A Generic Framework for Information Security Policy Development

Wan Basri Wan Ismail
Faculty of Communication, Visual Art and Computing
University of Selangor
Malaysia
wanbasri@unisel.edu.my

Setyawan Widyarto
Faculty of Communication, Visual Art and Computing
University of Selangor
Malaysia
swidyarto@unisel.edu.my

Raja Ahmad Tariqi Raja Ahmad
Faculty of Communication, Visual Art and Computing
University of Selangor
Malaysia
rmtariq@unisel.edu.my

Khatipah Abd Ghani
Faculty of Education and Social Science
University of Selangor
Malaysia
khatisj@unisel.edu.my

***Abstract*—Information security policies are not easy to create unless organizations explicitly recognize the various steps required in the development process of an information security policy, especially in institutions of higher education that use enormous amounts of IT. An improper development process or a copied security policy content from another organization might also fail to execute an effective job. The execution could be aimed at addressing an issue such as the non-compliance to applicable rules and regulations even if the replicated policy is properly developed, referenced, cited in laws or regulations and interpreted correctly. A generic framework was proposed to improve and establish the development process of security policies in institutions of higher education. The content analysis and cross-case analysis methods were used in this study in order to gain a thorough understanding of the information security policy development process in institutions of higher education.**

Keywords— security policy development, information security policy, information security.

I. INTRODUCTION

Information security and protection from insider threats are a major challenge in any organization today. Infrastructure technology such as the network perimeter is not a total solution against various threats. No matter how strong and sophisticated these technologies are configured, the flaws in information security always relates to the human factor as the weakest link of information security risks [1]–[11]. Currently, many security experts agree that the implementation and enforcement of security policy is one of the most practical ways to preserve and protect information systems [12] and also one of the keys to a successful security control program ([12]–[17]. However, in order to develop an effective policy, there are two elements in security policy that have a bearing on its effectiveness, which are the development process [9], [18], [19] and the contents of the security policy [20], [21].

Moreover, a good security policy should translate management expectations into clear, specific, and measureable objectives besides illustrating its effectiveness, readability and consistency [22]. Since the security policy should meet the organization's direction and objectives, security policy is not easy to develop. Duplicating a security policy from another organization might not be sufficient to address certain issues such as compliance with applicable rules and regulations. In certain circumstances, even the duplicated policy that is properly developed, referenced, cited with laws or regulations and interpreted correctly could be insufficient [23]–[25]. Hence, the security policy should be manifested based on the organization's culture, belief, operation, environment and policy requirement [26]–[29] such as in Institutions of Higher Education (IHE), where different management structures (e.g. faculties, departments) and types of behaviour are practiced [30]. Thus, the security policy formulation and development process must cater for different types of organizations, cultures, technology changes (hardware and software), users and management support [31]. According to [9], [19] most of the studies on security policy are focused on structure and content of the policy but less on developing the process, especially the step-by-step process. Thus, this paper focuses on security policy development in institutions of higher education. This paper is structured as follows: Section 2 discusses the importance of security policy development, Section 3 describes the research methodology, Section 4 covers the constructs of the proposed components and Section 5 discusses the results.

II. INFORMATION SECURITY POLICY DEVELOPMENT

A. Importance of the Security Policy Development Process

Information security policy expresses the organization's attitude towards internal and external information assets that need to be protected from unauthorized access, disclosure, destruction and modification [32]. The written policies are meant to control the dissemination and misuse of information. International organizations such as SANS and EDUCAUSE provide security policy templates, but these should only be considered as a preparatory platform for policy development [22], [24]. As stated by [8], the process of formulating a security policy is time-consuming, difficult, and also expensive. This statement is also supported by [22], "a good security policy is not a simple ''plug-and-play" component". Therefore, there are a few reasons why security policies are

