Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

Information security policy development and implementation: The what, how and who

Stephen V. Flowerday *, Tite Tuyikeze

Department of Information Systems, University of Fort Hare, 50 Church Street, East London, 5241, South Africa

ARTICLE INFO

Article history:
Received 8 May 2015
Received in revised form 15 April 2016
Accepted 7 June 2016
Available online 20 June 2016

Keywords:
Security policy development
Security policy implementation
Security policy life cycle
Security policy management
Risk assessment

ABSTRACT

The development of an information security policy involves more than mere policy formulation and implementation. Unless organisations explicitly recognise the various steps required in the development of a security policy, they run the risk of developing a policy that is poorly thought out, incomplete, redundant and irrelevant, and which will not be fully supported by the users. This paper argues that an information security policy has an entire life cycle through which it must pass during its useful lifetime. A formal content analysis of information security policy development methods was conducted using secondary sources. Based on the results of the content analysis, a conceptual framework was subsequently developed. The proposed framework outlines the various constructs required in the development and implementation of an effective information security policy. In the course of this study, a survey of 310 security professionals was conducted in order to validate and refine the concepts contained in the key component of the framework: the ISPDLC.

1. Introduction

Organisations today are more dependent than ever on Information Technology (IT) as IT supports their day-to-day transactions as well as numerous other critical business functions. According to Doughty and Grieco (2005), “IT should be seen as a way for increasing the accessibility, speed and comprehensiveness of information that supports the decision-making processes within the organisation”. However, the dependency on IT has unfortunately resulted in an increase in potential threats to organisations’ information assets.

A 2014 cybercrime survey in the United States of America found that more damage was caused by insider attacks than by outsider attacks, with insider involvement comprising the highest percentage of damage in the following incidents: private or sensitive information unintentionally exposed (82%); confidential records compromised or stolen (76%); customer records compromised or stolen (71%); and employee records compromised or stolen (63%) (CERT Insider Threat Center, 2014). Based on the findings of this survey, it is evident that organisations must have security controls in place to ensure the confidentiality, integrity and availability of their information.

This paper posits that one important mechanism for protecting organisations’ information assets is the formulation and implementation of an effective information security policy. The main contribution made by this paper is the proposal of a key component “1” in the framework termed the “Information Security Policy Development Life Cycle” (ISPDLC – Fig. 2). This framework indicates the various constructs that information security practitioners need to consider in the development and implementation of an effective information security policy.

The remainder of this paper is structured as follows: The background to an information security policy is discussed in Section 2, Section 3 describes the research methodology, and Section 4 covers the constructs of the proposed component

* Corresponding author.
E-mail addresses: sflowerday@ufh.ac.za (S.V. Flowerday), nyonitite@gmail.com (T. Tuyikeze).

http://dx.doi.org/10.1016/j.cose.2016.06.002
0167-4048/© 2016 Elsevier Ltd. All rights reserved.

(ISPDLC). The relationship between the constructs of the ISPDLC is highlighted in Section 5, while Section 6 highlights the stakeholders that are involved in the development and implementation of the information security policy. Finally, Sections 7 and 8 discuss the findings and offer a conclusion.

2. Information security policy

The literature contains many definitions for an information security policy. Chen and Li (2014) state that an information security policy is used by management to differentiate between employee behaviours that are either permitted or prohibited, as well as the consequent sanctions if the forbidden behaviours take place. On the other hand, ISO/IEC 27002 (2013) states that the objective of an information security policy is to provide management with direction and support in accordance with business requirements and regulations when dealing with information security. As highlighted in these two definitions, it is clear that an information security policy contributes significantly to the well-being of an organisation when protecting its information. However, the processes involved in developing and implementing an effective information security policy are difficult at best.

The existing literature concentrates on describing the structure and content of a security policy, but fails, in general, to describe in detail the processes for developing the policy. Consequently, there is little guidance for the people involved in information security policy development with regard to the processes they should follow.

In view of this lack of guidance, the developers of such policies often use those developed by other organisations, commercially available sources, or templates available from public sources such as the Internet. However, the document that results from such methods will not provide proper direction for the information security within the context of the organisation that it is supposed to protect. In such cases, the policy statements developed may not be directly applicable to the risks they are designed to nullify, and thus they will not combat the security threats that the specific organisation is facing. McKenna (2010) states that "Unfortunately, many IT security people do not understand business risks, so they end up writing these huge security policies that are all about protecting everything".

The process of developing and implementing an effective information security policy is not straight forward, but is driven by multiple issues such as regulatory requirements, the complexities of new technologies, and external and internal threats. The existing literature highlights certain information security policy development and implementation methods (Anand, 2012; Bayuk, 2009), but these methods do not include a comprehensive, integrated method that details step-by-step processes. Accordingly, this paper aims to find a solution to the problem of the Information Security Policy Development Life Cycle (ISPDLC) in order to address the challenges that have been highlighted in this section. The next section discusses the research methodology that was used to achieve the objective of this paper.

3. Research methodology

This study used a mixed method approach, combining both qualitative and quantitative methods during the data collection and data analysis processes. Firstly, the study adopted a qualitative approach during the formal content analysis of existing theories on and methods for developing an information security policy. The interpretation of the results of the content analysis subsequently resulted in the development of a conceptual framework. Secondly, quantitative data was collected using a survey in order to validate the constructs contained in the ISPDLC (component 1 of Fig. 2) with the objective of generalising the findings.

3.1. *Secondary data collection: the content analysis*

A content analysis of security policy development was conducted using secondary sources in the literature in order to obtain a thorough understanding of the processes necessary to formulate and implement the policy.

A total of 21 documents were chosen for the sample in this study as shown in Appendix A. These documents constitute cited and prevalent published items on the topic on Google Scholar; it comprised journal articles, conference proceedings and industry publications. These 21 sampled documents were subsequently imported into the MAXQDA software package. MAXQDA is a software program that has been designed for computer-assisted qualitative and mixed methods data, text and multimedia analysis (MAXQDA, 2012). Each document was individually coded by highlighting the sentence or the paragraph that mentions the process of developing a security policy. On completion of the coding process, a total of 42 codes and 568 accumulative codes had emerged. These codes varied from the general to the specific. General codes included for example "security policy construction", while the specific ones included "draft the policy", "write policy" and "write policy procedure". The 42 codes that had emerged during the coding process were reduced to ten codes (see Fig. 1), with some of the smaller codes merged with similar allied codes. For example, the codes labelled "identification of vulnerabilities", "identification of threats" and "identification of assets to be protected" were grouped under one code termed "risk assessment" as they were all part of evaluating the security risk processes. Based on the results of the content analysis, a conceptual framework was proposed. The proposed framework was then refined on the basis of suggestions made by the professionals who were surveyed.

