Applied Computing and Informatics (2011) 9, 107–118

King Saud University
Applied Computing and Informatics
www.ksu.edu.sa
www.sciencedirect.com

ORIGINAL ARTICLE

A new comprehensive framework for enterprise information security risk management

Mohamed S. Saleh [a], **Abdulkader Alfantookh** [b,*]

[a] *Bradford University, Bradford, United Kingdom*
[b] *Ministry of Higher Education, Riyadh, Saudi Arabia*

Received 25 November 2009; accepted 14 February 2011
Available online 6 June 2011

KEYWORDS

Enterprise security;
Information security;
Risk management;
Six-sigma;
STOPE view

Abstract With the wide spread use of e-transactions in enterprises, information security risk management (ISRM) is becoming essential for establishing a safe environment for their activities. This paper is concerned with presenting a comprehensive ISRM framework that enables the effective establishment of the target safe environment. The framework has two structural dimensions; and two procedural dimensions. The structural dimensions include: ISRM "scope" and ISRM "assessment criteria", while the procedural dimensions include: ISRM "process" and ISRM "assessment tools". The framework uses the comprehensive STOPE (strategy, technology, organization, people, and environment) view for the ISRM scope; while its assessment criteria is considered to be open to various standards. For the procedural dimensions, the framework uses the widely known six-sigma DMAIC (define, measure, analyze, improve, and control) cycle for the ISRM process; and it considers the use of various assessment tools. It is hoped that the framework would be widely used in the future as an open reference for ISRM.

* Corresponding author.
E-mail addresses: a@fantookh.com, afantookh@mohe.gov.sa (A. Alfantookh).

Peer review under responsibility of King Saud University.
doi:10.1016/j.aci.2011.05.002

Production and hosting by Elsevier

1. Introduction

One of the essential functions of information technology (IT) governance is risk management, which aims at providing a safe environment for e-business and e-commerce. In support of this function, various IT organizations, concerned with standards have published different risk management methods. These methods have been and are being partially or fully adopted by enterprises using IT, and working in different fields, for identifying, analyzing, and minimizing risks for their IT activities.

It would have been more convenient for such enterprises if a comprehensive method that accommodates the various requirements of these methods, in a well designed and enhanced manner, is available. This would support risk management compatibility among enterprises, using IT, providing a common and safe environment for their e-business interaction.

This paper is concerned with introducing a comprehensive information security risk management (ISRM) framework for enterprises using IT. The structural scope of the framework is based on the STOPE (strategy, technology, organization, people, and environment) view which is becoming of increasing importance for structuring information security issues over its five distinct domains (Saleh et al., 2006, 2007, 2008; Esteves and Joseph, 2008); and the management process of the framework is associated with well known six sigma DMAIC (define, measure, analyze, improve, and control) cyclic phases (Pyzdek, 2003). In addition, the framework adds management criteria to its structural issues; and considers evaluation tools for its procedural phases. The framework also enables the integration and enhancement of the various available risk management methods and standards into its structural and procedural components. The paper describes the framework, and emphasizes its importance as a potential open reference for enterprise ISRM.

2. Related work

Nowadays, there are number of different types of risk management methodologies, some of them issued by national and international organizations (ISO/IEC TR 13335, 1998; NIST SP800-30, 2002; AS/NZS 4360, 2004; HB231, 2004; BSI Standard 100-3, 2005; ISO/IEC 27005, 2008), others issued by professional organizations (CRAMM, 2001; CORAS, 2003; OCTAVE, 2005; Magerit, 2006; Microsoft, 2006; Mehari, 2007) and the rest presented by research projects (Kailay and Jarratt, 1995; Smith and Eloff, 2002; Robert and Rolf, 2003; Karabacak and Sogukpinar, 2005; Hoffanvik and Stolen, 2006; Mayer et al., 2007). Each of these methods has been developed to meet a particular need and hence has a different objectives, steps, structure, and level of application. The common goal of these methods is to prioritize and estimate the risk value and to suggest the most suitable mitigation plan to eliminate or minimize that risk to an acceptable level (Vorster and Labuschagne, 2005).