978-1-5386-0549-3/17/$31.00 ©2017 IEEE

challenging to develop. First, the policies might differ significantly in the way the policy and procedures are set forth for certain types of organizations and management. Information security policy approaches are portrayed as meeting stipulations that oversee the data security implementation of an organization. The stipulations incorporate aspects of technological, legal, economic, political, and social concerns ([22]). Thus, a security policy must be grounded and solidly tied as well as, shaped according to the organization's needs and pertinent to appropriate regulations and laws [33]. Second, people are often referred to as the weakest link since the most threats or incidents occur because of ignorance or negligence by employees [16], [34]. According to [35], an information security policy should fulfil and cater for rules of expected behaviour by users, system administrators, management, security personnel and all stakeholders in the organization. This sets the boundaries for people behaviour and empowers people to do the right thing, which could be challenging because people need to identify the strategies of organizational law as it characterizes acceptable behaviour within the culture of an organization [20]. A well-structured organized policy framework is expected to empower top management to manage all the risks associated with security and to ensure that security controls based on risk mitigation strategies are implemented in order to meet business objectives [36]. Consequently, development of a security policy consist of numerous tasks of critical importance such as evaluating policy needs, risk assessment and business objectives intended to meet security requirements such as a combination of confidentiality, integrity and availability [9].

Third, the process of developing a security policy is occasionally confusing because it is misconstrued as a policy structure or misused as a term by professional policy administrators, legal counsels, and others [37]. This is referred in a study by [38], whereby there were many cases of employees having problems in complying with the security policy, either because of an absence of properly defined security policies or it is simply defined on an ad-hoc and unstructured basis. [39], also mentioned that a number of policies had failed not because they were intrinsically bad ideas, but due to poor design. Thus, the policy must be composed in a straightforward language, easy to understand and free from jargon. A security policy that is written using technical terms and not understood by the intended audience will result in disarray, confusion and misinterpretation.

B. The Current Security Policy Development Process

Nowadays, there are many ways to approach policy development and the formulation process. Table 1 shows the summarization of other authors' concepts and perception on security policy development methods and processes. There are nine conceptual models compared for each process and the comparison starts by identifying the steps involved in the security development process as shown in Table 1. For example, the author [35] emphasised on team development, risk assessment, policy construction, implementation and maintenance. In contrast, authors [40] laid prominence on risk assessment, organizational culture and technology, security control, construction, implementation and maintenance. Table 1 and Table 2 shows the comparison in terms of process especially on risk management, team developers, benchmarking and consultation. Risk assessment is the most important part, as suggested by the generic security development process (Table 1), meanwhile (Table 2) displays only three university's emphasis on risk assessment. These issues are similar to team development and benchmarking, which are the opposite of the generic and university's approach to the development process.

TABLE 1. Steps in the Security Development Process

Stage	Development Method	Author
Step 1	Team Development	[35][41]
Step 2	Risk Assessment	[42][40][43], [35][12], [41], [44], [45], [46]
Step 3	Identify Organization Culture and Technology	[40]
Step 4	Identify Security Control	[40], [43], [45][35]
Step 5	Policy Construction	[42][40][43], [35][12], [41], [44], [46]
Step 6	Policy Implementation	[42], [40][43], [35][12], [41], [44], [45], [46]
Step 7	Monitoring & Maintenance	[40][43], [35][12], [41], [44]

Meanwhile, Table 2 shows the compilation of the security development process from fifteen universities that have published their development process on their websites. Most of the universities surveyed were from Australia, United Kingdom and the United States. All the fifteen universities had emphasised on the main processes such as identifying and evaluating policy needs, drafting the document, obtaining approval, implementing, monitoring and reviewing the policy.

TABLE 2. Security policy Development Process in Universities

Stage	Main Process	Sub Process	# of Universities involved on the Related process.
Pre Development	Identify and evaluate need	Identification of Policy Requirements	15
		Risk Assessment	3
	Research and Consultation	Team Development	10
		Benchmarking Consultation	4
Development	Draft Document	Drafting Revision Quality Control	15
	Get Approval	Endorsement Promulgation	15
Implementation	Implementation	Awareness Training	15
	Monitoring & Review	Compliance Feedback	15

III. METHODOLOGY

This study adopted a qualitative approach and used the formal content analysis method for developing an information security policy and reviewing existing theories and methods. A

content analysis was used to identify the generic security policy development in general as applied in various organizations and security policy development process in institutions of higher education. This study also uses the Acceptable Use Policy as an example in order to identify the current security policy contents. There are thirty universities were studied for the content of acceptable use policy. The technique of identifying the content analysis in this study was greatly dependent on the coding process. The basic coding process in content analysis aims to organize large quantities of text into much fewer content categories. All these data were analysed using the HyperRESEARCH qualitative research tool. The study on the content of security policy is important in order to locate the elements that should be included in security policy documents. Once the contents were recognized, it is ease to identify to development process. Second is the case study, which was used to focus on the contemporary phenomena of how an institution of higher education formulates and develops its security policy [47].