3.2. *Primary data collection: the survey*

The primary data collection in this paper included a survey, which was conducted in order to validate the constructs of the ISPDLC component of the framework. A research instrument was developed and distributed to 400 security professionals – 200 in the United Kingdom and 200 in the United States of America. A total of 310 security professionals (182 from the UK and 128 from the USA) responded to the survey questionnaire, which was administered using SurveyMonkey software. The information security professionals targeted by the survey

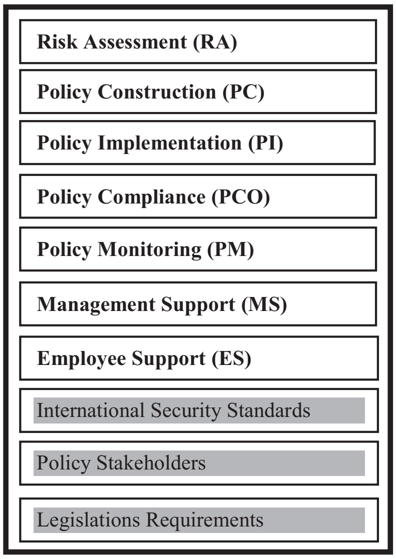

Fig. 1 – Framework codes.

included IT managers, chief information security officers and security specialists. The participants were chosen because they are involved in information security related issues in their daily activities and therefore may be considered to exert significant influence on information security management in their organisations. The respondents were asked to specify the type of organisation for which they worked. It emerged that 41.92% worked in industry; 17.69% in government; 14.23% in the banking sector; 13.46% in the consulting sector; and 12.69% in the trading sector. In addition, the respondents were asked to indicate the number of employees working in their organisation. The findings revealed that 35.71% worked for organisations with fewer than 500 employees; 25.65% for organisations with between 500 and 1000 employees; 23.70% for organisations with between 1000 and 5000 employees; 6.17% for organisations with between 5000 and 10000 employees, and 8.77% for organisations with more than 10 000 employees. The findings also showed that 62% of the respondents were male, while 38% were female.

The survey questionnaire was based primarily on the results of the content analysis that had been conducted on the secondary data. Additionally, the questionnaire contained open-ended questions which gave the respondents the opportunity to respond in their own words. The respondents were asked to offer suggestions in respect of the processes for developing and implementing an information security policy which they felt was important, but which had not been included in the questionnaire. The questionnaire also included closed questions based on a Likert-type scale that restricted the respondents to selecting answers from a predefined set.

3.3. *Evaluation of the research*

This research used a mixed method approach which combined qualitative and quantitative data. According to Johnson and Onwuegbuzie (2004), mixed method research involves mixing or combining quantitative and qualitative research techniques, methods, approaches, concepts or language into one study. Oates (2006) explains that combining both research methods provides the researcher with multiple modes of "attack" on the research objective. In addition, the findings or conclusions of such a study are more likely to be convincing and accurate than would otherwise have been the case (Yin, 2003). The next section highlights the evaluation of the qualitative and quantitative data.

3.3.1. *Qualitative data*

Borrego et al. (2009) state that "just as rigorous statistical analysis is essential in quantitative research to ensure reliability and generalisability of the results, so too is the rich description of the context and experiences of the participants essential in qualitative research to ensure trustworthiness". In this paper, trustworthiness was ensured because the constructs were evaluated by security experts. The participants were chosen purposefully (purposeful sample) for their involvement in security-related matters in their daily activities, and were therefore viewed as information rich.

Furthermore, Lincoln and Guba (1985) propose four criteria for trustworthiness:

- Credibility – this refers to confidence in the "truth" of the findings. Critical and constructive feedback from the security experts that were surveyed enabled this research contribution to be refined.
- Transferability– this entails that the findings have applicability in other contexts. The proposed ISPDLC provides guidelines that organisations can follow in order to improve their mechanisms for developing an information security policy.
- Dependability – this shows that the findings are consistent. The data used in this paper were obtained from multiple sources and the findings were supported by literature, extant theories, and the empirical results.
- Confirmability – this refers to a degree of neutrality or the extent to which the findings of a study are shaped by the respondents and not by researcher bias, motivation, or interest. In this paper, the researchers were neutral as the data used included the findings of the content analysis and the input of the surveyed security professionals.

3.3.2. *Quantitative data*

Tavakol and Dennick (2011) maintain that reliability and validity are two fundamental concerns in the assessment of a measurement instrument. In this paper, Cronbach's alpha was used to measure the reliability of the constructs of the proposed ISPDLC. Raerd (2012) indicates that Cronbach's alpha is the most commonly used statistical test to determine the reliability of multiple Likert-type questions in a survey. In addition, construct validity was assessed by performing a Factor Analysis on the items (variables constituting a construct) of each construct and calculating the validity of the resulting factors.

3.3.2.1. *Reliability of constructs.* Table 1 provides the findings of the reliability statistics of all combined constructs.

As depicted in Table 1, the Cronbach's alpha was $\alpha = 0.943$ for all combined constructs. In addition, Cronbach's alpha was used to establish the internal consistency of the questions related to the variables of each construct. The Cronbach's alphas

Table 1 – Reliability statistics (Cronbach's alpha).

Item	Combined constructs	RA	PC	PI	PCO	PM	MS	ES
Cronbach's alpha	.943	.907	.916	.894	.909	.898	.904	.900
No items	7	4	4	4	4	4	4	4

achieved for these variables ranged from 0.916 (highest) to 0.894 (lowest). This, in turn, indicates that the variables asked in the questionnaire in relation to all the combined constructs were both reliable and consistent. A Cronbach's alpha value of 0.7 or greater is considered acceptable (Gefen et al., 2000; Nunnally and Bernstein, 1994).

3.3.2.2. Validity of constructs. A principle component Factor Analysis was conducted on all combined constructs. Table 2 shows the results of the Factor Analysis.

Furthermore, a principle component Factor Analysis was also done on the variables of each construct. As depicted in Table 3, the Factor Analysis findings for all the combined constructs and their variables ranged from 0.925 (highest) to 0.831 (lowest). Therefore, the Factor Analysis indicated that all scales proved to be highly valid, thus measuring what they are expected to measure. According to Hair et al. (1998), loadings of .5 or greater represent items of practical significance.

Table 2 – Combined constructs factor matrix (validity).

Item	RA	PC	PI	PCO	PM	MS	ES
Loading	.850	.886	.885	.875	.859	.884	.870

Table 3 – Items factor matrix.

Item	Loading
RA1	.897
RA2	.925
RA3	.892
RA4	.861
PC1	.893
PC2	.884
PC3	.901
PC4	.862
PI1	.831
PI2	.903
PI3	.893
PI4	.860
PCO1	.878
PCO2	.894
PCO3	.890
PCO4	.884
PM1	.872
PM2	.861
PM3	.892
PM4	.874
MS1	.879
MS2	.900
MS3	.890
MS4	.857
ES1	.877
ES2	.886
ES3	.882
ES4	.866

The next section discusses the results of the content analysis and the input of the surveyed security professionals.

4. Framework codes: the WHAT

The ten framework codes are based on the integration of the existing information security policy development and implementation methods and models found in the current literature, plus the input of the surveyed security professionals. The findings revealed different codes that organisations should consider when developing and implementing an effective information security policy. Fig. 1 depicts the final ten codes of the proposed framework.

By reflecting on the different codes depicted in Fig. 1, it became clear that seven codes – namely Risk Assessment, Policy Construction, Policy Implementation, Policy Compliance, Policy Monitoring, Management and Employee Support – encompass all the processes needed to develop and implement an information security policy. Therefore, these codes thus constituted the *Information Security Policy Development Life Cycle* (ISPDLC component in Fig. 2) and became the seven constructs.

The second component: *Security Policy Drivers* (see component 2 in Fig. 2) consisted of three codes. This component is composed of the threats that place the organisation under pressure so that mechanisms are implemented in order to protect information. Abdel-Aziz (2010) states that "before discussing information security policy and the process to assess it, it is important to know what drives information security in the first place". The development of an information security policy is driven by both external and internal influences that exert pressure on the organisation to put in place mechanisms to protect the organisation's information. The internal threats include insider employees who place the organisation's information at risk, while external threats include hackers. In addition, there is the necessity of complying with proliferating government legislative requirements.