In spite of the increasing number of standard and commercial risk management methods, various reports, surveys, and related literature indicate that the diffusion of the current risk management methods, within organizations has been very limited so far due to lack of awareness, high cost, need for expertise, and long process (NCC, 2000; DTI, 2002). In addition, the trust in these methods is very low due to the poor results, bulky confused reports and the narrow technological scope (Labushehagne and Eloff, 1998; Spears, 2006). Furthermore, the confused huge number of risk management methods (more than 200 now) create a problem to any organization willing to adopt one of these methods and the absent of an agreed reference benchmark or comparative framework for evaluating these methods limit its practical use in assessing the enterprises information security risks (Vorster and Labuschagne, 2005; Bornman and Labuschagne, 2006; Syalim et al., 2009).

Labuschagne and Eloff (1998) argues that most of the available risk management methods have a scientific core that emerged from the engineering origins of computing. These traditional methods used to manage enterprises risk and generally focused on the technology and this proposes technical solutions. The majority of these methods seldom consider human, organizational, strategic, or environmental factors. While technology is a necessary consideration, it is not the only element requiring recognition (Hang et al., 2008; Werlinger et al., 2009). In addition, the IT-centric approach to security risk analysis does not involve business users to the extent necessary to identify a comprehensive set of risks or to promote security awareness throughout the organization (Lategan and Solms, 2006). Nosworthy (2000) mentioned that in order to apply business continuity measures in a consistent, manageable and cost effective manner an organization-wide approach to a practical business continuity risk analysis should be adopted and applied to the business as a whole and not just the IT department.

Recently, many authors suggest the need for a holistic information security risk management method that minimizes the several shortcomings of the traditional risk management methods (Niekerk and Labuschagne, 2006; Spears, 2006; Zuccato, 2006; Anderson, 2007; Huang et al., 2008). The suggested method should be based on the standards and considers the special characteristics of information security domain and uses different techniques to combine the standard and professional methods under a comprehensive and practical information security risk management framework (Jung et al., 1999).

3. The target enterprise ISRM framework

The target ISRM framework has two main parts: one part is concerned with its structural view; while the other is associated with its procedural view. The structural view has two dimensions: scope and criteria; while the procedural view also has two other dimensions: process and tools. The framework is described in the following, in terms of these four dimensions.

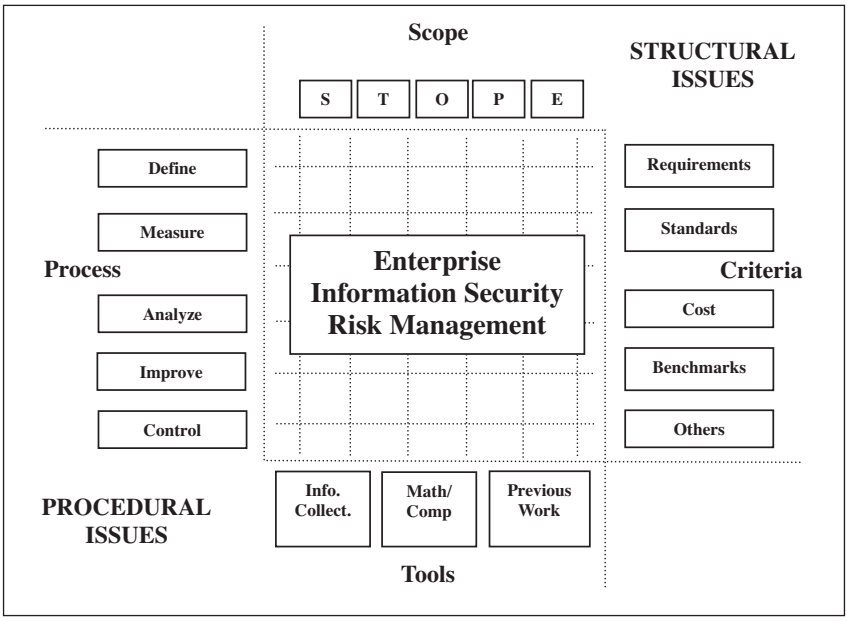

Figure 1 The structure of the proposed enterprise ISRM framework.