A. Content Analysis

Since content analysis is useful for examining trends and patterns in documents [48] & [49], this paper focused on two phases of content analysis; first, to analyse a security policy development process for security policy in institutions of higher education and second, to compare it to the generic security policy development in general as applied in various organizations, which would be discussed in the next section. This process is important in order to identify the most common development process in security policies, especially in IHE. To fulfil this requirement, this study focused on fifteen universities that published their security policy development process on their websites and generic security development process models. Moreover, in this study, the development process was coded based on the Association of College and University Policy Administrators (ACUPA) that promotes a policy process with best practices for IHE. ACUPA is an informal network of professionals working on policy development and administrative areas in their institutions, It has grown to 135 participants and has a mission to explore both policy processes in college and university campuses as well as to discuss specific policy issues [44].

B. Case Study

Three institutions of higher education were selected for this study and were referred to as Case A, B and C. The criteria of selection were based on different populations and categories of higher education. Case B was referred to as a public university, Case A was a private university and Case C was a private university college. The details of the case study process are illustrated in Figure 1.

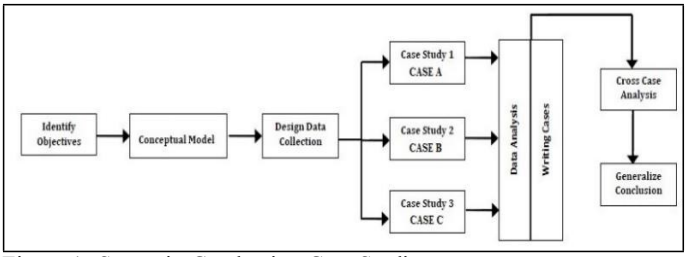

Figure 1: Stages in Conduction Case Studies

This study used the interview method as its research instrument so that it would provide a deeper understanding on certain themes or phenomenon. Based on the content analysis of security policy development process results, the interview questions were categorized into eight themes. The themes were Policy on Team Development, Risk Assessment, Create and Review Existing Policy, Policy Content and Structure, Write Initial Draft, Review by Stakeholders and Obtain Approval, Policy Implementation and Policy Maintenance. The respondent (interviewee) from the Case A institution was the IT officer who was in charge for ICT rules and regulations. For the Case B institution, the respondent was the Deputy Chief Information Officer and for the Case C institution, it was represented by its Head of the ICT Department. As part of the data analysis process, the cross-case analysis had focused on areas suggested by these three cases, which were areas in agreement, different areas and areas that conflicted. Thus, the result from the cross-case analysis was used to identify the crucial elements in the security policy development process.

IV. DISCUSSION

The results of the case studies were discussed based on qualitative responses by verbatim quotes from the interviews and cross-case analysis. The major finding in the case study analysis was that there was no specific process for security policy development as proposed by international standards or any generic security development process. Second, there was no comprehensive security policy implemented in the three targeted case study institutions such as system-specific or issue-specific security policies. Due to these issues, there are several reasons why security policies are not well developed and implemented in these targeted institutions. Management support is one of the major barriers or issues related to security policy development. Without top management support and authorization, IT departments cannot do anything in efforts to develop and implement information security in institutions of higher education.

The second barrier is lack of resources and time constraint. The evidence suggests that most colleges and universities devote insufficient resources to assess risks management, form a special team to develop policies, hire a technical writer, subject matter expert and sometimes impossible to involve all user groups to participate in policy team development especially when dealing with third parties. Financial limitations are a continuing challenge in institutions of higher education. With the ever-changing nature of technology, an effective security policy must be reviewed, revised, and updated on a regular basis. A policy that is not maintained will simply become worthless. Information security policies must be carefully formulated to reflect the mission of the organization. However, interviews with these institutions show that all three institutions wished to secure their information. They added that the most important thing in risk analysis process is to identify the actual security threats faced by their institutions. They also believe that information security could be achieved by increasing awareness and providing training.

