in the implementation phase, mainly because best practices have to be followed during the implementation of technical, as well as non-technical, controls."

Monitoring of these controls is initiated in the implementation phase (do phase), because once the controls are deployed, the key performance indicators (KPI's) and key goal indicators (KGI's) are created and initiated. Even though allocation of roles and responsibilities are done in the 'Plan' phase, the creation of the RACI matrix, where the people are allocated to respective IT controls, is done at this phase.

4.1.3 'Check' phase

Three predominant themes in the 'Check' phase are monitoring controls, measurement using KPIs and KGIs, and the use of automated tools for measurement and monitoring (see appendix – 7). In this phase, monitoring is based on activities planned in the first phase of the PDCA cycle, especially the audit plan. Monitoring controls enable a business to view the past, present and forecast the future during the risk assessment process. Since the level of risk acceptance changes over time due to changing business and security requirements, one of the best practices suggested by respondents is for the monitoring mechanism to have adequate flexibility to change and improve controls as necessary. Furthermore, it was suggested that an effective monitoring mechanism could show the change in risk appetite over the longer term, as well as the improvements made to the controls to mitigate the changed risk. Respondents also suggested the need to visually track the IT control performance over a period.

In the ISG process, all security parameters have to be monitored using KPIs. From an ISG perspective, respondents highlighted the relevance of KPIs to keep track of the frequent multiple attacks on organizational network and website. In this regard, respondents were unanimous in recommending the practice of measuring relevant ISO 27 K controls from a quantitative perspective. Accordingly, the controls are measured using KPIs and KGI's to enable tracking over time, including "deviations to the KGIs and KPIs."

Automated tools are preferred in the security domain, as it is an efficient method for control, but due to the cost involved, one cannot deploy them the way an organization implements their security program. This is because management must have justification of the investments proposed and undertaken. Thus, respondents, have recommended, as well as cautioned against, automation of the IT controls monitoring process. From a security perspective, the IT Manager did not see the relevance of the automation of controls, since "it would take the security people back to the administrative level." The supporters of automation (Director - Strategic Security Consulting, Senior Consultant - Security & Trust, and Director and CEO) perceived it from a commercial off-the-shelf (COTS) perspective, citing the need for automated multidimensional measurement tools to view and track historical scores. The role of Security Information and Event Management (SIEM) solutions as part of IS governance, was emphasized, and it was stated that organizations were leveraging SIEM solutions not only to track, analyze, and manage how the technical and non-technical controls are being satisfied, but also to take appropriate actions against deviations.

4.1.4 'Act' phase

Best practices in this phase includes modification and updating controls based on internal feedback and changes in the external environment, use of automated tools to serve as dashboards, and reports for decision making. Three major updates in the 'Act' phase are the asset list, security governance steering committee review meetings, and security policy. First, the ISG personnel should update the asset list regularly, which helps them to continually revisit the nature of the risk. During the regular audit phase, some of the things that the auditor should check from an ISG perspective are the review and update of the previous audit asset list, mainly to see any difference between the two asset lists. Second, the auditor needs to checks the outputs of the regular security steering committee review meetings, to look for recommendations. It has been affirmed by the IT Manager, that a lack of recommendation/s typically indicate a non-productive outcome of the steering committee meeting with reference to ISG. In the normal ISG process, during the ‘Act’ phase, “the security governance steering committee meets every month to review the attacks/risks. Moreover, the security environment being highly dynamic, updates would definitely lead to improvement.” Third, due to the changes to the asset list and review meetings, there is a need to update the security policy. Apart from the above, any IS asset, or process that can affect “system effectiveness,” needs to be updated. This includes “penetration testing, access control, vulnerabilities list, scanning for new threats, and password management.”

The ‘Act’ phase is thus “an update based on the ‘Plan’ phase, to search for degrees of variance on each element of the plan” (Director - Strategic Security Consulting). Once the organization detects any degrees of variance, they decide to either accept the variance, or go back to the cycle of ‘Plan’, where the PDCA cycle is started all over again. Subsequently, once the audit report is checked, the controls are left untouched, or updated. In this regard, the Director - Strategic Security Consulting stated:

> “If, from your audit, it is known that the firewall is not good – either the firewall or the firewall security architecture – the security architecture at the perimeter is updated which again leads to the planning stage and the security governance cycle is repeated again.”

Thus, the ‘Act’ phase consists of the review/update process, whose feedback loop differs from the normal IT governance process in its focus of the review, update, and feedback from ISMS systems, mainly the ISO 27K series of standards (see appendix - 8).

4.1.5 Training, best practices, feedback and security governance

Three major themes in training with regard to ISG focus on the objective, training perspective and the training culture. In this regard, respondents commented on the need to train both the IT staff as well as the management with the objective to focus on the ‘dynamic risk’ environment faced by organizations. Accordingly, building an ISG culture involves injecting IT controls into the DNA of the IT security staff and management. Best practices normally involve following the industry practices, competitors and peers and customizing these to the target organization. Respondents have repeatedly emphasized the concept of the feedback loop on the lines of the PDCA. In this regard, they recommend an iterative loop with gradual increment of IT controls in each subsequent PDCA cycle. A significant benefit of “appending ‘IT governance’ in security is to provide end to end security” (Senior Consultant – Security and Trust), since it “does away with a siloed approach” (Director and CEO).

5. Discussion of Propositions

5.1 PDCA cycle

Being the focus of the ISG process (see appendix 3 for the alignment of the propositions with the themes), the proposition of using the PDCA cycle was fully supported by all the respondents (Figure 5). Regarding its use for information security governance, all the respondents supported the cycle model’s four stages of continuous improvement, where they recommended starting with a simple process, followed by additional IT processes as the cycle moves along. Once the ‘Plan’, ‘Do’, and ‘Check’ processes are done, the ‘Act’ stage will materialize automatically in the form of audit and assessment reports that are the outputs of ‘Check’ and, which assists improvement as the process continues its cycle. Here, the advantage of the cycle is the concept of continuous improvement. In this respect, the IT Strategy Manager stated:

> “If you plan it properly, it can never go wrong and the best thing to plan is to start with the simple steps. Start with a few controls, with a small phase in a single domain like the IT department or within the IT department, with certain applications. As you proceed further, increase the scope in the coming years and slowly, gradually cover the entire governance domain. …, and the PDCA cycle ensures this process”

Respondents thus unanimously supported the use of PDCA cycle, citing the ‘continuous improvement’ clause in ISO 27K series standard that must be followed when implementing the ISO 27K series standard. Moreover, the “dynamic threat environment, with hundreds of threats” requires changing the plan on a regular basis. As information security moves to respond to existing and new threats, organizations find that the goal posts are not only moving, but also widened each time, making it very difficult to protect information and its infrastructure (Dlamini, Eloff, & Eloff, 2009).