- The "scope" of the framework is based on the five STOPE domains of strategy, technology, organization, people, and environment with different levels of details, associated with each domain.
- The management "criteria" of the framework is considered to be associated with the controls of the ISO family of information security standards. However, other requirements can also be considered.
- The "process" of the framework adopts the five cyclic phases of six-sigma model DMAIC: define, measure, analyze, improve, and control.
- The support "tools" of the framework may include the various means that would promote the work, including: survey tools, mathematical models, and computer software.

Fig. 1 illustrates the structure of the proposed framework. Further explanations of both its structural view and procedural view are to follow.

3.1. The structural view of the framework

The structural view of the proposed ISRM framework is described here in terms of its two dimensions: the STOPE-based scope, and the management criteria.

The STOPE-based scope of the framework would enable mapping the basic elements of the enterprise, associate with IT, to the domains of "strategy, technology, organization, people, and environment". The basic elements of an enterprise, with

Table 1 Enterprise assets considered by different references (ISO/IEC TR 13335, 1998; CRAMM, 2001) mapped on the STOPE domains.

STOPE	Assets main groups	
	Tangible (*Examples*)	Intangible
S	Information: (*Policy document*)	– Goodwill
T	Information: (*Data files*)	– Service to clients
	IT services: (*Messaging-active directory*)	– Public confidence
	Software: System (*Solaris*), Application (*Oracle*),	– Public trust
	Utilities (management tools)	– Competitive advantage
	Hardware: Hosts (*Servers*) other (*Printers*)	– Image of the organization
	Communication: Network (*Routers*), (*Cable*)	– Reputation
O	Documents: (*Management commitment*)	– Trust in services
	Agreements: (*Confidentiality-third party*)	– Employee moral
	Information: (*Research*)	– Productivity
	Other: (*User manuals-training material*)	– Loyalty
P	IT staff: (*IT security manager*)	– Ethics
	Employee: (*Senior management*)	
	Users: (*Inside/Outside*)	
	Contractors:(*Consultants*)	
	Owners:(*Stakeholders*)	
E	Services: (*Heating-lighting-power-AC*)	
	Equipment: (*Desks-Fax machines-Cables*)	
	Physical (infrastructure): (*Offices-facilities*)	

regards to ISRM, are considered to be its: assets, security challenges, and security controls. These are addressed in the following according to the STOPE-based scope.

"*Asset management*" is one of the main clauses of ISO 17799, and has two objectives: "responsibility of assets" and "information classification". ISO defines an asset "*as anything that has value to the organization*" (ISO/IEC 17799, 2005). This definition brings up the consideration of two types of assets: "tangible" and "intangible". Table 1 maps the tangible assets considered by different references to the five STOPE domains; this is a high-level mapping that can be refined into sub-levels of further details. The Table also considers intangible assets that are associated with multiple-domains.

Security challenges can be viewed as negative coins of two faces: threats and vulnerabilities. ISO defines threat as "*a potential cause of an unwanted incident, which may result in harm to a system or organization*"; and it defines vulnerability as "*a weakness of an asset or group of assets that can be exploited by one or more threats*" (ISO/IEC 17799, 2005). Table 2 maps ISO threats and vulnerabilities to the five STOPE domains. With regards to threats, the Table marks them as either: deliberate (D), accidental (A), or both (D&A).

Security controls are defined by ISO as "means of managing risk, including policies, procedures, guidelines, practices, or organizational structures, which can be of administrative, technical, management, or legal nature". Table 3 maps ISO information security clauses, objectives and controls (ISO/IEC 17799, 2005) to the five STOPE domains.

Table 2 Threats and vulnerabilities considered by different references (ISO/IEC TR 13335, 1998; CRAMM, 2001) mapped on the STOPE domains.