The third component is the *Security Policy Guidance* (see Fig. 2). This component is composed of the security standards that guide organisations in constructing an information security policy. As discussed, international security standards such as ISO/IEC 27002 (2013) are used as a major guide at the beginning stage of information security policy development.

Finally, organisations need to use relevant *Existing Theories* (component 4 in Fig. 2) in order to understand the behavioural intention of employees concerning information security policy compliance. The content analysis revealed that General Deterrence Theory (GDT) and the Theory of Planned Behaviour (TPB), among others, are key theories for understanding employees' behavioural intention to comply with an information security policy of an organisation. The TPB explains that the intention of an individual to perform a given behaviour is influenced by attitude, subjective norms and perceived behavioural control (Ajzen, 1991). On the other hand, GDT predicts that an increase in the severity of the punishment imposed on those who violate the rules of the organisation reduces certain criminal acts (Blumstein et al., 1978).

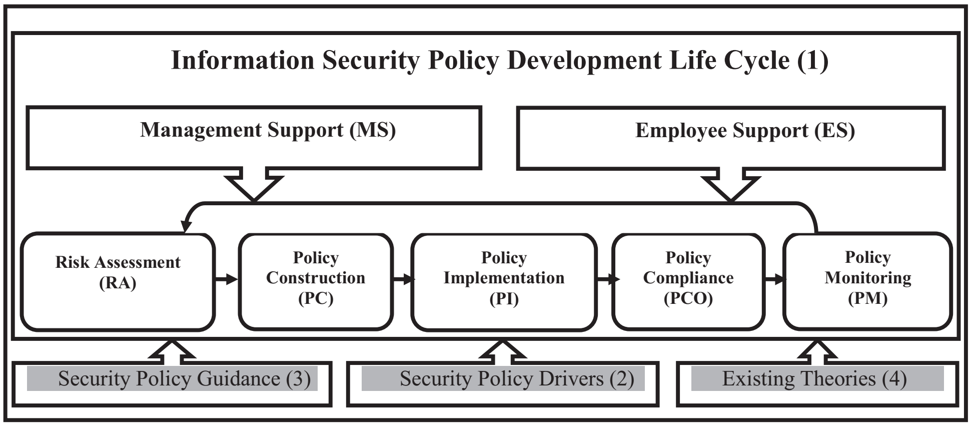

Fig. 2 – The policy development framework including the ISPDLC component.

As discussed in this section, the proposed framework, depicted in Fig. 2, comprises four components that constitute the main pillars of the information security policy development and implementation process. However, this paper focuses on component 1 and the seven constructs which constitute this component.

The seven constructs of the ISPDLC component, namely Risk Assessment (RA), Policy Construction (PC), Policy Implementation (PI), Policy Compliance (PCO), Policy Monitoring (PM), Management Support (MS) and Employee Support (ES), were evaluated based on the survey result. The software used to conduct the statistical analysis was SPSS v22.0. The next section discusses the descriptive data analysis findings relating to the constructs of the ISPDLC.

4.1. *ISPDLC evaluation*

Once the data had been entered in SPSS, various statistical tests were conducted. Descriptive statistical tests were used to generate frequencies, the median, the mean, and the standard deviation. Table 4 presents the descriptive statistics of the constructs of the ISPDLC with the mean values arranged from highest to lowest.

As shown in Table 4, the mean of all constructs was above 3 – the middle value in the five-point scale (Dewberry, 2004). Accordingly, the results of the descriptive statistics revealed that, in general, the respondents agreed that all constructs of the ISPDLC component were important. The overall results of the survey showed that Risk Assessment was the most important construct of the various measured constructs. This result is not surprising given that the main reason for developing an information security policy is to mitigate the various security risks that organisations face. The second most important construct was Management Support. Management plays a significant role in decision-making in an organisation, especially with regard to budgeting and information security policy approval and enforcement. The findings also revealed that the respondents believed that Policy Compliance and Employee Support were important steps for inclusion in an information security development and implementation process. The overall results showed that Policy Monitoring was the least important of the measured constructs. The formal content analysis revealed similar results, with Information Security Monitoring showing the lowest frequency of tags compared to the other constructs.

Table 4 – Descriptive statistical results of the ISPDLC component.

	N	Mean	Median	Std. deviation
Risk assessment (RA)	308	4.1623	3.0000	1.04909
Policy construction (PC)	308	4.0032	3.0000	1.01294
Policy implementation (PI)	307	4.0130	3.0000	1.00318
Policy compliance (PCO)	307	4.0749	3.0000	.93808
Policy monitoring (PM)	307	3.9644	3.0000	1.07602
Management support (MS)	309	4.0814	3.0000	.97177
Employee support (ES)	309	4.0615	3.0000	.98335

4.1.1. *Results of the Risk Assessment (RA) variables*

Table 5 presents the descriptive statistics pertaining to the Risk Assessment variables, with the mean values arranged from highest to lowest.

Table 5 reveals that the mean was above 3, which shows that the respondents deemed all four variables to be important. The identification of *vulnerabilities and threats* process had the highest mean of 4.1392. This indicates that the respondents believed this process to be very important compared to the other processes of the Risk Assessment construct.

4.1.2. *Results of the Policy Construction (PC) variables*

Table 6 shows the descriptive statistics pertaining to the Policy Construction variables.

Table 5 – Results of Risk Assessment variables.

	N	Mean	Median	Std. deviation
Vulnerabilities and threats	309	4.1392	3.0000	.98201
Assets identification	310	4.0774	3.0000	.96230
Legislation	308	4.0714	3.0000	.94547
Risk identification	308	4.0455	3.0000	.96412

Table 6 – Results of the Policy Construction variables.

	N	Mean	Median	Std. deviation
Write detailed security policy	306	3.9804	3.0000	.93015
Write high level security policy	309	3.9612	3.0000	.97623
Consultation with stakeholders	307	3.9609	3.0000	.90664
Write lower level security policy	307	3.8567	3.0000	1.03168

As highlighted in Table 6, the results revealed that the mean was above 3. The development of *detailed security policies* had the highest mean of 3.9804, indicating that the respondents believed that this process was very important as compared to the other processes of the Policy Construction construct.

4.1.3. *Results of the Policy Implementation (PI) variables*

Table 7 presents the descriptive statistics pertaining to the Policy Implementation variables, with the mean values arranged from highest to lowest.

Table 7 illustrates that the mean was above 3, which shows that respondents deemed all four variables to be important. *Defining the role of stakeholders* had the highest mean of 4.0550, indicating that the respondents believed that this process was very important as compared to the other processes of the Policy Implementation construct.

4.1.4. *Results of Policy Compliance (PCO) variables*

Table 8 presents the descriptive statistics pertaining to the Policy Compliance variables.

Table 8 shows that the mean was above 3 – the middle value in the five-point scale (Dewberry, 2004). *Knowledge* emerged as an important variable with the highest mean of 3.9934, thus indicating that the respondents believed this process to be very important as compared to the other processes of the Policy Compliance construct.

Table 9 – Results of Policy Monitoring variables.

	N	Mean	Median	Std. deviation
Periodical review	308	4.0162	3.0000	.97346
Audit information	310	4.0161	3.0000	.96024
Non periodical review	307	3.9935	3.0000	.95996
Automated review	306	3.9052	3.0000	.97552

4.1.5. *Results of the Policy Monitoring (PM) variables*

Table 9 presents the descriptive statistics pertaining to the Policy Monitoring and assessment variables, with the mean values arranged from highest to lowest.