A. Proposed Generic Information Security Development Process

Based on the combination of the literature and empirical study pertaining to the development process of a security policy, this study proposed a theoretical framework for the

formulation process of a security policy development process for institutions, shown in Figure 2. The ideas generated from this framework were used in combination with the content analysis on the structure of Acceptable Use Policy, quoted from the interviews, cross case analysis, practitioner's views and literature reviews. Based on the interviews, even the practitioners admitted that their institutions had not fully applied the common practices according to international standards; however, they agreed with this security policy development process framework. Moreover, the crucial results from the cross case-analysis shows that the Case B institution, which had thoroughly implemented best practices found in the corporate security policy according to international standard, had less complains on security breaches compared to others case institutions. Thus, based on all these analyses, the proposed framework is divided into three main areas of security policy development, namely the pre-development, development and implementation phases.

1) Pre-Development Phase

The formation of a policy team developer is crucial once new or revised policies and procedures are developed or reviewed. As proposed by [35] , proper policy team members should include the ICT Security team, Technical Writer, Technical Personnel, Legal Counsel, Human Resources and User Groups. Each member has his/her own responsibilities, especially during the policy content development process. The policy content should cover purpose, scope, security objective, security control, policy statement, legislation, etc. Thus, all these need to be brainstormed by this committee. The feedback from case study institutions also emphasises on a dedicated policy team developer. It is important to ensure that the one person in charge of policy development is not responsible for developing everything.

2) Development Phase

The second phase in the security development framework is the development process. This phase consists of four processes, namely risk assessment, preparation, policy writing and approval. Risk assessment is the major part of this process when it refers to systematically identifying, analysing and evaluating the information security risks associated with an information system or service, together with the controls that are required to manage them [18], [50], [51]. The risk identification process starts by identifying the information assets, potential threats and vulnerabilities. These elements are important when identifying the source of incidents that affect the university information assets [50]. The results from cross-case analysis also indicate that risk assessment was the key element that could determine the comprehension of the security policy's contents. Currently, there are various tools available for security threat assessment such as Common Criteria, OCTAVE, CORAS and CySeMoL [52]. However, even though there are numerous tools and techniques that can facilitate the identification and analysis of risks, it is recommended that a multidisciplinary workshop discussion be included in the threat analysis [18]. This workshop is important as it can assess and evaluate all IT elements that cover every department in the organization [50].

In addition, it requires the subject matter expert on operations or business owners to identify threats, vulnerabilities, incidents and events or the assessors to come from policy team members to evaluate these elements. The next stage is the development process, which prepares policy construction. Once the policy team has identified the issues, the team needs to investigate the security control and legal requirements concerning the allegations against the identified issues. This preparation process will also consider cultural elements, organizational structure and change management issues during the construction of the policies. One other element that should be considered in this prepatory stage is to identify the best practice guides and standards in the industry and government as well as in the field of higher education. This might include the benchmarking of similarities in the policies with other institutions in order to analyse the contents and legislation or other external regulations that outfit the policy proposal. Once all the above elements are analysed, the final stage in the preparation process is to create and review the existing policies. Meanwhile, the rest of the development process concerns writing policy documents and obtaining policy approval. However, before it can be endorsed by the top management and later implemented, the policy should be reviewed by numerous stakeholders or any group that has an interest in the policy. It is important to ensure that all the users in the organization have a sense of ownership of the security policy and facilitate the acceptance of the security policy.

3) Implementation Phase

Once the policy has been approved by the management, the policy documents should be published via any mode of communication provided it is made available to all organization employees or users [53]. This is usually executed by posting the policies on the company intranet site, emailing it or circulating it as a printed document. The documents should also be easily accessible and available to be downloaded, printed, or saved. Moreover, when dealing with people who are ignorant about their organisation's security policy, the awareness program will be a solution [54]. However, this program must specify the actions required by users and the solemnity actions that could be taken against those who are non-compliant or violate the security policy. Furthermore, an effective security awareness process needs the support of top management to improve security awareness by endorsing the security awareness program and setting a high priority for security compliance [54].

The last process in the implementation phase is the maintenance and monitoring of policies. A security policy is commonly designed as a dynamic document and should be flexibly to allow frequent updates as technology or management experience periodically changes. The development of a security policy is not a simple project. To be an effective policy, the policy custodian should be responsible for maintaining a policy team that is knowledgeable in security techniques, the target information systems environment and the organization's regulations. It is important for the security policy to be constantly evaluated and reviewed to ensure that the new regulations, latest threats, and government policies are kept up-to-date [55]. In addition, [35] also agreed that the

security violations, deviations, and audit information should also be regularly reviewed in line with security policy update. The result of this process helps to identify the area where the policy is not enforced or where frequent policy violations occur.