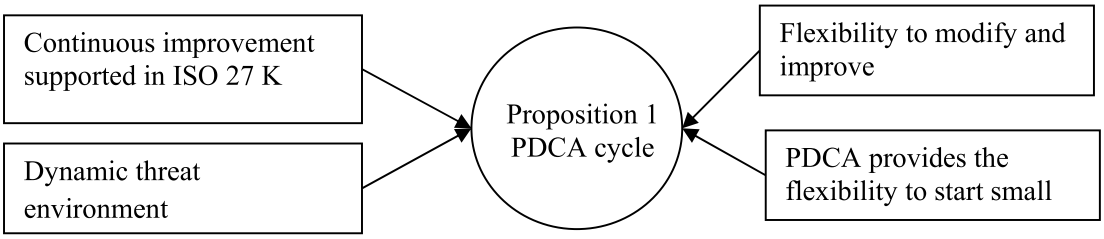

Continuous improvement supported in ISO 27 K
Dynamic threat environment
Proposition 1 PDCA cycle
Flexibility to modify and improve
PDCA provides the flexibility to start small

Figure 5. PDCA cycle in the ISG process

5.2 Risk based perspective of ISG

As discussed in section 4.1.1.2, all respondents stated that the ISG process starts with risk assessment (Figure 6). According to the Director and CEO, “governance starts after risk assessment, because you have a risk and you want to manage it.” It was stated that management should communicate the fact that “risk assessment is the heart of any security program, such that the more effective the risk assessment, the more effective the security program will be” (Senior Consultant - Security & Trust). All respondents reiterated the necessity for a holistic perspective of IS risk in the ISG model due to growing understanding that, managing IT-based risk must be a strategic activity that is not just the responsibility of a small group of IT specialists, but part of a mindset that extends from partners and suppliers to employees and customers (Smith & McKeen, 2009).

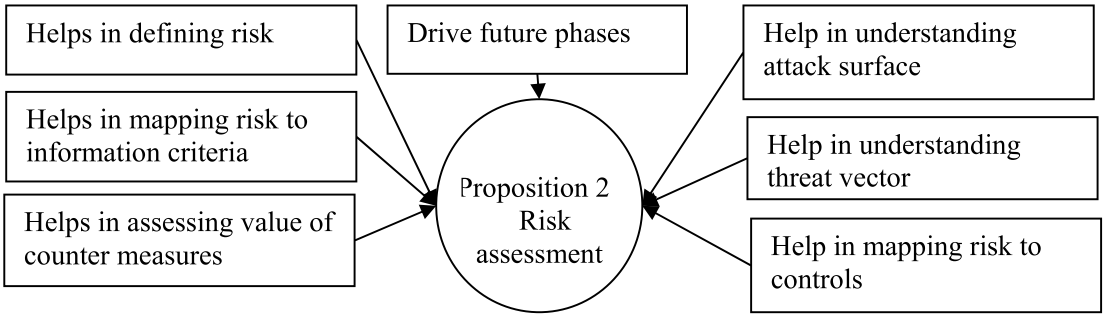

Helps in defining risk
Helps in mapping risk to information criteria
Helps in assessing value of counter measures
Drive future phases
Proposition 2 Risk assessment
Help in understanding attack surface
Help in understanding threat vector
Help in mapping risk to controls

Figure 6. Risk-based perspective of the ISG process

5.3 Select relevant security governance framework

As discussed in detail in section 4.1.1.3, while respondents had differing views on the selection of relevant frameworks due to being in five different business sectors, all of them were unanimous in stating the central role of the ISO 27 K series standards, while two respondents stated the need to include NIST for detailed implementation methodology (Figure 7). Two respondents supported categorizing frameworks, with ISO 27K having a central role in an ISG model. However, all stated the need to select relevant governance and IS frameworks based on industry best practices, to be deployed in the peripheral layer of the ISG model.

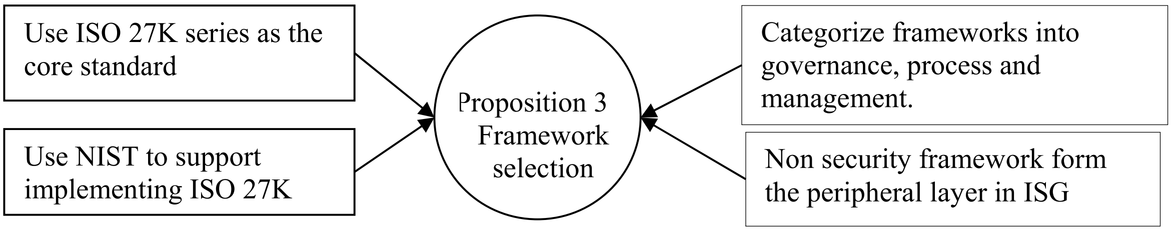

Use ISO 27K series as the core standard
Use NIST to support implementing ISO 27K
Proposition 3 Framework selection
Categorize frameworks into governance, process and management.
Non security framework form the peripheral layer in ISG

Figure 7. Framework selection in ISG process

5.4 Map relevant controls of the ISG

Due to the overlapping nature of controls, the respondents supported control selection and mapping from frameworks and standards (Figure 8). Mapping not only helps in the integration of controls at the same level (horizontal), but also integration between the higher and lower levels IT controls (vertical). In contrast to an IT governance implementation, ISG focuses mainly on ISO 27 K mapping with other IT controls.

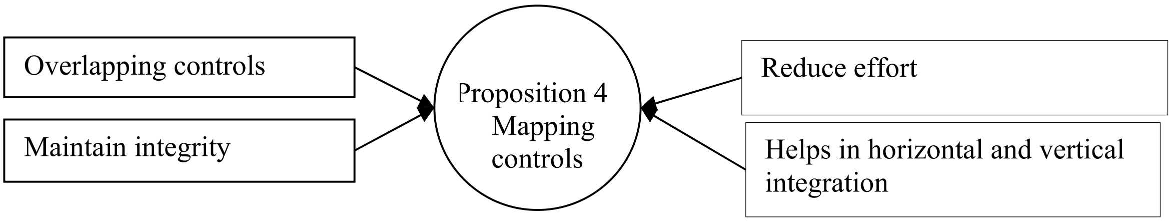


Figure 8. Mapping controls in the ISG process

5.5 Monitoring and measurement

This encompasses the 'Do' and 'Check' phases, in which the monitoring mechanism is initiated in the 'Do' phase, while measurement and tracking are done in the 'Check' phase (Figure 9). All respondents supported Proposition 5, which focuses on the automation and tracking of security-related IT controls. They saw this as an effective technique for security threat detection, monitoring and control.