Table 9 indicates that the mean was above 3. The *periodical review* had the highest mean of 4.0162, indicating that the respondents believed this process to be the most important process of the Policy Monitoring.

4.1.6. *Results of Management Support (MS) variables*

Table 10 presents the descriptive statistics of the Management Support variables with the mean values arranged from highest to lowest.

As highlighted in Table 10, the results revealed that the mean was above 3. *Management involvement* had the highest mean of 4.0455, indicating that the respondents believed this process to be the most important process of the Management Support construct.

4.1.7. *Results of Employee Support (ES) variables*

Table 11 presents the descriptive statistics of the Employee Support variables with the mean values arranged from highest to lowest.

Table 11 reveals that the mean was above 3, which shows that the respondents found all four variables to be important. *Employee involvement* had the highest mean of 4.0326, thus indicating that the respondents believed that this process was very important compared to the other processes of the Employee Support construct.

The next section discusses the relationship between the ISPDLC constructs.

Table 7 – Results of Policy Implementation variables.

	N	Mean	Median	Std. deviation
Role of stakeholders	309	4.0550	3.0000	.97379
Security policy education	309	4.0356	3.0000	.99121
Security policy training	309	3.9385	3.0000	.95658
Security policy awareness	310	3.7968	3.0000	.99870

Table 10 – Results of Management Support variables.

	N	Mean	Median	Std. deviation
Management involvement	308	4.0455	3.0000	.94017
Budget	307	4.0391	3.0000	.94891
Policy enforcement	308	4.0195	3.0000	1.00792
Policy approval	305	3.9508	3.0000	.96699

Table 8 – Results of the Policy Compliance variables.

	N	Mean	Median	Std. deviation
Knowledge	305	3.9934	3.0000	.90682
Attitude	308	3.9838	3.0000	.89683
Perceived benefit	307	3.9772	3.0000	.90900
Perceived social pressure	307	3.9739	3.0000	.95279

Table 11 – Results of the Employee Support variables.

	N	Mean	Median	Std. deviation
Employee involvement	307	4.0326	3.0000	.92474
Binding agreement	309	3.9968	3.0000	1.00162
Job termination	307	3.9870	3.0000	.99991
Deterrence measure	307	3.8436	3.0000	.99754

5. The relationship between the ISPDLC constructs: the HOW

The results of the content analysis revealed a high frequency of occurrence of Management Support and Employee Support. Accordingly, it was assumed that it is essential that Management Support and Employee Support are involved in all the processes when developing and implementing an information security policy. Therefore, inferential statistical tests were conducted to ascertain whether there is a relationship between Management Support and the Information Security Policy Development Life Cycle (ISPDLC) constructs.

Similarly, inferential statistical tests were therefore used to ascertain whether there is a relationship between Employee Support and the ISPDLC constructs.

As illustrated in Table 12, Pearson's correlation coefficient was conducted to examine the strength and direction of correlations among the various constructs of the ISPDLC. The following abbreviations are used for these constructs: Management Support (MS), Risk Assessment (RA), Policy Construction (PC), Policy Implementation (PI), Policy Monitoring (PM), Policy Compliance (PCO), and Employee Support (ES).

As shown in Table 12, Pearson correlation indicates the strength of association between the constructs of the ISPDLC component. The findings show a positive correlation between the constructs of the ISPDLC, namely $p < 0.05$, which is statistically significant. Therefore, the results show that the different constructs of the ISPDLC are reliable and consistent.

5.1. *Management Support (MS) and Risk Assessment (RA) correlation analysis*

A positive correlation was found between Management Support and Risk Assessment [$r = 0.804$, $n = 307$, $p = 0.000$]. With $p < 0.05$, this correlation is statistically significant, with high scores for Management Support being associated with high scores for Risk Assessment.

Risk Assessment is the first step that an organisation needs to embark on in order to identify the threats, vulnerabilities and risks that need to be mitigated. At this stage, management involvement is the variable that is most needed. Subsequently, based on the results of the Risk Assessment stage, management should conduct a cost–benefit analysis on the implementation of the recommended controls to reduce the identified risks to an acceptable level. The Business Dictionary (2001) defines cost–benefit analysis as a "process of quantifying costs and benefits of a decision, program, or project (over a certain period), and those of its alternatives (within the same period), in order to have a single scale of comparison for an unbiased evaluation". Based on the result of the cost–benefit analysis, management will decide if it is worthwhile implementing the recommended control and, if the envisaged costs are within the budget, the Risk Assessment plan is approved and the next phase of Policy Construction can commence. If not, the risk mitigation strategies will either need to be revised to bring them within budget or the budget will have to be increased.

5.2. *Employee Support (ES) and Risk Assessment (RA) correlation analysis*

A positive correlation was found between Employee Support and Risk Assessment [$r = 0.756$, $n = 307$, $p = 0.000$]. With $p < 0.05$, this correlation is statistically significant, with high scores for Employee Support being associated with high scores for Risk Assessment.

The most important threats to organisations' information security are the employees who work in the organisation. Therefore, the involvement of employees in the Risk Assessment process is crucial. Douglas (2011) advises that during the Risk Assessment stage, organisations need to identify the assets to

Table 12 – Correlation analysis between the ISPDLC constructs.

		MS	RA	PC	PI	PM	PCO	ES
MS	Pearson correlation	1	.804	.765	.673	.669	.654	.680
	Sig. (2-tailed)		.000	.000	.000	.000	.000	.000
	N	309	307	307	306	306	306	308
RA	Pearson correlation	.804	1	.792	.673	.740	.707	.756
	Sig. (2-tailed)	.000		.000	.000	.000	.000	.000
	N	307	308	307	305	306	305	307
PC	Pearson correlation	.765	.792	1	.737	.733	.691	.731
	Sig. (2-tailed)	.000	.000		.000	.000	.000	.000
	N	307	307	308	305	306	305	307
PI	Pearson correlation	.673	.673	.737	1	.797	.682	.717
	Sig. (2-tailed)	.000	.000	.000		.000	.000	.000
	N	306	305	305	307	305	304	306
PM	Pearson correlation	.669	.740	.733	.797	1	.781	.741
	Sig. (2-tailed)	.000	.000	.000	.000		.000	.000
	N	306	306	306	305	307	304	306
PCO	Pearson correlation	.654	.707	.691	.682	.781	1	.774
	Sig. (2-tailed)	.000	.000	.000	.000	.000		.000
	N	306	305	305	304	304	307	306
ES	Pearson correlation	.680	.756	.731	.717	.741	.774	1
	Sig. (2-tailed)	.000	.000	.000	.000	.000	.000	
	N	308	307	307	306	306	306	309

be protected and to assess the threats and vulnerabilities. It is important to involve employees in asset identification, as assets include the computers employees use. Therefore, employees have to cooperate with the staff members who will be involved in carrying out the identification activities. The same cooperation is necessary during the threat and vulnerability identification process.

5.3. *Management Support (MS) and Policy Construction (PC) correlation analysis*

A positive correlation was found between Management Support and Policy Construction [r = 0.765, n = 307, p = 0.000]. With $p < 0.05$, this correlation is statistically significant, with high scores for Management Support being associated with a high score for Policy Construction.