STOPE	Challenges main groups	
	Threats	Vulnerabilities
S	Policy:(inadequate)	
T	Malicious codes: (*Viruses*) D	Software: (*Configuration errors*)
	Software: (*Failures*) D&A	Hardware: (*Missing patches*)
	Hardware: (*Failures*) D&A	Communication: (*Unnecessary protocol*)
	Communication: (*Infiltration*) D	Media: (*Electrical interference*)
O	Agreement: (*Inadequate*) D	Document: (*No care at disposal*)
	Information: (*Errors*) D	
	Planning: (*Problems*) D	Procedures: (*Violations not reported*)
	Procedures: (*Incorrect*) D&A	
P	Employee: (*Sabotage*) D	Employee: (*Insufficient training*)
	Users: (*Inside/Outside/Theft*) D	
	Crackers: (*Malicious hacking*) D	
E	Industrial: (*Espionage*) D	Natural: (*Facility in flood zone*)
	Natural: (*Earthquake*) A	Physical: (*Unlocked doors*)
	Services: (*Power outage*) A	

Table 3 ISO information security clauses, objectives and controls (ISO/IEC 17799, 2005) mapped on the STOPE domains.

STOPE	ISO 17799: 2005 BASIC PARTS				
	Part No.	Clause	No. of objectives/ controls/factors		
S	5	Security policy	1	2	15
T	10	Communications and operations management	10	32	188
	11	Access control	7	25	120
	12	Information systems acquisition, development, and maintenance	6	16	96
O	6	Organization of information security	2	11	82
	7	Asset management	2	5	7
	13	Information security incident management	2	5	13
	14	Business continuity management	1	5	33
P	8	Human resources security	3	9	30
E	9	Physical and environmental security	2	13	59
	15	Compliance	3	10	39
Total objectives, controls, and measures			39	133	682

The controls of ISO 17799 information security management standards have been previously investigated according to the STOPE view, for the purpose of easing their application to enterprises, and achieving safe IT activities (Saleh et al., 2006, 2007).

It should be noted that the framework would not be limited to the issues of the assets, threats, vulnerabilities, and controls considered above, but it would also be open to other potential issues.

The management criteria of the structural view would appear at all domains of the STOPE-scope of the proposed framework. The criteria may specify the

required security controls, on the various STOPE domains, relative to cost-benefit analysis. For the controls considered, it may provide benchmarks to their acceptable levels. In general, the management criteria would be associated with the strategy and requirements of the enterprise considered.

3.2. The procedural view

The procedural view of the proposed ISRM framework is described here in terms of its two dimensions: the six-sigma-based process and the support tools.

The six-sigma based process has the five-phase cyclic process of define, measure, analyze, improve, and control: DMAIC In the following, the processes of the risk management methods of the standards organizations and of the professional companies given above are mapped on the phases of the DMAIC process. Each of these phases is then addressed in terms of its objective, input and output.

Table 4 maps the processes of the key risk management methods, considered above, to the six-sigma cyclic phases of: ''define, measure, analyze, improve, and control''. This shows how the DMAIC process can accommodate these processes, providing a potential comprehensive risk management process for the future. This is enhanced further by giving the functions of each phase, in the process, as summarized in Table 5, and explained in the following.

The ''*define*'' *phase* specifies the basic elements of the risk management process. This phase would use the output of a previous cycle of the DMAIC process, or start a new process, depending on the case considered. This phase has a number steps as follows:

- establish the context of the reviewed area;
- map the existing situation of the enterprise (assets, threats, vulnerabilities, controls) to the STOPE domains;
- specify the owner of each asset;
- specify the location of each asset;
- specify the source of the threat;
- define the level of detail; and
- give security requirements.

The output of this phase would be a STOPE view of the current state of the basic elements of information security in the considered enterprise.

The ''*measure*'' *phase* assess the basic elements of the framework according to a specified criteria. It receives the output of the ''define'' phase and add the following information to each element:

- assessment of the current state of assets;
- assessment of the current state of threats;
- assessment of the current state of vulnerabilities; and
- assessment of the current state of controls.