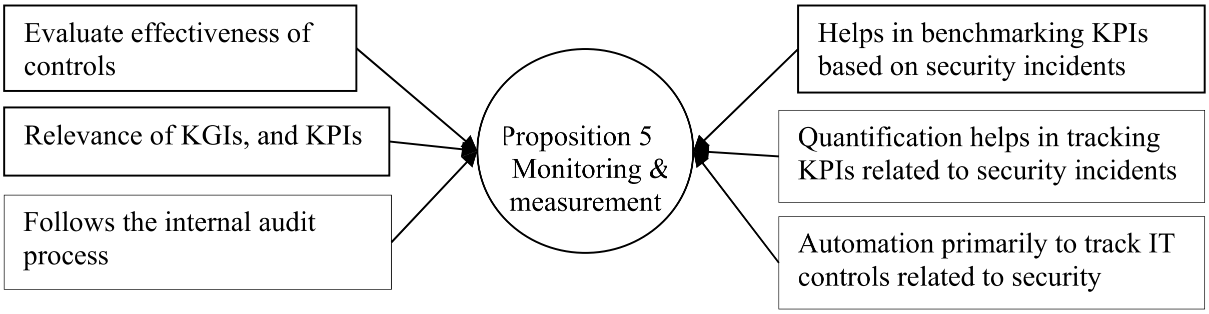

Evaluate effectiveness of controls
Relevance of KGIs, and KPIs
Follows the internal audit process
Proposition 5
Monitoring &
measurement
Helps in benchmarking KPIs based on security incidents
Quantification helps in tracking KPIs related to security incidents
Automation primarily to track IT controls related to security

Figure 9. Monitoring and measurement in the ISG process

5.6 Feedback loop

The concept of having a feedback loop was unanimously supported, due to the highly dynamic nature of IS security threats emanating from external, as well as internal, sources (Figure 10). The 'Act' phase takes in the output of the 'Check' phase, process it, and provide it as an input to the subsequent 'Plan' phase.

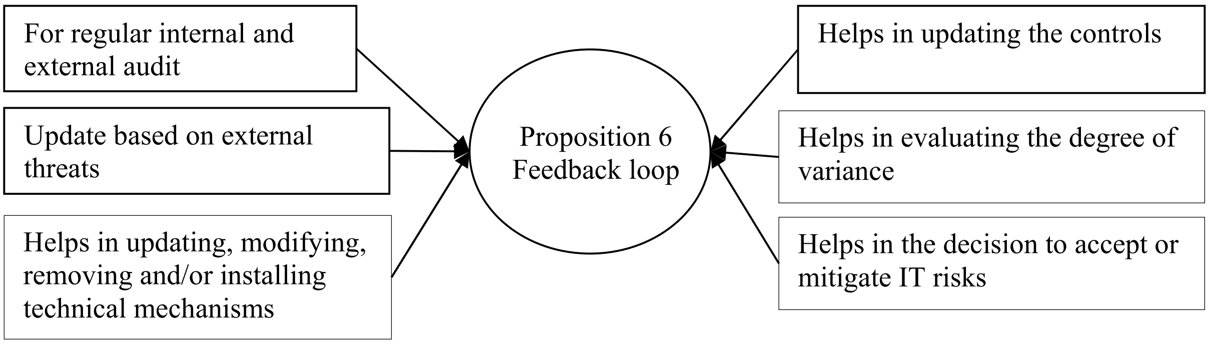

For regular internal and external audit
Update based on external threats
Helps in updating, modifying, removing and/or installing technical mechanisms
Proposition 6
Feedback loop
Helps in updating the controls
Helps in evaluating the degree of variance
Helps in the decision to accept or mitigate IT risks

Figure 10. The role of feedback loop in the ISG process

5.7 Security culture

The concept of an ISG oriented security culture was supported by all the respondents. In this respect, the IT Manager stated that security culture "should be injected into the DNA of the IT security division, the management, and the employees" helping them to follow the security controls (Figure 11). From a management perspective, security culture helps the management understand IT risks, as well as understands the need for investments in IT security. Regarding training, respondents did not delve into the specifics of training to impart at different managerial levels.

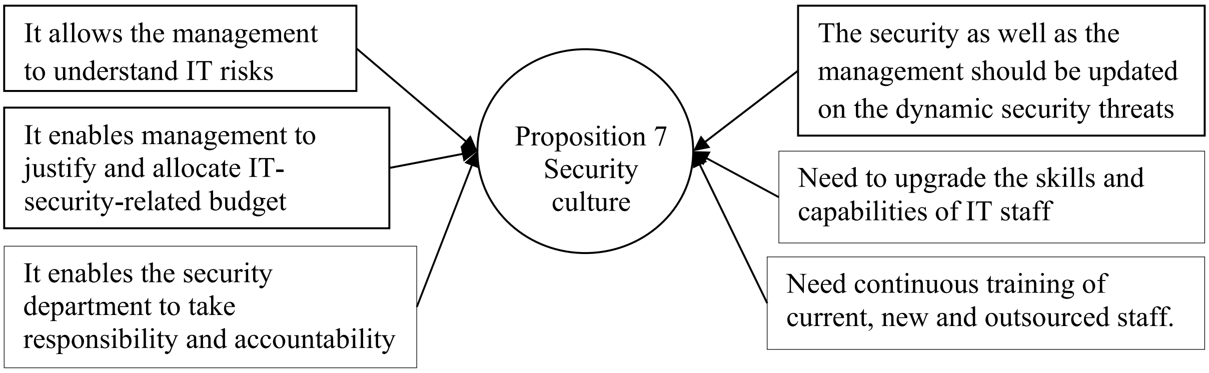

It allows the management to understand IT risks
It enables management to justify and allocate IT-security-related budget
It enables the security department to take responsibility and accountability
Proposition 7 Security culture
The security as well as the management should be updated on the dynamic security threats
Need to upgrade the skills and capabilities of IT staff
Need continuous training of current, new and outsourced staff.

Figure 11. Relevance of security culture in the ISG process

5.8 Best practices

Respondents supported the use of training to impart the use of best practices, a step that is predominantly employed in the 'Do' phase (Figure 12), but also evident in subsequent phases. From an ISG perspective, optimal implementation of IT security policies, technical safeguards like firewall policies and configuration come from best practices. However, the Senior Consultant - Security & Trust stated that the "best practices should come during implementation, in the 'Do' phase, because best practices mostly happen at the technical side." According to the Director and CEO:

> "You look at what industry practitioners are doing, what competitors are doing, what your peers are doing what the industry generally do. It is a good guideline to follow, but you have to be very careful about it because if you just copy, it may not work for you. It has to be customized for you, but it's good to have guidelines."