Bayuk (2009) points out that the construction of an information security policy should start with top management. Accordingly, directives or high-level security policies emanating from the executive management are disseminated from the strategic level to the tactical level where they are translated into standards or guidelines; finally, they are disseminated to the operational level in the form of procedures (Von Solms et al., 2011). During the information security policy construction stage, management involvement is essential because it is needed to approve the security policy. If management approves the security policy, the next stage is the publication of the policy. On the other hand, if management refuses to approve the policy, the security policy team will need to incorporate management's recommendations and resubmit the policy to management for approval.

5.4. *Employee Support (ES) and Policy Construction (PC) correlation analysis*

The results show a positive correlation between Employee Support and Policy Construction [r = 0.731, n = 307, p = 0.000]. With $p < 0.05$, this correlation is statistically significant, with high scores for Employee Support being associated with high scores for Policy Construction.

Kadam (2007) advises that, when constructing an information security policy, employees need to be involved in order to create a sense of ownership. In addition, it is critical at this stage to start preparing employees for the upcoming changes and the new ways in which they will be operating when the new policy requirements are implemented. Involvement is thus critical in moving users through the stages of commitment – from preparation through acceptance and ultimately to the commitment stage.

5.5. *Management Support (MS) and Policy Implementation (PI) correlation analysis*

A moderate positive correlation was found between Management Support and Policy Implementation [r = 0.673, n = 306, p = 0.000]. With $p < 0.05$, this correlation is statistically significant with high scores for Management Support being associated with a high score for Policy Implementation.

During the Policy Implementation stage, the policy is rolled out to the entire organisation. The content analysis revealed that this stage comprises four variables: Policy Awareness, Policy Training, Stakeholders' Role, and Policy Education. At this stage, the involvement of Management Support is crucial as communication from top management has to be disseminated throughout the different organisational levels. The committed participation of management will motivate employees to comply with the new policy requirements and will also help to increase employees' acceptance and commitment to the organisation's security policy. Management also plays an important role in Policy Awareness as it is their place to ensure that all stakeholders are aware of and understand their responsibilities as they relate to the security policy requirements. In order to reach the various audiences, different forms of business communication (notices, intranet, posters, newsletters, etc.) can be used to promote Policy Awareness. Furthermore, management needs to ensure that there are mechanisms in place for training and educating users on the new information security policy requirements. Such training can be organised regularly or intermittently, depending on the need for such training and education sessions.

5.6. *Employee Support (ES) and Policy Implementation (PI) correlation analysis*

A positive correlation was found between Employee Support and Policy Implementation [r = 0.717, n = 306, p = 0.000]. With $p < 0.05$, this correlation is statistically significant, with high scores for Employee Support being associated with high scores for Policy Implementation.

When implementing a new information security policy, it is crucial to involve the employees. The Mauritian Computer Emergency Team (2011) emphasises that employees should be required to sign the policy formally. This will mean that the new information security policy document is a binding contractual agreement between the employers and the employees. As such, the contract contains the rules that employees must follow to protect the organisation's information assets. It also includes the penalties that will be imposed on employees should they violate the policy.

In addition, employees will be required to attend training and education programmes so that they understand the requirements of the policy. The main objective of such programmes is to increase knowledge about the policy requirements.

5.7. *Management Support (MS) and Policy Compliance (PCO) correlation analysis*

A moderate positive correlation was found between Management Support and Policy Compliance [r = 0.654, n = 306, p = 0.000]. With $p < 0.05$, this correlation is statistically significant, with moderate scores for Management Support being associated with moderate scores for Policy Compliance.

Once the information security policy has been implemented in the organisation and the employees have been trained and are aware of the policy, management needs to put appropriate measures for information security policy compliance in place. These measures are designed to ascertain whether the requirements of the information security policy have been met. In order to understand the employees' compliance behaviour, Bulgurcu et al. (2010) recommend using existing theories related to information security policy compliance, such as the TPB and the GDT.

5.8. *Employee Support (ES) and Policy Compliance (PCO) correlation analysis*

A positive correlation was found between Employee Support and Policy Compliance [r = 0.774, n = 306, p = 0.000]. With $p < 0.05$, this correlation is statistically significant, with high scores for Employee Support being associated with high scores for Policy Compliance.

Bulgurcu et al. (2010) argue that organisations need to rely on existing theories related to information security policy compliance in order to understand employees' intentions to comply with such policy. Employees should not consider a security policy as a form of punishment, rather they should see them as measures that will help to protect the organisation's assets and thus grow the organisation's business.

5.9. *Management Support (MS) and Policy Monitoring (PM) correlation analysis*

A moderate positive correlation was found between Management Support and Policy Monitoring [r = 0.669, n = 306, p = 0.000]. With $p < 0.05$, this correlation is statistically significant, with moderate scores for Management Support being associated with moderate scores for Policy Monitoring construct.

Management plays a significant role in the information security policy monitoring and assessment stage. Management, who are responsible for the well-being of the organisation, needs to be aware of the *status quo* of the organisation's information security. In the Direct–Control cycle presented by Von Solms et al. (2011), the emphasis falls on the importance of the controlling step. Von Solms et al. (2011) state, "In order to effectively control, it is necessary to capture data to test for compliance with the policies which were drafted and implemented through directing. At the Operational level, this data could be extracted from, for example, log files of operating systems, databases and firewalls". The information gained from these files must be compiled in a report and submitted to management. Thereafter, management should assess the report and make decisions accordingly.

5.10. *Employee Support (ES) and Policy Monitoring (PM) correlation analysis*

A positive correlation was found between Employee Support and Policy Monitoring [r = 0.741, n = 306, p = 0.000]. With $p < 0.05$, this correlation is statistically significant, with high scores for Employee Support being associated with high scores for Policy Monitoring and Assessment.

As highlighted by Talbot and Woodward (2009), one of the objectives of information security policy monitoring and assessment is to produce measurable results that show users' behaviour. These results should then be used to assess the employees' performance in terms of security policy compliance. During an audit of security policy compliance, employees that demonstrate high security policy compliance should be encouraged and rewarded. On the other hand, those who are found to be violating the organisation's information security policy should be cautioned and penalised.

The next section discusses the information security policy stakeholders.

6. Information security policy stakeholders: the WHO

In order for an information security policy to survive and attain its objectives, management, employees and stakeholders need to support the entire process involved in developing and implementing it. The development of an effective security policy requires a combination of skills which emanate from the experiences of the different stakeholders (Diver, 2007). Respondents in the survey suggested various stakeholders that should be involved in the process of developing and implementing the policy. This section therefore discusses the various stakeholders that are critical in this process. The content analysis and the input received from the surveyed security professionals revealed six stakeholders that should be involved in the development and implementation of the policy. These are depicted in Fig. 3.

The following section discusses each of the stakeholders showed in Fig. 3.

6.1. *Executive management*

Bayuk (2009) argues that the first step in formulating a security policy involves ascertaining the way in which top management understands security in the organisation. In view of the fact that management plays a significant role in organisational decision-making, the involvement of executive management in information security policy development is key to its success (Maynard et al., 2011). Kadam (2007) highlights the fact that it is essential that management are aware of the importance of information security policy development activities so that the necessary resources are allocated to them.

6.2. *End-users*

Employee Support refers to the support of the end-users who perform various activities in an organisation. Szuba (1998) posits

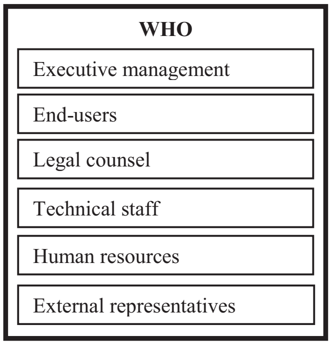

Fig. 3 – Information security policy stakeholders.

that involving employees in the development of an information security policy results in their “buy-in” and support, while also creating a sense of ownership of the information security policy.