Table 4 Mapping the processes of key risk management methods to the adopted DMAIC phases of the six-sigma.

Six-Sigma	Key risk management methods					
	AS/NZS: 4360	ISO/IEC TR 13335-3	NIST 800-30	OCTAVE	CRAMM	Microsoft
Define	Communicate and consult	Risk analysis	System characterizations	Knowledge of management–operational area–staff	Asset identification	
	Establish the context			Create threat profile		
Measure	Identify risks		Threat identification	Identify key components	Asset valuation	
			Vulnerability identification	Evaluate selected components	Threat and vulnerability assessment	
Analyze	Analyze risk		Control analysis			Assessing risk
			Likelihood determination			
	Evaluate risk		Impact analysis			
			Risk determination			
Improve	Treat risk	Safeguards selection	Recommended controls	Develop protection strategy	Countermeasure selection and recommendation	Conducting decision support
		Policy and plan implementation	Risk assessment report			
			Cost-benefit analysis and selection of controls			Implement controls
			Implementation			
Control	Monitor and review	Follow-up	Test and evaluate			Measuring risk management program effectiveness

Table 5 The use of six-sigma five phase cyclic process DMAIC for ISRM.

	DMAIC Explanation		Output
Define	*Objective:* Specify current state enterprise IS		A STOPE view of the current state of the basic elements of information security in the considered enterprise
	Input: Collect information about enterprise basic elements		
	Assets	Tangible/intangible/owner/location	
	Threats	Deliberate/accidental	
	Vulnerabilities	Technical/organizational	
	Controls	Existing/planned	
Measure	*Objective:* Assess the current state of information security		A STOPE view of the critical assets, associated with the assessment of the threats & vulnerabilities they are facing, and with the security controls used
	Input: Define stage outputs/expert or owner view		
	Assets	Valuation (direct/indirect)	
	Threats/assets	Possible damage	
	Vulnerability/asset	Weakness in the security measures	
	Controls / assets	STOPE/ISO based evaluation approach for control analysis (Saleh et al., 2007)	
	Assets requirements	Confidentiality/availability/integrity	
Analyze	*Objective:* Find the gap between the current state and the required state of protection		A STOPE view of the gap between security requirements and the current state of security, considering all critical assets
	Input: Assessment of enterprise current state from "measure" phase; and "required security protection criteria		
	Model	Development of an analytical model for gap analysis	
	Evaluation	Using the model to evaluate current state of security versus required one	
	Gap	Determination of the security gap that needs to be closed, so that the required improvement is achieved	
Improve	*Objective:* Specify required improvements to close the gap between the current state and required state		A STOPE view of a plan of action of what should be done to close the gap and achieve the required security
	Input: Required state and current state		
	Directions	Development of directions to close the security gap and achieve the required improvement	
	Plan	Designing an action plan that follows the directions	
Control	*Objective:* Implement improvement, monitor and evaluate; repeat process.		Implementation of the plan, operation, performance, process activation
	Input: Action plan for improvement		
	Implementing	The action plan for improvement	
	Monitoring	The changing state	
	Documentation	Documenting the work	
	Re-initiating	The DMAIC process	

The output of this phase would be a STOPE view of the critical assets, associated with the assessment of the threats and vulnerabilities they are facing, and with the security controls used.

The "analyze" phase analyzes the gap between the current state and the required state of protection from challenges. This will be based on the output of the

"measure" phase on the one hand, and on required "criteria" on the other. The basic steps of this phase are as follows:

- development of an analytical model for gap analysis;
- using the model for the evaluation of the current state versus the required state; and
- determination of the security gap between the current state and the required state.

The output of the phase is a STOPE view of the gap between security requirements and the current state of security, considering all critical assets.

The "improve" phase considers the security state and the required state. It has the following main steps:

- development of directions to close the security gap and achieve the required improvement; and
- designing an action plan that follows the directions.