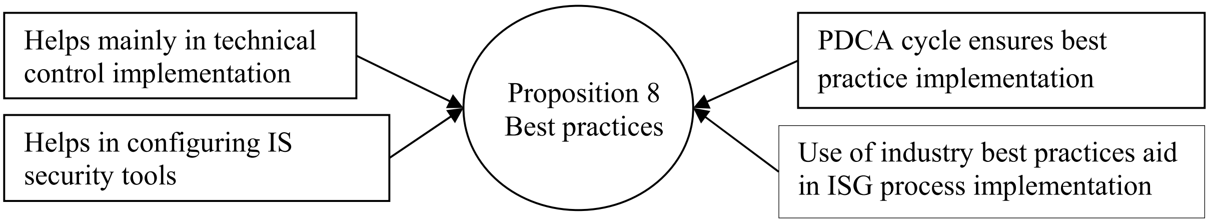

Helps mainly in technical control implementation
Helps in configuring IS security tools
Proposition 8 Best practices
PDCA cycle ensures best practice implementation
Use of industry best practices aid in ISG process implementation

Figure 12. Best practices in the ISG process

Governance in security

Success of information security depends on whether it is perceived from an ISG perspective. Governance is the cornerstone of ISG, as "without governance this whole concept of information security governance, will not be possible, as it will tear apart" (Senior Consultant: Security & Trust). Hence, "if each department is responsible for its own security, there is no governance, leading to non-uniformity where one department is very good, the other one not," for a chain is only as strong as its weakest link (Senior Consultant: Security & Trust). Accordingly, the IT Manager stated the "importance of 'governance' in information security governance, which provides vertical, as well as horizontal, end-to-end security." Accordingly, ISG implementation should be regarded as a "phased approach, starting with the implementation of IS security controls (ISO 27K and NIST) in the IT department, covering critical assets and gradually increasing the scope to cover other departments' assets" (IT Strategy Manager). This should be followed by progressively expanding the scope to "cover relevant IT governance frameworks, which is how it [ISG] works" (IT Strategy Manager)

Out of the eight propositions, five propositions (1, 2, 6, 7, and 8) were fully supported by all of the respondents, while the other three (3, 5, and 9) were supported with exceptions (summarized in Table 2).

Table 2. Validation of the eight propositions

1. Implementing ISG through the Plan Do Check Act cycle;	Fully supported by all respondents.
2. Viewing IT governance security from a risk based perspective;	Fully supported by all respondents.
3. Selecting relevant IS security and governance frameworks (technical as well as non-technical);	Supported by all respondents with exceptions. All respondents were unanimous in stating the central role of the ISO 27 K series standards, while two respondents stated the need to include NIST for detailed implementation methodology.
4. Mapping relevant IT controls of ISG frameworks and standards;	All respondents supported this proposition, but with exceptions. In this regard, two respondents stated that the focus of the ISG model should be mapping ISO 27 K/NIST IT controls with relevant IT controls from a horizontal as well as vertical perspective.
5. Implementing a measurement framework for tracking and monitoring IS security governance entities using quantifiable metrics;	All respondents supported this proposition with exceptions. However, three respondents stated the need to track and monitor IT security controls through automation, while automating IT governance controls should be left at the discretion of the organization.
6. A feedback loop that takes in the outputs from the 'Check' phase to provide	Fully supported by all respondents.

corrective actions;	
7. Making sure that the people involved in the ISG framework share a security culture through continuous, multi-level, optimally-crafted, technical and non-technical training;	Supported by all respondents, to the extent of imparting training at all levels, but respondents did not specify the need for multi-level, optimally crafted, technical and non-technical training.
8. Using best practices in the industry to implement ISG in each stage of the PDCA cycle.	Fully supported by all respondents without reservations.

6. Conclusion and Future Research

This study, primarily conducted to empirically validate the ISG process model derived from the extant literature confirms the relevance of integrating IT governance controls into IS security resulting in a phased methodology to implement ISG. First, the paper confirms the role of the Plan-Do-Check-Act Deming cycle in ISG where concepts of IS security and IT governance were conspicuous throughout the ISG process model. Second, the study provides guidelines/best practices to consider in each phase of the PDCA cycle. Third, the relevance of an automated feedback mechanism using appropriate metrics throughput the cycle was methodologically demonstrated. Fourth, the research affirms the relevance of inculcating an IT security as well as IT governance culture in any organization prior and during the process of ISG. Finally, the guidelines provided in the study aid in continuously updating the model to align with the highly dynamic nature of information security threats.

The validated model helps academics, and practitioners gain insight into the methodology of the phased implementation of an information systems governance process through the PDCA model, as well as the positioning of ITG and ITG frameworks in ISG. Practitioners can glean valuable insights from the empirical section of the research where experts detail the critical success factors, the subsequent steps, and justifications of each factor on the ISG implementation process. This can assist practitioners in incrementing and building an ISG knowledge base to apply the steps outlined in each of the four phases of PDCA.

Our study highlights several directions for future research. First, since the practices in the PDCA cycle may differ between countries, mainly due to the country-specific governance regulations and compliance, extension to this study is encouraged in this direction. Second, respondents have provided numerous best practices and guidelines during the empirical model validation process. In this regard, we encourage researchers to collate these, differentiate between success factors, critical success factors, and undertake ranking using Delphi research for the four phases of PDCA cycle. Third, further empirical studies in different sectors are required to come up with sector-wide positioning of different ISG frameworks and models (see Figure 4). Finally, while the role of training has been emphasized for both IT staff and the management to ensure a balanced approach in IS security and business needs, the 'what' and 'how' trainings is a promising area of research. Since, ISG frameworks have been categorized into operational, tactical and strategic levels in the literature, researchers can delve into categorizing the best practices and guidelines that have been stated in PDCA process of ISG into the three levels. We hope that the proposed ISG process model support and assist the governance and security managers to successfully implement ISG in a phased manner incorporating appropriate IT governance controls into IS security.

Our study is not without its limitations. First, the study was done in one country (UAE) in the services sector, which may not be generalized to other countries, or sectors. Hence, validation of the model in different regions and sectors is recommended to arrive at a core set of global and region-centric factors. Second, the core IS security controls may not depend on ISO 27K series standard, as different countries may adopt different IS security standards. The above limitations notwithstanding, we believe that the results reported in this paper adds to the understanding of how IS security governance can be implemented in a phased cyclical manner to successfully address the dynamic nature of IS security threats.

7. References

Abu-Musa, A. (2010). Information Security Governance in Saudi organizations: An Empirical Study. *Information Management & Computer Security, 18*(4), 226-276.

Al Hogail, A. (2015). Design and validation of information security culture framework. *Computers in Human Behavior, 49*, 567-575.

Chen, P.-y., Kataria, G., & Krishnan, R. (2011). Correlated Failures, Diversification, and Information Security Risk Management. *MIS Quarterly, 35*(2), 397-422.

Choobineh, J., Anderson, E., & Grimaila, M. R. (2010). *Security Management Life Cycle (SMLC): A Comparative Study.* Paper presented at the Americas Conference on Information Systems, Lima, Peru.

Choobineh, J., Dhillon, G., Grimaila, M. R., & Rees, J. (2007). Management of Information Security: Challenges and Research Directions1. *Communications of the Association for Information Systems, 20*(57), 958- 971.

Cone, B. D., Irvine, C. E., Thompson, M. F., & Nguyen, T. D. (2007). A Video Game for Cyber Security Training and Awareness. *Computers & Security, 26*, 63-72.