Maynard et al. (2011) further recommend that the end-user community be included as part of the development effort to ensure that the multidisciplinary nature of an organisation is incorporated in the information security policy development process. This involvement by end-users should take place at an early stage so that they are given an opportunity to identify errors and difficulties, which may then be remedied before the security policy is implemented. “If the policy documents are hard to understand, users may not read them fully or may fail to understand them correctly, thereby needlessly risking security compromise” (Diver, 2007).

6.3. *Legal counsel*

During the survey, one respondent stated: “It is important that the legal team is involved in the information security policy development to ensure that organisations’ policies are in line with government laws.” The legal department is important because it provides information on current laws as well as anticipated legislative requirements.

6.4. *Technical staff*

Technical staff members possess the technical knowledge that the security policy development team may lack. One of the survey respondents stated that security specialists must be involved in security policy development because of their expertise, which might be lacking in the team tasked with policy development.

Diver (2007) maintains that security specialists should guide the development and revision of each policy document and serve as policy development consultants. However, although security specialists are familiar with security matters, they may not possess comprehensive knowledge and understanding of computer systems and communication network systems, which is the role of the ICT specialists. Maynard et al. (2011) claim that ICT specialists are usually one of the driving forces in information security policy development, as they provide technological knowledge and can advise on the level of security that is needed in a specific organisation.

6.5. *Human resources*

In order to ensure that the security policy is in line with standard organisational practices, it is critical that the human resource department be involved in the security policy development life cycle (Maynard et al., 2011). In this way, consistency between the organisation’s security policy and standard organisational practices will be assured. Diver (2007) supports this notion of consistency by stating that “where the policy touches on topics covered by existing HR policy, e.g., email usage, physical security, you must make sure that both sets of policy say the same thing”. In other words, the security policy should not conflict with human resources policy.

6.6. *External representatives*

Maynard et al. (2011) motivate the need to include external representatives, such as customers, suppliers and other external entities, in the development of an information security policy. This is particularly important if the external entities depend on the organisation’s computer systems for their activities. As discussed in this section, the development of an effective security policy requires a combination of the various skills that result from the experiences of different stakeholders. Therefore, the inclusion of multiple stakeholders in the development of an effective security policy is crucial because it gives the organisation as a whole a sense of ownership of the security policy which facilitates the acceptance and adoption of the policy.

7. Conclusion

The main objective of the research on which this paper is based was to provide a framework (including the SPDLC) that would ensure a comprehensive structured methodology for developing and implementing an effective information security policy.

A formal content analysis of current information security policy development methods was conducted using secondary sources to obtain a deep understanding of the processes. The content analysis revealed various codes that are considered to be the main pillars of this Life Cycle (Fig. 1). Based on these codes, a conceptual framework (Fig. 2) was developed and subsequently refined on the basis of the suggestions made by the security professionals who participated in the survey.

The focus of this paper was on the Information Security Policy Development Life Cycle component of the framework, and thus the seven constructs of the ISPDLC were empirically tested. The findings of the descriptive data analysis showed that, while the respondents believed that all the constructs were important, Risk Assessment was the most important overall. Hence, when developing an information security policy, the first step to undertake is Risk Assessment in order to identify the threats and vulnerabilities that must be mitigated.

The second most important construct was Management Support. Executive managers use policies to make their management intentions and direction known. On the other hand, the overall results of the survey showed that Policy Monitoring was the least important construct, which implies that this area needs more attention. The content analysis highlighted similar results, with information security monitoring showing the lowest frequency of tags compared to the other categories.

The findings of the inferential statistical data analysis showed a positive correlation between Management Support and the ISPDLC, with a statistically significant result. It emerged that as Management Support increased/decreased, a concomitant increase/decrease could be expected in the ISPDLC constructs. For example, a high degree of involvement on the part of management, for example allocating sufficient resources for the risk assessment process, would result in an increased likelihood of success in the information security policy construction process.

The findings also revealed the existence of a significant relationship between Employee Support and the ISPDLC constructs. In other words, as Employee Support increased/

decreased, an increase/decrease could be expected in the ISPDLC constructs of the framework. For example, a high degree of employee support, such as participation in information security policy training, education and awareness sessions, would result in an increased likelihood of success in the information security policy implementation process.

8. Discussion and limitations

The first limitation of this paper is related to the demographics of the respondents in the survey. The respondents of the survey were from the United States of America and the United Kingdom only, which may constitute a limitation with regard to the generalisability of the study findings, as these two countries are developed countries with advanced technology. It is therefore important that the proposed framework should provide guidelines that underdeveloped countries could follow in order to improve their mechanisms for developing an information security policy. Future research could involve an empirical study that compares the development of information security policies in developing and developed countries. In most developed countries, senior management or a board of directors are by law responsible for information security and risk management. Thus, many have no option but to spend resources on putting mechanisms in place to protect the organisation's information. In practice, however, this does not always happen, particularly in smaller organisations.

The second limitation is the time and cost that would be involved in implementing all the processes suggested in the proposed framework. The development of an information security policy requires that organisations have sufficient budgetary resources to cover all the costs. These costs include, for example, the costs of conducting a risk assessment, constructing the information security policy, consulting with stakeholders, conducting training and education sessions, and monitoring users' activities by, perhaps, using an automated monitoring system. Moreover, costs will increase with the size of the organisation, with larger organisations requiring considerable time and money compared to smaller organisations. Finally, the decision to embark on drawing up an information security policy should be based on the organisation's risk appetite. In this regard, a cost–benefit analysis should be conducted in order to ascertain whether it is worth spending an excessive amount of resources on this exercise.

Appendix A

No	Author	Paper contribution
1	Talbot and Woodward (2009)	This research paper examined the implementation of security policies in an organisation. The paper makes recommendations on the processes involved in improving an organisation's culture; creating an awareness mechanism for policies; reviewing the policy periodically; updating the policy; policy compliance and policy enforcement.
2	InstantSecurityPolicy.com (2013)	This paper discusses the integration of security policy creation processes with a business management model in terms of which the security risks may be easily quantified.
3	Abdel-Aziz (2010)	This paper addresses the information security policy review and assessment.
4	Hong et al. (2006)	The finding of this paper highlights that organisations should focus on procedures and implementation items, rather than on the policy documents only. The contribution of this paper is relevant to the objectives of this study.
5	Von Solms et al. (2011)	This paper stresses the importance of information security policy as the main control with which to mitigate information security threats. In addition, the paper highlights how the information security policy should be implemented based on the strategic, tactical and operational management levels.
6	Kadam (2007)	This paper points out a wide range of issues which were considered important to the research objectives of this study, including the need to conduct a risk assessment, developing security policy and procedures' processes, and management support.
7	Bayuk (2009)	Bayuk emphasises the importance of information security management and policy control.
8	Avolio et al. (2007)	This paper discusses the processes involved in writing a security policy to protect the network security. It emphasises that security policies should be initiated by top managers. Furthermore, it highlights that, before writing a security policy, it is essential that organisations take into account the regulations that apply to that specific organisation.
9	Chen and Li (2014)	The paper emphasises that deterrence measures will effectively decrease omission behavioural intention.
10	Wahsheh and Alves-Foss (2008)	The paper presents a model which describes the engineering processes of developing security policies.
11	Bulgurcu et al. (2010)	Based on the theory of planned behaviour, this article investigates the reasons that drive an employee to comply with requirements of the information security policy. It also investigates the impact of information security awareness on an employee's outcome beliefs.
12	RSA Security Inc. (2013)	This paper discusses important issues related to security policy implementation such as policy communication and policy enforcement.
13	Karyda et al. (2005)	This paper explores the processes involved in formulating, implementing and adopting a security policy in an organisation. The paper looks specifically at the contextual factors that affect the successful adoption of information security policies.

