Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2008 Proceedings

Americas Conference on Information Systems (AMCIS)

2008

An Open Reference Framework for Enterprise Information Security Risk Management Using the STOPE Scope and the Six-Sigma Process

Mohamed Saad Saleh
University of Bradford, msmsaleh@bradford.ac.uk

Abdulkader Alfantookh
King Saud University, a@fantookh.com

John Mellor
University of Bradford, j.e.mellor@bradford.ac.uk

Saad Haj Bakry
King Saud University, shb@ksu.edu.sa

An Open Reference Framework For Enterprise Information Security Risk Management Using the STOPE Scope and the Six-Sigma Process

Mohamed Saad Saleh
University of Bradford
msmsaleh@Bradford.ac.uk

Abdulkader Alfantookh
King Saud Univesity
a@fantookh.com

John Mellor
University of Bradford
j.e.mellor@Bradford.ac.uk

Saad Haj Bakry
King Saud Univesity
shb@ksu.edu.sa

ABSTRACT

With the wide-spreading 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 introducing a new and 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 DAMIC (*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 provides useful tools for future applications.

Keywords

Enterprise security, information security, risk management, six-sigma, STOPE view.

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 and business, have published different risk management methods (AS/NZS, 2004; HB231, 2004; BSI Standard 100-3, 2005; ISO/IEC TR 13335, 1998; NIST SP800-30, 2002; OCTAVE, 2005; CRAMM, 2001; Microsoft, 2006). In the past, these methods have been used 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 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 scope of the framework is based on the STOPE (Strategy, Technology, Organization, People, Environment) view which is becoming of increasing importance for structuring information security issues over its five distinct domains (Saleh, Alrabiah, and Bakry, 2006, 2007, 2008); and the management process of the framework is associated with well known six sigma DMAIC (Define, Measure, Analyze, Improve, 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.

For presenting the framework, the paper starts by providing a background on ISRM considering the key methods available on the subject. The framework is then described in terms of its structural issues: scope and criteria; and its procedural issues: process and tools. Discussions and remarks are then given emphasizing the importance of the framework as a potential open reference for enterprise ISRM. The paper finally calls for the widespread use of the framework, in order to achieve a common and safe environment for e-business interactions among enterprises.

BACKGROUND

This section provides a background on risk management, as a preparation step toward introducing the target framework. The background includes two main sections: the first introduces the risk management concepts through presenting selected ISO (International Standards Organization) key ISRM terms; while the second reviews key ISRM methods including those recommended by standards organizations, professional companies, and other important sources.

Understanding Risk Management

ISO provides standards definitions to terms associated with risk and risk management. Here are some basic terms together with their definitions (ISO/IEC Guide 73, 2002):

- **Risk**: the combination of the probability of an event and its consequence.
- **Risk analysis**: the systematic use of information to identify sources, and to estimate risk.
- **Risk evaluation**: the process of comparing the estimated risk against given risk criteria to determine the significance of the risk.
- **Risk assessment**: the overall process of risk analysis and risk evaluation.
- **Risk treatment**: the process of selection and implementation of measures to modify risk.
- **Risk management**: the coordinated activities to direct and control an organization with regards to risk.
- **Risk policy**: the overall formal risk management intentions and directions.

Figure 1 provides an integrated view of the above terms illustrating their inter-relationships.