DeLone, W. H., & McLean, E. R. (2003). The DeLone and McLean Model of Information Systems Success: A Ten-Year Update. *Journal of Management Information Systems, 19*(4), 9-30.

Dhillon, G., & Backhouse:, J. (2001). Current Directions in IS Security Research: Towards Socio-Organizational Perspectives. *Information Systems Journal, 11*(2), 127-154

Dlamini, M., Eloff, J. H., & Eloff, M. M. (2009). Information Security: The moving Target. *Computers & Security, 28*(3), 189-198.

Dlamini, M. T., Eloff, J. H. P., & Eloff, M. M. (2007). Information Security: The Moving Target. *Computers & Security, 28*(3-4), 189-198.

Dorussen, H., Lenz, H., & Blavoukos, S. (2005). Assessing the reliability and validity of expert interviews. *European Union Politics, 6*(3), 315-337.

dos Santos Moreira, E., Andréia Fondazzi Martimiano, L., José dos Santos Brandão, A., & César Bernardes, M. (2008). Ontologies for information security management and governance. *Information Management & Computer Security, 16*(2), 150-165.

Firestone, W. A. (1987). Meaning in Method: The Rhetoric of Quantitative and Qualitative Research. *Educational Researcher, 16*(7), 16-21.

Flores, W. R., Antonsen, E., & Ekstedt, M. (2014). Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture. *Computers & Security, 43*, 90-110.

Gebrasilase, T., & Lessa, L. F. (2011). Information Security Culture in Public Hospitals: The Case of Hawassa Referral Hospital. *The African Journal of Information Systems, 3*(3), 1.

Geer Jr, D., Hoo, K. S., & Jaquith, A. (2003). Information Security: Why the Future Belongs to the Quants. *Security & Privacy, IEEE, 1*(4), 24-32.

Gikas, C. (2010). A General Comparison of FISMA, HIPAA, ISO 27000 and PCI DSS Standards. *Information Systems Journal, 19*(3), 132-141.

Gorla, N., & Somers, T. M. (2014). The impact of IT outsourcing on information systems success. *Information & Management, 51*(3), 320-335.

Gregor, S. (2002). A theory of theories in information systems. *Information Systems Foundations: building the theoretical base*, 1-20.

Grembergen, W. V., & Haes, S. D. (2009). *Enterprise Governance of Information Technology*. New York: Springer Science.

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*(2), 203-236.

Iden, J., & Langeland, L. (2010). Setting the Stage for a Successful ITIL Adoption: A Delphi Study of IT Experts in the Norwegian Armed Forces. *Information Systems Management, 27*(2), 103-112. Retrieved from <Go to ISI>://000277476400003

Ifinedo, P. (2009). Information technology security management concerns in global financial services institutions Is national culture a differentiator? *Information Management & Computer Security, 17*(5), 372-387.

International Standards Organization. (2013). ISO 27000 - An Introduction to ISO 27001 / ISO27001. Retrieved from http://www.27000.org/iso-27001.htm

ISACA, I. (2011). Global Status Report on the Governance of Enterprise IT (GEIT)—2011. *Available on line at http://www. isaca. org/Knowledge-Center/Research/Documents/Global-Status-Report-GEIT-10Jan2011-Research. pdf.*

ISO. (2011). ISO/IEC 27002:2005. Retrieved from http://www.iso.org/iso/catalogue_detail?csnumber=50297

IT Governance Institute. (2006). *Information Security Governance: Guidance for Boards of Directors and Executive Management* (2 ed.). Rolling Meadows, Illinois: IT Governance Institute.

Johnston, A. C., & Hale, R. (2009). Improved Security Through Information Security Governance. *Communications of the ACM, 52*(1), 126-129.

Kohnke, A., & Shoemaker, D. (2015). Making Cybersecurity Effective: The Five Governing Principles for Implementing Practical IT Governance and Control. *EDPACS, 52*(3), 9-17.

Kruger, H., & Kearney, W. (2006). A Prototype for Assessing Information Security Awareness. *Computers & Security, 25*(4), 289-296.

Laredo, V. G. (2009). PCI DSS compliance: a matter of strategy. *Card Technology Today, 20*(4), 9.

Luftman, J., & Brier, T. (1999). Acheiving and Sustaining Business-IT Alignment. *California Management Review, 1*(Fall), 109-122.

Luftman, J. N., Lewis, P. R., & Oldach, S. H. (1993). Transforming the enterprise: the alignment of business and information technology strategies. *IBM Systems Journal archive, 32*(1).

Markus, L., Tanis, S., Petrie, D., & Tanis, C. (2000). Learning from Adopters' Experiences with ERP: Problems Encountered and Success Achieved. *Journal of Information Technology 15*(4), 245-265.

Mataracioglu, T., & Ozkan, S. (2011). Governing Information Security in Conjunction with COBIT and ISO 27001. *International Journal of Network Security & Its Applications 3*(4).

Merhout, J. W., & Havelka, D. (2008). Information Technology Auditing: A Value Added IT Governance Partnership between IT Management and Audit. *Communications of the AIS, 23*(26), 463-482.

Meuser, M., & Nagel, U. (2009). The expert interview and changes in knowledge production *Interviewing experts* (pp. 17-42): Springer.

Mishra, S., & Dhillon, G. (2006). *Information Systems Security Governance Research: A Behavioral Perspective.* Paper presented at the 1st Annual Symposium on Information Assurance, Academic Track of 9th Annual NYS Cyber Security Conference.

Mishra, S., & Weistroffer, H. R. (2007). A Framework for Integrating Sarbanes-Oxley Compliance into the Systems Development Process. *Communications of the Association for Information Systems, 20*.

Moulton, R., & Coles, R. S. (2003). Applying Information Security Governance. *Computers & Security, 22*(7), 580-584.

Nicho, M. (2012). *An optimized dynamic process model of IS security governance implementation.* Paper presented at the CONF-IRM 2012Proceedings.

Nicho, M., & Avinash, A. (2012). *A Data Centric Security Cycle Model for Data Loss Prevention of Custodial Data and Company Intellectual Property.* Paper presented at the SECURWARE 2012: The Sixth International Conference on Emerging Security Information, Systems and Technologies A.

Niekerk, J. F. V., & Solms, R. V. (2010). Information Security Culture: A Management Perspective. *Computers & Security 29*, 4 7 6 - 4 8 6.

Nor Aza, R., & Normaziah, A. A. (2012). *Risk Identification for an Information Security Management System Implementation.* Paper presented at the SECURWARE 2012, The Sixth International Conference on Emerging Security Information, Systems and Technologies.

Paans, I. R., & Herschberg, I. S. (1987). Computer Security: The Long Road Ahead. *Computers & Security, 6*(5), 403-416.

Pederson, K., Kraemmergaard, P., Lynge, B. C., & Schou, C. D. (2010). ITIL Implemntation: Critical Success Factors - A Comparative Case Study Using the BPC Framework. *Journal of Information Technology: Case and Application Research, 12*(2), 11-35.