(continued on next page)

No	Author	Paper contribution
14	National Computer Board (2011)	This report is important because it points out that there are different policy audiences in every organisation, and therefore it is imperative that the development of security policies take this issue into account. The report also refers to the responsibilities of the various stakeholders in security policy development.
15	University of Newcastle (2009)	The document cites the processes which are required during the policy review, drafting the policy and policy consultation. It also highlights the roles of stakeholders in approving the security policy.
16	Diver (2007)	This paper offers a unique perspective that the other papers in the sample did not offer. It emphasises the need to consider regulatory requirements before developing security policies. The paper also recommends taking into account the current security policy maturity before choosing which approach to follow in developing security policy.
17	Al-Awadi and Renaud (2007)	The paper highlights the important issues to be considered during the implementation of an information security policy. These issues include awareness and training, management support, budget and information security policy enforcement and adaptation.
18	Griffins (2009)	The paper discusses the various steps involved in writing policies and in the approval process. It also discusses the processes involved in distributing new security policies.
19	Corpuz and Barnes (2010)	The objective of this paper was to integrate information security policy management with corporate risk management. The paper also mentions the various risk assessment processes.
20	Yayla (2011)	This paper discusses different socio-behavioural control mechanisms that are useful in mitigating insider threats to information security. These include, for example, deterrence measures that may be used to ensure that employees do not violate the organisation's rules.
21	Khan (2010)	This paper emphasises the importance of the information security policy communication and publication within an organisation. It also points out the need for detailed process documentation of an information security programme.

Appendix B

Survey to assess the importance of information security policy development and implementation processes

1. Organisation type (Government, Industrial, Banking, Education, Others: please specify)

2. Occupation

A- CIO,

B- Security specialist,

C- IT manager,

D- Others (specify)

3. How many employees work in your organisation? Less than 500; between 500 and 1000; between 1000 and 5000; 5000 – 10 000; > 10 000

4. Does your organisation have an information security policy? (Yes or No):

5. Please specify your gender (Male or Female):

How **important** do you believe the following issues are for the successful implementation of an information security policy in your organisation?

Where **1) is Not important, 2) Somewhat important, 3) Neutral, 4) Important and 5) is Very important.**

	1	2	3	4	5
6. Visible support and commitment from top executive management.					
7. A clear understanding of the organisation's security risks.					
8. The information security policy writing process is based on the findings and the recommendations of the risk assessment process.					
9. Suitable information security policy training and education during the information security policy implementation stage.					
10. Regularly assess and monitor the information security policy to ensure that it is effective.					
11. Effective information security policy compliance mechanisms to ensure that employees adhere to the organisation's information security policy requirements.					
12. Ensure that employees support and understand their roles and responsibilities concerning the information security policy requirements.					

Assessment of the information security policy development process

In order to have an effective information security policy, an organisation should select a set of processes to be implemented. Please indicate the importance of each of the following security policy development processes where

1) is Not important, 2) Somewhat important, 3) Neutral, 4) Important and 5) is Very important.

Risk Assessment (RA) processes

	1	2	3	4	5
RA.1. Develop a risk assessment plan that includes the identification of assets to be protected.					
RA.2. Develop a risk assessment plan that includes the assessment of vulnerabilities and security threats.					
RA.3. The security policy is constructed based on the findings of the risk assessment result.					
RA.4. Identify all legal and regulatory requirements pertaining to the organisation.					

(*continued on next page*)

	1	2	3	4	5
Please add any activity that you feel is important with respect to the risk assessment process within your organisation:					
Policy Construction (PC) processes					
	1	2	3	4	5
PC.1. At the strategic level, develop high level policies which are a set of management mandates that show how executive management plan to protect the organisation's information assets.					
PC.2. At the tactical level, develop detailed security policies which are detailed statements showing what should be done to comply with the security policy.					
PC.3. At the operational level, develop lower level security policies which define the procedures, plans or processes that address the details of how to perform a specific action.					
PC.4. Organisations' stakeholders must be consulted before the information security policy is submitted to senior management for final approval.					
Please add any activity that you feel is important with respect to the security policy construction process within your organisation:					
Policy Implementation (PI) processes					
	1	2	3	4	5
PI.1. Different business communication (notices, posters, newsletters, etc.) are used to promote security policy awareness.					
PI.2. There are mechanisms to train all stakeholders so that they understand their responsibilities towards the security policy requirements.					
PI.3. Clearly define the roles of various organisational stakeholders (executive management, information security officials, everyone).					
PI.4. There are mechanisms in place to educate employees about the new information security policy requirements.					
Please add any activity that you feel is important with respect to the security policy implementation process within your organisation:					
Policy Monitoring (PM) processes					
	1	2	3	4	5
PM.1. Review the information security policy on a regular basis to make sure that it incorporates the latest threats and new regulations and is kept up to date.					
PM.2. Use of an automated review scheduling system which alerts when major changes have occurred to existing practices.					
PM.3. Review the audit information to identify the area(s) of frequent security policy deviation.					
PM.4. An established information security policy review and update process exists.					
Please add any activity that you feel is important with respect to the security policy assessment and monitoring process within your organisation:					
Management Support (MS) processes					
	1	2	3	4	5
MS.1. The involvement of executive management in the information security policy development is crucial to the approval of the security policies.					
MS.2. Top management plays a significant role in enforcing the information security policy so as to ensure that employees regard the policy requirements in a serious light.					
MS.3. Executive management is involved in the whole process of information security policy development.					
MS.4. Executive management must have sufficient budget for information security policy development.					
Please add any activity that you feel is important with respect to the management support process within your organisation:					
Employee Support (ES) processes					
	1	2	3	4	5
ES.1. There should be mechanisms in place to punish employees who intentionally violate the information security policy.					
ES.2. Employees should sign off that they have received and reviewed the policies and agree to be bound by them.					
ES.3. Job termination should be considered for employees who repeatedly violate the information security policy.					
ES.4. Employees that have been trained and are aware of information security policy requirements are likely to comply with such information security policy.					
Please add any activity that you feel is important with respect to the employee support process within your organisation:					
Policy Compliance (PCO) processes					
	1	2	3	4	5
PCO.1. An employee's positive attitude towards compliance with the organisation's information security policy positively influences their intention to comply with the requirements of the policy.					

(*continued on next page*)

	1	2	3	4	5
PCO.2. An employee's perceived social pressure about their compliance with the requirements of the information security policy positively influences their intention to comply with the requirements of the policy.					
PCO.3. An employee's perceived benefit of compliance with the organisation's information security policy will positively influence their attitude towards complying with the requirements of the policy.					
PCO.4. An employee's judgment of his/her own knowledge in complying with the requirements of the information security policy positively influences his/her intention to comply with the requirements of the policy					
Please add any activity that you feel is important with respect to the information security policy compliance process within your organisation:					

REFERENCES

Abdel-Aziz A. How to review and assess information security policy: the six-step process. <http://www.sans.edu/>; 2010 [accessed 15.05.13].