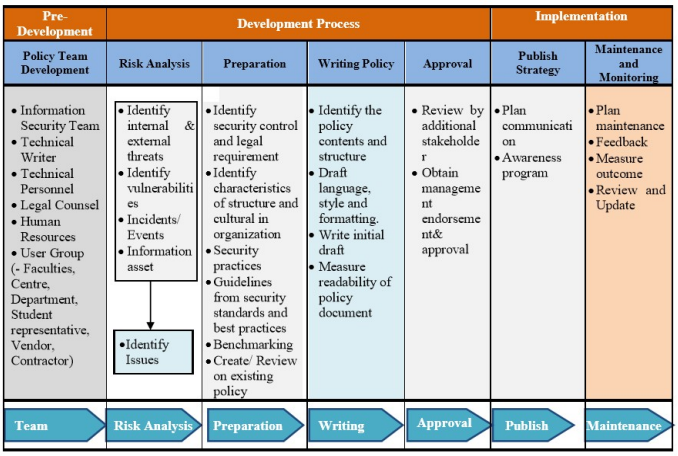

Figure 2: A Generic Framework for Information Security Policy Development.

V. CONCLUSION

It is necessary for the university community in general to be aware of the importance of strategic security policy planning and development in institutions of higher education. The process of developing an effective information system security policy is straightforward. However, the challenges to corporate information system security policies are that they need to understand how to effectively develop and implement security policy according to the needs of the entire institution's stakeholders. The second challenge is risk analysis, which is the core process involved when developing any type of information security process. The common mistake reported by respondents in case study analyses is that they were ignored as well as the lack of feedback on security threats from user groups such as users from faculties, departments, students and contractors. As a result, in cases where a violation of the information security-related rules occurs, it is less likely that related rules would be enforced because incomplete or incomprehensible security policies were developed. Thus, the proposed framework provides a holistic process for IHE to envisage during security policy development and implementation practices. This proposed framework could guide both the comprehensive and sustainable information security policies. Most importantly, the framework is able to aid any practitioner in improving or establishing a policy management program in his organization. Practitioners can also use this framework as a training tool to teach security policy development and management. Practitioners can use the framework to develop and analyse new policy or their current policy programs from a holistic or system's viewpoint that takes into consideration the overall flow and interacting phases.

FUTURE WORK

Since this study focused on a generic framework for information security policy, there is still a need for further exploration of specific development processes such as Acceptable Use Policy or any specific system security policy. This can be used as a guideline for any policy maker in IHE to construct a comprehensive information security policy.

REFERENCES

[1] B. Lebek, J. Uffen, M. H. Breitner, M. Neumann, and B. Hohler, "Employees' information security awareness and behavior: A literature review," in *Proceedings of the Annual Hawaii International Conference on System Sciences*, 2013, pp. 2978–2987.

[2] Z. A. Soomro, M. H. Shah, and J. Ahmed, "Information security management needs more holistic approach: A literature review," *Int. J. Inf. Manage.*, vol. 36, pp. 215–225, 2016.

[3] M. E. Whitman and H. J. Mattord, *Principles of Information Security*. 2012.

[4] J. Cox, "Information systems user security: A structured model of the knowing–doing gap," *Comput. Human Behav.*, vol. 28, no. 5, pp. 1849–1858, Sep. 2012.

[5] P. Ifinedo, "Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition," *Inf. Manag.*, vol. 51, no. 1, pp. 69–79, Jan. 2014.

[6] S. A. Waddell, "A Study of the Effect of Implementing Information Security Policy on Information Security Culture and Information Security Effectiveness in an Organization," 2013.

[7] R. E. Crossler, A. C. Johnston, P. B. Lowry, Q. Hu, M. Warkentin, and R. Baskerville, "Future directions for behavioral information security research," *Comput. Secur.*, vol. 32, pp. 90–101, Feb. 2013.

[8] S. Waddell, "A Study of the Effect of Information Security Policies on Information Security Breaches in Higher Education Institutions (Order No. 3604516).," 2013.