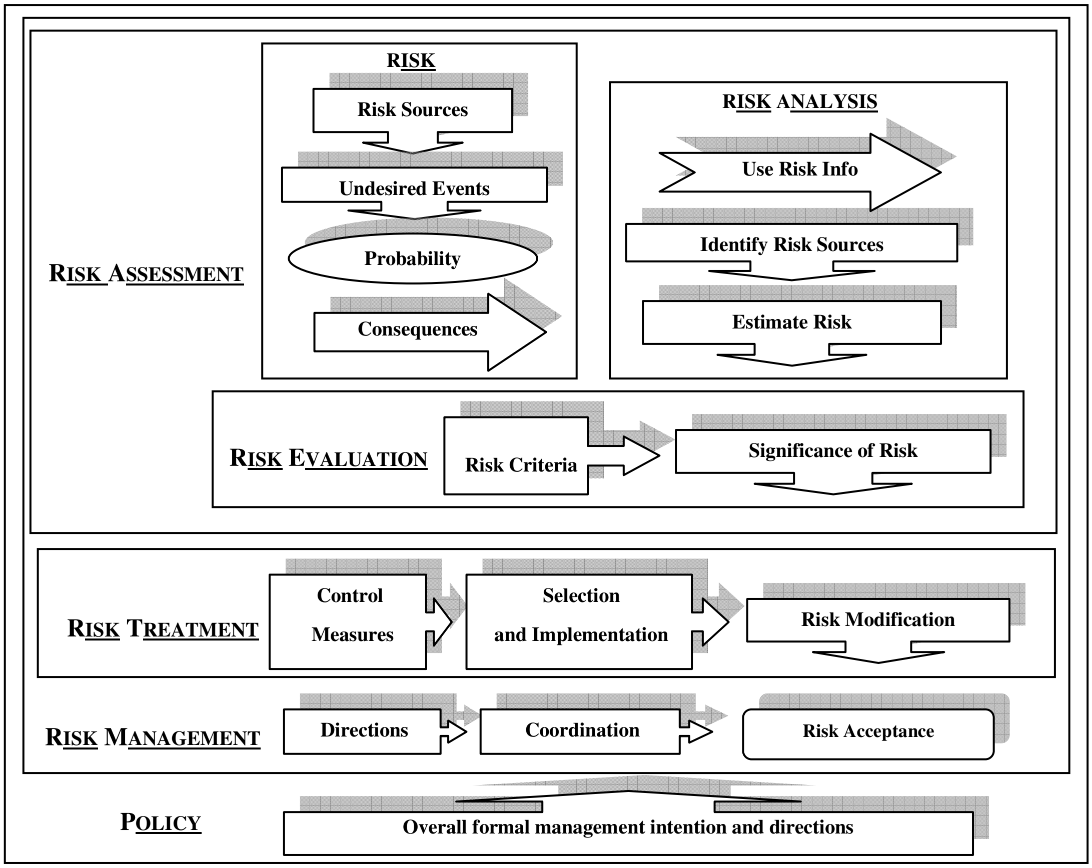

Figure 1. An illustrative view of ISO risk management terms.

Key Risk Management Methods

Key risk management methods are reviewed in the following including: methods given by standards organizations; methods provided by professional organizations; in addition to methods introduced by different researchers.

Standards Organizations Methods

Five risk management methods introduced by organizations concerned with standards are given here. The first is of generic nature that can be associated with risks in different fields; while the other four are related to information and IT.

- The first method is a part of a recommended risk management standard issued jointly by standard organizations of Australia and New Zealand (AS/NZS, 2004).
- The second method provides recommended guidelines, also issued jointly by the standards organization of Australia and New Zealand (HB231, 2004).
- The third is presented in the standard document recommended by the "*Bundesamt Fur Sicherheit in der Informationstechnik*" of Germany (BSI Standard 100-3, 2005).
- The fourth is given in a technical report recommended by the International Standards Organization (ISO/IEC TR 13335, 1998).
- The fifth is presented in a guide issued by the National Institute of Standards and Technology of the USA (NIST SP800-30, 2002).

Further related information on these methods is given in Table 1.

	Organization	Document	Title	Description
1	Australian/ New Zealand Standards	AS/NZS 4360:2004	Risk Management	Generic standard: Industry independent www.standards.com.au
2	Australian/ New Zealand Document	HB 231:2004	Information Security Risk Management Guidelines	Guidelines: For Information Security www.standards.com.au
3	Bundesamet fur Sicherheit in der Informationstechnik	BSI Standard 100-3:2005	Risk Analysis based on IT-*Gundschutz*	Methodology: Based on the IT-Grundschutz catalogues www.bsi.com.ge
4	National Institute of Standards and Technology: USA	NIST 800-30:2002	Risk Management Guide for Information Technology Systems	Recommendation: For IT systems www.nist.gov
5	International Standards Organization / International Electro-technical Commission	ISO/IEC TR 13335-3: 1998	Information Technology –Guidelines for the Management of IT Security – Part 3	Technical report: For IT systems security www.iso.org

Table 1. Key standards organizations documents concerned with risk management

Professional Organizations Methods

Professional organizations and IT companies also suggested a number of risk management methods three of these methods are presented below.

- The first; is given by a specialized group working at Carnegie Mellon University (OCTAVE, 2005).
- The second; is issued by UK Central Computer and Telecom Agency (CRAMM, 2001).
- The third; is recommended by Microsoft (Microsoft, 2006).

Further related information on these methods is given in Table 2.