Ajzen I. The theory of planned behaviour. Special Issue: theories of cognitive self-regulation. Organ Behav Hum Decis Process 1991;50:179–211.

Al-Awadi M, Renaud K. Success factors in information security implementation in organisations. Proc IADIS Int Conf e-Society 2007;6:169–76.

Anand V. Security policy management process within a six sigma framework. J Inf Secur 2012;3:49–58.

Avolio F, Fallin S, Pinzon DS. Producing your network security policy. WatchGuard Technologies; 2007.

Bayuk J. How to write an information security policy. Computerworld 2009. <http://www.computerworld.com/article/2525539/security0/how-to-write-an-information-security-policy.html>.

Blumstein A, Cohen J, Nagin D. Deterrence and incapacitation: estimating the effects of criminal sanctions on crime rates. Washington: National Academy of Sciences; 1978.

Borrego M, Douglas E, Amelik C. Quantitative, qualitative, and mixed research methods in engineering education. J Eng Educ 2009;98(1):112–22.

Bulgurcu B, Cavusoglu H, Benbasat I. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS Q 2010;34(3):523–48.

Business Dictionary. Definition of binding agreement. 2001. <http://www.businessdictionary.com/definition/causal.html>.

CERT Insider Threat Center. U.S. State of Cybercrime Survey. 2014. <http://resources.sei.cmu.edu/asset_files/Presentation/2014_017_001_298322.pdf>; 2014 [accessed 16.06.14].

Chen H, Li W. Understanding organisation employee's information security omission behaviour: an integrated model of social norm and deterrence. 2014. Proceedings of PACIS, Chengdu, China.

Corpuz M, Barnes P. Integrating information security policy management with corporate risk management for strategic alignment. In: Proceedings of the 14th World Multi-Conference on Systemic, Cybernetics and Informatics (WMSCI). Orlando, Florida: 2010.

Dewberry C. Statistical methods for organizational research: theory and practice. Oxford: Routledge Psychology Press Business and Economics; 2004.

Diver S. Information security policy: a development guide for large and small companies. <http://www.sans.org>; 2007 [accessed 12.06.13].

Doughty K, Grieco F. IT governance: pass or fail? Inf Syst Audit Control Assoc 2005;6(12):124–32.

Douglas J. Risk appetite and tolerance. <http://www.theirm.org/media/464806/IRMRiskAppetiteExecSummaryweb.pdf>; 2011.

Gefen D, Straub D, Boudreau M. Structural equation modelling and regression: guidelines for research practice. Commun AIS 2000;4:61–77.

Griffins M. How to write a policy manual. <http://www.templatezone.com/download-free-ebook/office-policy-manual-reference-guide.pdf>; 2009 [accessed 14.05.14].

Hair J, Anderson R, Tatham R, Black W. Multivariate data analysis. 5th ed. Patparganj, Delhi, India: Pearson Education, Inc; 1998.

Hong K, Chi Y, Chao L. An empirical study of information security policy on information security elevation in Taiwan. Inf Manag Comput Secur 2006;14(2):104–15.

InstantSecurityPolicy.com. The IT Security Guide: why need one, what it covers, and how to implement it. <http://www.instantsecuritypolicy.com/Introduction_To_Security_policies.pdf>; [accessed 14.06.14].

ISO/IEC 27002. Code of practice for information security management. <http://www.bsi-global.org>; 2013 [accessed 15.06.14].

Johnson R, Onwuegbuzie A. Mixed methods research: a research paradigm whose time has come. Educ Res 2004;33(7):14–26.

Kadam A. Information security policy development and implementation. Inf Syst Secur 2007;16(5):246–56.

Karyda M, Kiountouzis E, Kokolakis S. Information systems security policies: a contextual perspective. Comput Secur 2005;24(3):246–60.

Khan R. Practical approaches to organisational information security management. <http://www.sans.org/reading-room/whitepapers/leadership/practical-approaches-organisational-information-security-management-33568>; 2010 [accessed 05.01.14].

Lincoln Y, Guba E. Naturalistic inquiry. Newbury Park, CA: Sage Publications; 1985.

Mauritian Computer Emergency Team. Guidelines on information security policy. Mauritius: National Computer Board; 2011 CMSGu2011-04.

Maynard S, Ruighaver A, Ahmad A. Stakeholders in security policy development. In: Proceedings of the 9th Australian Information Security Management Conference. Perth, Western Australia: 2011.

MAXQDA. Qualitative data analysis software for Mac and Windows. <http://www.maxqda.com/>; 2012 [accessed 18.12.13].

McKenna S. Keeping it real: updating your security policy. Inf Secur J 2010;7(2):18–21.

National Computer Board. Guideline on information security policy. <http://www.ncb.mu/English/Documents/Downloads/Reports%20and%20Guidelines/Guideline%20on%20Information%20Security%20Policy.pdf>; 2011 [accessed 08.06.13].

Nunnally J, Bernstein I. Psychometric theory. 3rd ed. New York: McGraw Hill; 1994.

Oates B. Researching information systems and computing. London: Sage Publications; 2006.

Raerd Y. Cronbach's Alpha (α) using SPSS. <https://statistics.laerd.com/spss-tutorials/cronbachs-alpha-using-spss-statistics.php>; 2012.

RSA Security Inc. A guide to security policy – a primer for developing an effective policy. <www.sans.org/security

-resources/policies/Policy_Primer.pdf>; 2009 [accessed 30.11.13].
Szuba T. Safeguarding your technology: practical guidelines for electronic education information security. <http://nces.ed.gov/pubs98/98297.pdf>; 1998 [accessed 19.01.13].
Talbot S, Woodward A. Improving an organisations existing information technology policy to increase security. In: Proceedings of the 7th Australian Information Security Management Conference. Perth, Western Australia: 2009.
Tavakol M, Dennick R. Making sense of Cronbach's alpha. Int J Med Educ 2011;2:53–5.
University of Newcastle. Policy Development and Review process –Guideline. <http://www.newcastle.edu.au/Resources/Divisions/Services/Corporate%20Governance/Policy/Policy-Development-Guideline.pdf>; 2009 [accessed 12.06.14].
Von Solms R, Thomson KL, Maninjwa M. Information security governance control through comprehensive policy architectures. Johannesburg, South Africa: In ISSA; 2011.
Wahsheh L, Alves-Foss J. Security policy development: towards a life-cycle and logic-based verification model. Am J Appl Sci 2008;5(9):1117–26.
Yayla A. Controlling insider threats with information security policies. In: Proceedings of 19th European Conference on Information Systems: ECIS, Helsinki, Finland, vol. 9, 12. 2011. p. 242–57.
Yin RK. Case study research: design and methods. 3rd ed. California: SAGE Publications; 2003.

Stephen V. Flowerday

Department of Information Systems, University of Fort Hare, East London, South Africa

Stephen holds a doctoral degree in Information Technology from the Nelson Mandela Metropolitan University. He is presently a professor focusing on Information Security at the University of Fort Hare. Stephen has supervised postgraduate students and published extensively within his research field.

Tite Tuyikeze

School of ICT, Sol Plaatje University, Kimberley, South Africa

Tite holds a DPhil in Information Systems from the University of Fort Hare. His primary research area focuses on the maturity assessment of information security policy. He has previously published research papers in this research area. Tite works as a senior lecturer at Sol Plaatje University.