Peltier, T. R. (2005). Implementing an Information Security Awareness Program. *Information Systems Security, 14*(2), 37-49.

Posthumus, S., & Solms, R. v. (2004). A Framework for the Governance of Information Security. *Computers and Security, 23*, 638 - 646.

Rebollo, O., Mellado, D., & Fernández-Medina, E. (2012). A Systematic Review of Information Security Governance Frameworks in the Cloud Computing Environment. *J. UCS, 18*(6), 798-815.

Rebollo, O., Mellado, D., Fernández-Medina, E., & Mouratidis, H. (2015). Empirical evaluation of a cloud computing information security governance framework. *Information and Software Technology, 58*, 44-57.

Sahibudin, S., Sharifi, M., & Ayat, M. (2008). *Combining ITIL, COBIT and ISO/IEC 27002 in Order to Design a Comprehensive IT Framework in Organizations.* Paper presented at the Second Asia International Conference on Modelling & Simulation, Malaysia.

Savola, R. M. (2013). Quality of Security Metrics and Measurements. *Computers & Security, 37*, 78-90.

Simonsson, M., Johnson, P., & Wijkstrom, H. (2007). *Model Based IT Governance Maturity Assessments With COBIT.* Paper presented at the 15th European Conference on Information Systems, Switzerland.

Singleton, J. P., McLean, E. R., & Altman, E. N. (1988). Measuring Information Systems Performance: Experience with the Management by Results System at Security Pacific Bank. *MIS Quarterly, 12*(2), 325-337.

Siponen, M. T. (2000). A Conceptual Foundation for Organizational Information Security Awareness. *Information Management & Computer Security, 8*(1), 31-41.

Smith, H. A., & McKeen, J. D. (2009). Developments in Practice XXXIII: A Holistic Approach to Managing IT-based Risk. *Communications of the Association for Information Systems, 25*.

Solms, B. (2005). Information Security Governance- Compliance Management vs Operational Management. *Computers and Security, 24*, 443-447.

Solms, B. v. (2001). Information Security – A Multidimensional Discipline. *Computers & Security, 20*, 504-508.

Spremić, M. (2013). *Holistic Approach for Governing Information System Security.* Paper presented at the Proceedings of the World Congress on Engineering.

Straub, D., & Welke, R. (1998). Coping with Systems Risk: Security Planning Models for Management Decision-Making :Working paper version. *MIS Quarterly, 22*(4), 441-469.

Sullivan, R. J. (2010, May 21). *The Changing Nature Of U.S. Card Payment Fraud: Issues For Industry And Public Policy.* . Paper presented at the Workshop on the Economics of Information Security Harvard University.

Tan, W.-G., Cater-Steel, A., & Toleman, M. (2009). Implementing IT Service Management: A Case Study Focussing on Critical Success Factors. *The Journal of Computer Information Systems, 50*(2), 1-12.

Thomson, M. E., & R. von Solms. (1998). Information Security Awareness: Educating Your Users Effectively. *Information Management & Computer Security, 6*(4), 167-173.

Torres, J. M., Sarriegi, J. M., Santos, J., & Serrano, N. (2006). Managing Information Systems Security: Critical Success Factors and Indicators to Measure Effectiveness *Information Security* (pp. 530-545): Springer.

Turner, M. J., Oltsik, J., & McKnight, J. (2009). Security Management Survey: ISO, ITIL and COBIT Triple Play Fosters Optimal Security Management Execution Retrieved from http://www.bsmreview.com/security_best_practice_survey.shtml

Urquhart, C. (2001). An Encounter with Grounded Theory: Tackling the Practical and Philosophical Issues. *Qualitative Research in IS: Issues and trends*, 104-140.

Veiga, A. D., & Eloff, J. H. (2007). An Information Security Governance Framework. *Information Systems Management, 24*(4), 361-372.

Veiga, A. D., & Eloff, J. H. P. (2010). A Framework and Assessment Instrument for Information Security Culture. *Computers & Security, 29*, 196-207.

Verizon. (2012). 2012 Data Breach Investigations Report. Retrieved from http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf

von Solms, R., & von Solms, S. H. (2006). Information Security Governance: A Model Based on the Direct–Control Cycle. *Computers & Security, 25*(6), 408-412.

Wahyuni, D. (2012). The Research Design Maze: Understanding Paradigms, Cases, Methods and Methodologies.

Wang, C., & Wulf, W. A. (1997). *Towards a Framework for Security Measurement.* Paper presented at the 20th National Information Systems Security Conference, Baltimore, MD.

Whitman, M., & Mattord, H. J. (2014). Information Security Governance for the Non-Security Business Executive.

Whittaker, S. (2006). Qualitative Researchin Transfusion Medicine: Closing the Gap *ISBT Science Series, 1*, 133 - 139.

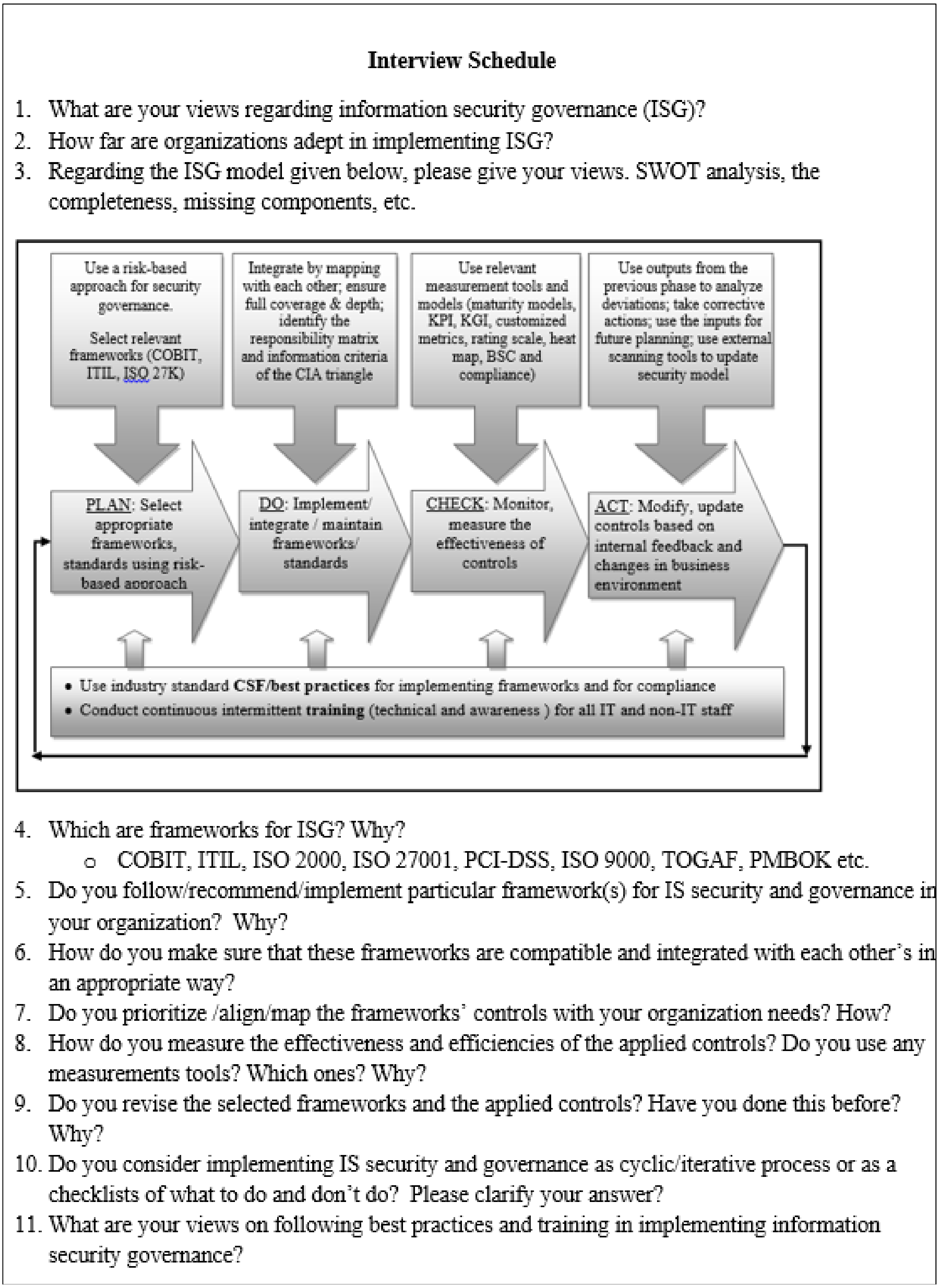
Williams, P. (2001). Information Security Governance. *Information security technical report, 6*(3), 60-70.