The output of the phase is a STOPE view of a plan of action of what should be done to close the gap and achieve the required security improvement.

The "control" phase considers the improvement plan and performs the following main steps:

- implementation of the plan;
- monitoring the changing state; and
- documenting the work.

The output of the phase is an improved security, in addition to going into another cycle for responding to new requirements and change.

3.3. Support tools

The proposed framework considers that "support tools" would be required for the execution of the various DMAIC phases. Such tools have also been considered by previous methods (Saleh and Bakry, 2008). The tools would include, but not limited to:

- information collection and survey tools;
- modeling and mathematical tools;
- computational methods and software packages; and
- other related or combined tools.

4. Conclusions

This paper has presented a new enterprise ISRM framework that enjoys attractive features for future use. The "STOPE-scope" of the framework enables it to accommodate the wide range of issues associated with ISRM, in a well structured

and open manner. This does not only integrates the issues that have been considered by other methods, but also permits other or emerging issues to be considered. The six-sigma ''DMAIC process'' of the framework allows it to accommodate the various processes of other ISRM methods in a one unified and widely accepted process. In addition, the framework respond to the need of using a ''management criteria'', and permits various criterion to be taken into account, including ISO information security controls, and considering pre-determined benchmarks. The framework also considers the use of ''support tools'' for performing the various phases of the process efficiently as is the case with other ISMR methods. The comprehensive and flexible nature of the framework makes it a candidate to become an ''open reference'' for ISRM that can be widely used by enterprises seeking safe environment for their e-based business. The authors hope that the time to be taken toward the wide scale use of the framework will not be very long.

References

Anderson, K., 2007. Convergence: a holistic approach to risk management. Network Security (5), 4–7.

AS/NZS 4360, 2004. Risk Management. 3rd ed. Standards Australia/Standards New Zealand, Sydney, Australia, Wellington, New Zealand.

Bornman, W.G., Labuschagne, L., 2006. A comparative framework for evaluating information security risk management methods. Technical report, Standard Bank Academy for Information Technology, Rand Afrikaans University.

BSI Standard 100-3, 2005. Risk Analysis based on IT-Grundschutz-Version 2.0, Federal Office for Information Security: Bundesmt Fur Sicherheit in der Informationstechnik, Germany.

CORAS, 2003. Available from: < http://coras.sourceforge.net/ > (accessed 24.05. 10).

CRAMM user guide, 2001. Risk Analysis and Management Method, United Kingdom Central Computer and Telecommunication Agency (CCTA), UK.

Department for Trade and Industry DTI, 2002. Information Security Breaches: 2002 Survey, Department for Trade and Industry, London.

Esteves, J., Joseph, R.C., 2008. A comprehensive framework for the assessment of e-Government projects. Government Information Quarterly 25, 118–132.

HB231, 2004. Information Security Risk Management Guidelines, Australia/New Zealand, Sydney, Australia, Wellington, New Zealand.

Huang, J., Ding, Y., Hu, Z., 2008. Knowledge based model for holistic information security risk analysis. In: International Symposim on Computer Science and Computational Technology, 20–22th Dec., IEEE, Shanghai, pp. 88–91.

Ida Hoffanvik, Detil Stolen, 2006. A graphical approach to risk identification. In: International Conference on Model Driven Engineering Languages and Systems (MoDELS'06), vikyme 4199 of Lecture Notes in Computer Science, Springer Verlag, pp. 574–588.

International Standards Organization, 2008. ISO/IEC 27005: 2008. Information Technology-Security Techniques-Information Security Risk Management, International Standards Organization, Geneva, Switzerland.

ISO/IEC 17799: (E), 2005. Information Technology-Security Techniques-code of Practice for Information Security Management, International Standards Organization, Geneva, Switzerland.

ISO/IEC TR 13335, 1998. Information Technology-guidelines for the Management of IT Security – Part 3, International Standards Organization, Geneva, Switzerland.