[9] N. B. Lucila, "Information Security Policy Development: A Literature Review," *Int. J. Innov. Res. Inf. Secur.*, vol. 3, no. 4, pp. 1–7, 2016.

[10] M. Warkentin, A. C. Johnston, J. Shropshire, and W. Bennett, "Continuance of Protective Security Behavior: A Longitudinal Study," *Decis. Support Syst.*, 2016.

[11] J. Shropshire, M. Warkentin, and S. Sharma, "Personality, attitudes, and intentions: Predicting initial adoption of information security behavior," *Comput. Secur.*, vol. 49, pp. 177–191, 2015.

[12] K. J. Knapp, R. Franklin Morris, T. E. Marshall, and T. A. Byrd, "Information security policy: An organizational-level process model," *Comput. Secur.*, vol. 28, no. 7, pp. 493–508, 2009.

[13] G. D. Doherty, "On quality in education," *Qual. Assur. Educ.*, vol. 16, no. 3, pp. 255–265, 2008.

[14] N. F. Doherty and H. Fulford, "Do Information Security Policies Reduce the Incidence of Security Breaches: An Exploratory Analysis," *Inf. Resour. Manag. J.*, vol. 18, pp. 21–39, 2005.

[15] N. F. Doherty, L. Anastasakis, and H. Fulford, "The information security policy unpacked: A critical study of the content of university policies," *Int. J. Inf. Manage.*, vol. 29, no. 6, pp. 449–457, Dec. 2009.

[16] T. Grobler and S. von Solms, "Assessing the policy dimension," in *Information Security South Africa*, 2004.

[17] N. Sohrabi, R. Von Solms, S. Furnell, P. Elizabeth, and S. Africa, "Information security policy compliance model in organizations,"

Comput. Secur., vol. 56, pp. 1–13, 2016.

[18] T. Tuyikeze and S. Flowerday, "Information Security Policy Development and Implementation: A Content Analysis Approach," in *Proceedings of the Eighth International Symposium on Human Aspects of Information Security & Assurance*, 2014, no. Haisa, pp. 11–20.

[19] S. V. Flowerday and T. Tuyikeze, "Information security policy development and implementation: The what, how and who," *Comput. Secur.*, vol. 61, pp. 169–183, 2016.

[20] N. F. Doherty, L. Anastasakis, and H. Fulford, "Reinforcing the security of corporate information resources: A critical review of the role of the acceptable use policy," *Int. J. Inf. Manage.*, vol. 31, no. 3, pp. 201–209, 2011.

[21] S. Maynard and A. Ruighaver, "What makes a good information security policy: a preliminary framework for evaluating security policy quality," in *Proceedings of the fifth annual security …*, 2006, pp. 1–15.

[22] S. Goel and I. N. Chengalur, "Metrics for characterizing the form of security policies," *J. Strateg. Inf. Syst.*, vol. 19, no. 4, pp. 281–295, Dec. 2010.

[23] R. P. Kusserow, "Developing and Managing Compliance Policy Documents," *J. Heal. Care Compliance*, no. June, pp. 27–31, 2014.

[24] R. Baskerville and M. Siponen, "An information security meta-policy for emergent organizations," *Logist. Inf. Manag.*, vol. 15, no. 5/6, pp. 337–346, Dec. 2002.

[25] F. Bjorck, "Institutional theory : A new perspective for research into IS / IT security in organisations," in *Proceedings of the 37th Hawaii International Conference on Systems Sciences*, 2004, vol. 0, no. C, pp. 1–5.

[26] J. D'Arcy, A. Hovav, and D. Galletta, "User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach," *Inf. Syst. Res.*, vol. 20, no. 1, pp. 79–98, Mar. 2009.

[27] M. Workman, W. H. Bommer, and D. Straub, "Security lapses and the omission of information security measures: A threat control model and empirical test," *Comput. Human Behav.*, vol. 24, no. 6, pp. 2799–2816, Sep. 2008.

[28] M. Asri, M. Stambul, and R. Razali, "An Assessment Model of Information Security Implementation Levels," in *International Conference on Electrical Engineering and Informatics*, 2011, no. July.