Wilson, P. (2007). Governance and Security: Side by Side. *Computer Fraud & Security*(April).

Wu, S. M., Guo, D., Lin, W. T., & Li, M.-H. (2015). Web-Based Analytic Hierarchy Process (AHP) Assessment Model for Information Security Policy of Commercial Banks.

Yadav, S. B. (2010). A Six-View Perspective Framework for System Security: Issues Risks and Requirements. *International Journal of Information Security and Privacy, 4*(1), 61-92.

Appendix – 1



Interview Schedule

1. What are your views regarding information security governance (ISG)?
2. How far are organizations adept in implementing ISG?
3. Regarding the ISG model given below, please give your views. SWOT analysis, the completeness, missing components, etc.

Use a risk-based approach for security governance.

Select relevant frameworks (COBIT, ITIL, ISO 27K)

Integrate by mapping with each other; ensure full coverage & depth; identify the responsibility matrix and information criteria of the CIA triangle

Use relevant measurement tools and models (maturity models, KPI, KGI, customized metrics, rating scale, heat map, BSC and compliance)

Use outputs from the previous phase to analyze deviations; take corrective actions; use the inputs for future planning; use external scanning tools to update security model

PLAN: Select appropriate frameworks, standards using risk-based approach

DO: Implement/ integrate / maintain frameworks/ standards

CHECK: Monitor, measure the effectiveness of controls

ACT: Modify, update controls based on internal feedback and changes in business environment

- Use industry standard **CSF/best practices** for implementing frameworks and for compliance
- Conduct continuous intermittent **training** (technical and awareness) for all IT and non-IT staff

4. Which are frameworks for ISG? Why?
    - COBIT, ITIL, ISO 2000, ISO 27001, PCI-DSS, ISO 9000, TOGAF, PMBOK etc.
5. Do you follow/recommend/implement particular framework(s) for IS security and governance in your organization? Why?
6. How do you make sure that these frameworks are compatible and integrated with each other's in an appropriate way?
7. Do you prioritize /align/map the frameworks' controls with your organization needs? How?
8. How do you measure the effectiveness and efficiencies of the applied controls? Do you use any measurements tools? Which ones? Why?
9. Do you revise the selected frameworks and the applied controls? Have you done this before? Why?
10. Do you consider implementing IS security and governance as cyclic/iterative process or as a checklists of what to do and don't do? Please clarify your answer?
11. What are your views on following best practices and training in implementing information security governance?

Appendix – 2

Mapping of interview questions with propositions

			Questions											
			1	2	3	4	5	6	7	8	9	10	11	Ots
Propositions	1	PDCA			✓							✓		
	2	Risk			✓							✓		
	3	Frameworks /Stds			✓	✓	✓							
	4	Integration			✓			✓	✓					
	5	Monitoring			✓					✓	✓			
	6	Feedback			✓						✓			
	7	Training			✓								✓	
	8	Best practices			✓								✓	
		Introductory questions	✓	✓										

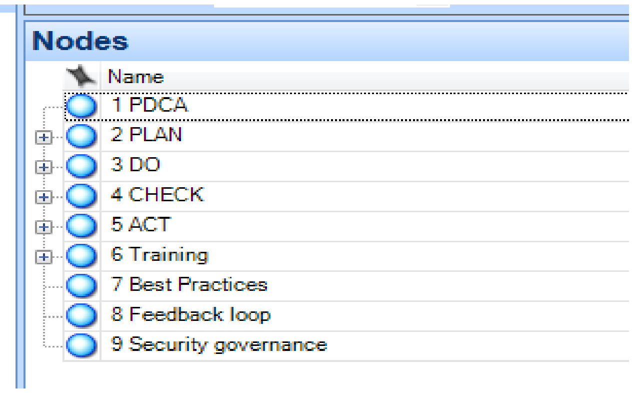
Appendix 3

Mapping of the pre determined themes with the propositions

		P1	P2	P3	P4	P5	P6	P7	P8
	Plan	✓	✓	✓					
	Do	✓			✓	✓	✓		
	Check	✓				✓	✓		
	Act	✓					✓		
	Training							✓	
	Best practices								✓
	Feedback loop						✓		
	ISG								