Jung, C., Han, I., Suh, B., 1999. Risk analysis for electronic commerce using case-based reasoning. International Journal of Intelligent Systems in Accounting, Finance and Management 8 (1), 61–73.

Kailay, M.P., Jarratt, P., 1995. RAMeX: a prototype expert system for computer security risk analysis and management. Computer & Security 14 (5), 449–463.

Karabacak, B., Sogukpinar, I., 2005. ISRAM: information security risk analysis method. Computer & Security 24 (2), 147–159.

Labushehagne, L., Eloff, J.H., 1998. The use of real-time risk analysis to enable dynamic activation of countermeasures. Computer & Security 17 (4), 347–357.

Lategan, N., Solms, R., 2006. Towards enterprise information risk management a body analogy. Computer Fraud & Security (12), 15–19.

Magerit, 2006. Methodology for Information Systems Risk Analysis and Management: Book1–The Method, Ministerio de Administracones Publicas, Madrid.

Mayer, N., Heymans, P., Matulevicius, R., 2007. Design of a modeling language for information system security risk management. In: Proceedings of the First International Conference on Research Challenges in Information Science (RCIS '07).

Mehari, 2007. Overview, Club de la Securite de I'Information Francais (CLUSIF).

Microsoft, 2006. The security risk management guide, Microsoft solutions for security and compliance & Microsoft security center of excellence, Microsoft Corporation, USA.

National Computing Center (NCC), 2000. The Business Information Security: 2000 Survey, National Computing Center, UK.

Niekerk, L., Labuschagne, L., 2006. The PECULIUM model: information security risk management for the south african SMME. In: Proceedings of the ISSA from Insight to Foresight Conference, 5–7th July 2006, Sandton, South Africa.

NIST SP800-30, 2002. Risk Management Guide for Information Technology Systems, National Institute of Standards and Technology, USA.

Nosworthy, J.D., 2000. A practical risk analysis approach: managing BCM risk. Computer & Security 19 (7), 596–614.

OCTAVE, 2005. Managing Information Security Risk, Carnegie Mellon, USA.

Pyzdek, T., 2003. The Six Sigma Handbook. McGraw-Hill, New York.

Robert, C., Rolf, M., 2003. Operationalizing IT risk management. Computer & Security 22 (6), 87–493.

Saleh, M.S., Alrabiah, A., Bakry, S.H., 2007. A STOPE model for the investigation of compliance with ISO 17799–2005. Journal of Information Management & Computer Security, Emerald 15 (4), 283–294.

Saleh, M.S., Alrabiah, A., Bakry, S.H., 2006. Using ISO 17799–2005 security management standard: a STOPE view with six sigma approach. International Journal of Network Management, Wiley 17 (1), 85–97.

Saleh, M.S., Bakry, S.H., 2008. An overview of key IT risk management methods. Saudi Computer Journal 6 (2).

Smith, E., Eloff, J.H.P., 2002. A prototype for assessing information technology risks in health care. Computer & Security 21 (3), 266–284.

Spears, J., 2006. A Holistic Risk Analysis Method for Identifying Information Security Risks: Security Management, Integrity, and Internal Control in Information Systems. ISBN:978-0-387-29826-9. pp. 185–202.

Syalim, A., Hori, Y., Sakurai, K., 2009. Comparison of risk analysis methods: mehari, magerit, NIST800-30 and microsoft's security management guide. In: Proceeding of the International Conference on Availability, Reliability and Security, 16–19th March 2009, IEEE, pp. 726–731.

Vorster, A., Labuschagne, L., 2005. A framework for comparing different information security risk analysis methodologies. In: Annual Research Conference of Computer Scientists and Information Technologists on IT Research in Developing Countries – SAICSIT, Conference Proceedings, pp. 95–103.

Werlinger, R., Hawkey, K., Beznosov, K., 2009. An integrated view of human, organizational, and technological challenges of IT security management. Information Management & Computer Security 17 (1), 4–19.

Zuccato, A., 2006. Holistic security management framework applied in electronic commerce. Computer & Security 26 (1), 256–265.