[29] M. Siponen and R. Willison, "Information security management standards: Problems and solutions," *Inf. Manag.*, vol. 46, no. 5, pp. 267–270, Jun. 2009.

[30] Y. Rezgui and A. Marks, "Information security awareness in higher education : An exploratory study," *Comput. Secur.*, vol. 27, no. 7–8, pp. 241–253, 2008.

[31] S. C. Clark, R. A. Griffin, and C. K. Martin, "Alleviating the policy paradox through improved institutional policy systems: A case study," *Innov. High. Educ.*, vol. 37, no. 1, pp. 11–26, 2012.

[32] C. T. Mauritian, "Guideline on Information Security Policy," Mauritius, 2011.

[33] T. Wiander, "Implementing the ISO/IEC 17799 standard in practice-experiences on audit phases," *Conf. Res. Pract. Inf. Technol. Ser.*, vol. 81, no. Aisc, pp. 115–119, 2008.

[34] V. Etsebeth, "Information Security Policies–the Legal Risk of Uninformed Personnel," in *Proceedings of the 6th Annual Information Security South Africa Conference,* 2006, pp. 29–1.

[35] S. Diver, "Information Security Policy - A Development Guide for Large and Small Companies," 2007.

[36] M. Corpuz, "The enterprise information security policy as a strategic business policy within the corporate strategic plan," in *Proceedings of the 15th World Multi-Conference on …*, 2011, pp. 275–279.

[37] M. Luker and R. Petersen, "Computer and Network Security in Higher Education Information Security," 2003.

[38] O. Sookdawoor, "An Investigation of Information Security Policies and Practices in Mauritius," 2002.

[39] R. . Hallsworth.M, Parker.S, "Policy Making in The Real World: Evidence and Analysis," 2015.

[40] M. Karyda, E. Kiountouzis, and S. Kokolakis, "Information systems security policies : a contextual perspective," *Computer. Security,* vol. 24, pp. 246–260, 2005.

[41] M. Computer, E. Response, and N. C. Board, "Guideline on Information Security Policy," no. 4, 2011.

[42] F. Cuppens and C. Saurel, "Specifying a security policy: a case study," in *Proceedings 9th IEEE Computer Security Foundations Workshop*, 1996, pp. 123–134.

[43] A. W. Kadam, "Information Security Policy Development and Implementation," *Inf. Syst. Secur.*, vol. 16, no. 5, pp. 246–256, Nov. 2007.

[44] M. S. Gross and K. Wada, "Campus IT Policy Development," in *EDUCAUSE Annual Conference*, 2013.

[45] V. Anand, J. Saniie, and E. Oruklu, "Security Policy Management Process within Six Sigma Framework," vol. 2012, no. January, pp. 49–58, 2012.

[46] C. Fischbach and D. Meeks, "Institutional Policy Management Critical Success Factors & Best Practices," in *ACUPA Annual Conference*, 2013, pp. 1–35.

[47] P. Runeson and M. Höst, "Guidelines for conducting and reporting case study research in software engineering," *Empir. Softw. Eng.*, vol. 14, no. 2, pp. 131–164, 2009.

[48] T. G. Harwood and T. Garry, "An Overview of Content Analysis," *Mark. Rev.*, vol. 3, no. 4, pp. 479–498, 2003.

[49] R. Franzosi, "Content Analysis: Objective, Systematic, and Quantitative Description of Content," 2008.

[50] T. Peltier, "Risk Assessment Process," 2014.

[51] B. Blakley and E. Mcdermott, "Information Security is Information Risk Management," 2002, pp. 97–104.

[52] J. E. Mbowe, I. Zlotnikova, S. S. Msanjila, and G. S. Oreku, "A Conceptual Framework for Threat Assessment Based on Organization ' s Information Security Policy," *J. Inf. Secur.*, vol. 5, no. October, pp. 166–177, 2014.

[53] C. R. McClure and P. T. Jaeger, "Government information policy research: Importance, approaches, and realities," *Libr. Inf. Sci. Res.*, vol. 30, no. 4, pp. 257–264, 2008.

[54] J. Bayuk, "Security through process management," 1997.

[55] K. Hong, Y. Chi, L. R. Chao, and J. Tang, "An empirical study of information security policy on information security elevation in Taiwan," *Inf. Manag. Comput. Secur.*, vol. 14, no. 2, pp. 104–115, 2006.