Appendix – 4

The pre defined themes



Nodes

Name

1 PDCA

2 PLAN

3 DO

4 CHECK

5 ACT

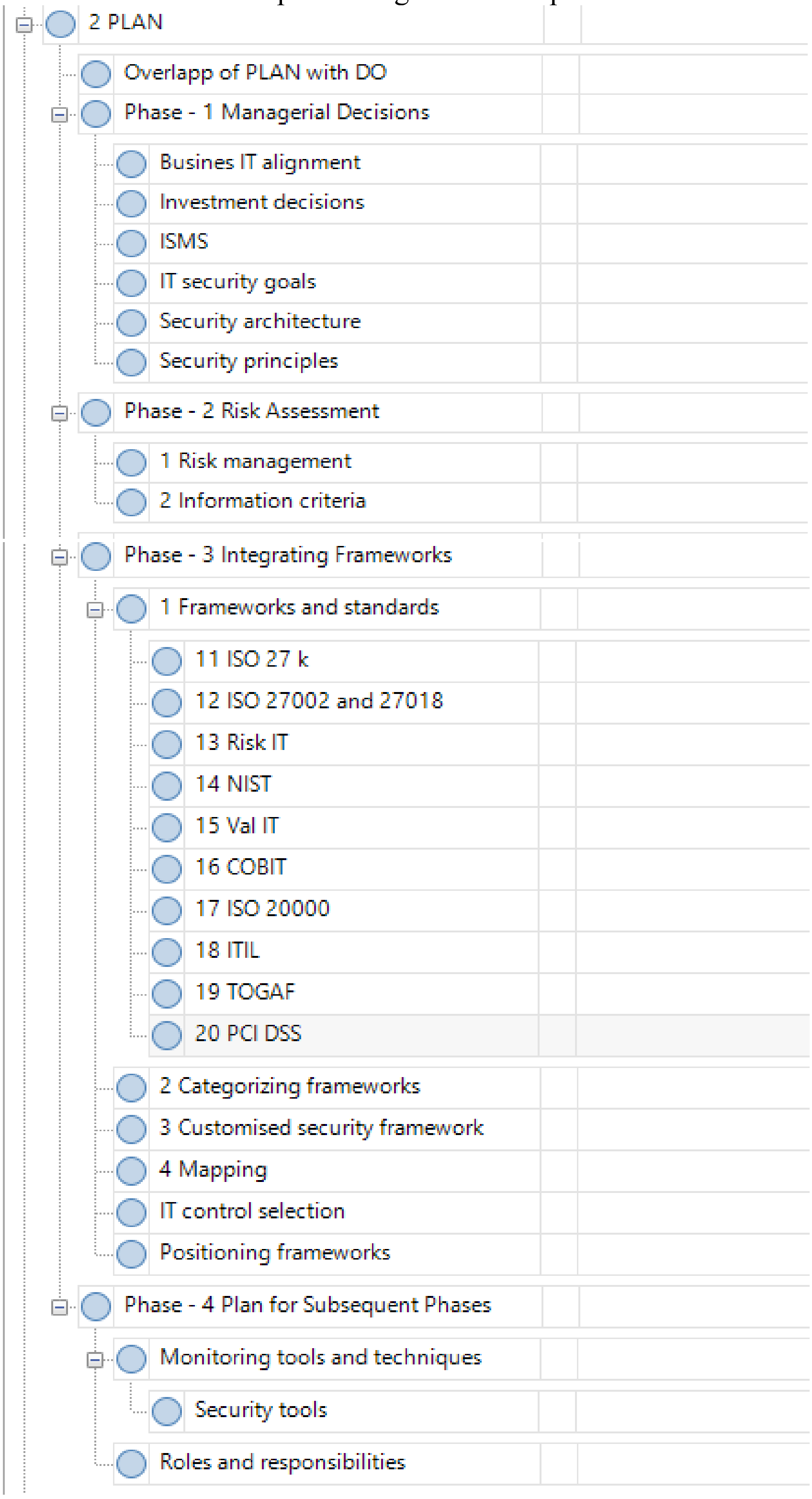
6 Training

7 Best Practices

8 Feedback loop

9 Security governance

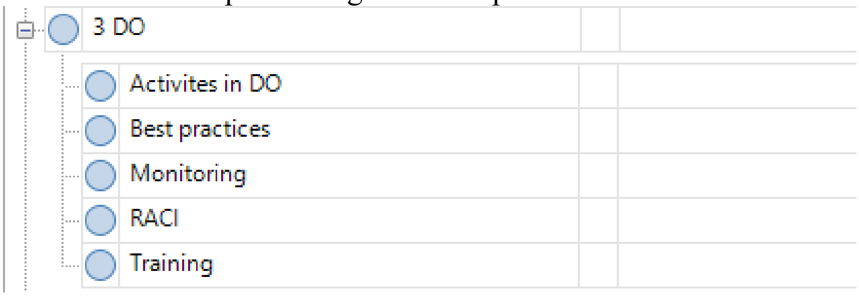
Appendix – 5
Open coding at the Plan phase



- 2 PLAN
  - Overlapp of PLAN with DO
  - Phase - 1 Managerial Decisions
    - Busines IT alignment
    - Investment decisions
    - ISMS
    - IT security goals
    - Security architecture
    - Security principles
  - Phase - 2 Risk Assessment
    - 1 Risk management
    - 2 Information criteria
  - Phase - 3 Integrating Frameworks
    - 1 Frameworks and standards
      - 11 ISO 27 k
      - 12 ISO 27002 and 27018
      - 13 Risk IT
      - 14 NIST
      - 15 Val IT
      - 16 COBIT
      - 17 ISO 20000
      - 18 ITIL
      - 19 TOGAF
      - 20 PCI DSS
    - 2 Categorizing frameworks
    - 3 Customised security framework
    - 4 Mapping
    - IT control selection
    - Positioning frameworks
  - Phase - 4 Plan for Subsequent Phases
    - Monitoring tools and techniques
      - Security tools
    - Roles and responsibilities

Appendix – 6

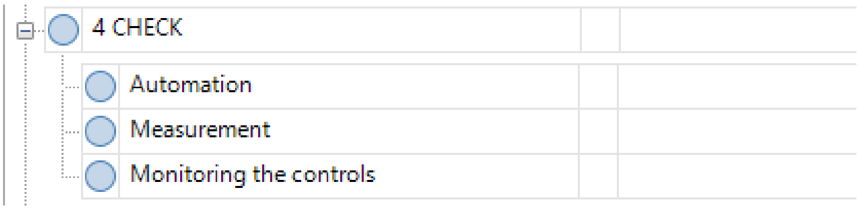
Open coding at the Do phase



- 3 DO
  - Activites in DO
  - Best practices
  - Monitoring
  - RACI
  - Training

Appendix – 7

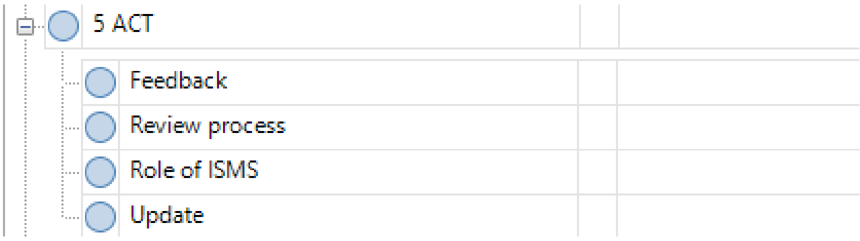
Open coding at the Check phase



- 4 CHECK
  - Automation
  - Measurement
  - Monitoring the controls

Appendix – 8

Open coding at the Act phase



- 5 ACT
  - Feedback
  - Review process
  - Role of ISMS
  - Update