Organization		Document	Title	Description
1	Carnegie-Mellon University / CERT: "Computer Emergency Response Team"	Operationally Critical Threat, Asset & Vulnerability Evaluation	OCTAVE Managing Information Security Risks	Guide with toolkits www.cert.org/octave
2	UK Central Computer and Telecom Agency	CCTA Risk Analysis and Management Methods	CRAMM Risk Assessment & Management	Guide with toolkits www.cert.org/octave
3	Microsoft	The Security Risk Management		Guide with toolkit www.microsoft.com

Table 2. Key professional organization documents concerned with risk management

The above methods issued by the standards organizations and the professional companies consider that risk management should be of continuous nature. In this respect, the Australian standard (AS/NZS 4360, 2004) states that: "*the risk management process is seen as an iterative one, consisting of steps that, when undertaken in sequence, enable continuous improvement in decision-making, and facilitate continuous improvement in performance*". In addition, the methods emphasize that enterprises should embed risk management practices into their culture and processes.

A recent paper by the authors has provided a more detailed review for these standards and methods (Saleh and Bakry, 2008). The paper stressed the need for a new comprehensive method, which arrange and combine the basic elements & steps of the risk management process in well-defined domains and clear successive steps, with continuous nature. This paper is a response to this emphasized need.

Other Methods

The management of information security risk has not been the concern of standards organizations or professional companies, but they were also the concern of individual researchers and research projects. Key methods of this type are introduced in the following.

Paper (Kailay and Jarratt 1995) introduced a qualitative computer security risk analysis and management prototype expert system (RAMeX) for small to medium sized commercial enterprises. The model deals only with intentional threats; and it relies on the European Commission Information Technology Security Evaluation Criteria (ITSEC) glossary to describe the terms concerned with risk management. Its procedure consists of seven steps; when undertaken in sequence, a report of recommended countermeasures to potential risks is produced. The model depends on the views and knowledge of the user of the system to identify risk. The paper also considers the development of software tool for easing the use of its model. The tool has four main components: the developer interface, the inference engine, the knowledge base, and the user interface.

The CORAS project (Raotis, Dimitrakos, et al., 2002) aims at addressing security-critical systems in general, but places particular emphasis on IT security. CORAS project considers a broad view to security that includes, not only the technology aspects, but also the humans interaction with the technology, and all relevant issues of the surrounding organization and society. The COARS risk management process is based on "AS/NZS 4360:1999 risk management" and on "ISO/IEC 17799:2000 code of practice for information security management". The COARS methodology has four dimensions, namely: the documentation framework, the risk management process, the integrated management and system development process, and the platform for the inclusion of tools.

Paper (Smith and Eloff, 2002) suggests a four steps risk management method entitled risk management in health care using cognitive fuzzy techniques (RiMaHCoF) for assessing IT risks in Health Care. The method is specific to health care business and uses the fuzzy logic technique to assess the risk. The paper focuses only on the third stage of the risk management method namely risk assessment.

In (Robert and Rolf, 2003) the authors suggest a risk management approach called "Business Process: Information Risk Management (BPIRM)". The approach combines the security focus, together with the business focus. The approach has two elements: the process and the content model. The BPIRM process has six phases linked by a feedback loop. The content model has seven layers and is based on the “value-chain” business view.

Method / Title		Year	Steps/Technique/Description
1	RAMeX	1995	Has two main phases: risk analysis and risk management The risk analysis has five steps producing identifications of: assets; threats; vulnerabilities; existing security countermeasures; and business impact The risk management has two steps: assessment of security countermeasures; recommendation of countermeasures to select from.
2	CORAS	2001	Has the following four pillars: A risk documentation framework. A risk management process based on AS/NZS 4360 and ISO 17799. An integrated risk management and development process. A platform for tool-inclusion based.
3	RiMaHCoF	2002	Concerned with IT risk in health-care. Considers four steps for risk management, including risk assessment. Risk assessment stage is based on a cognitive fuzzy-logic.
4	BPIRM	2003	Combines the security focus with the business focus. Has two elements: a process and a content model. The process has six phases, and the content model has seven layers The content model is based on the "value chain" business view.
5	Ontology-based method	2007	Enables knowledge sharing among security personnel, to support the management of risk for "Supply Chain Management (SCM) information security". Uses the ontology principles of the "Unified Problem-solving Method Development Language (UPML). Has three parts: "domain" associated with knowledge acquisition and modeling; "task" related to risk rating and management; and "resolution" concerned with minimizing SCM information security risks using problem solving method based on ontology.

Table 3. Key researchers risk management methods and techniques

Paper (Liu, 2007) is concerned with minimizing "Supply Chain Management (SCM) information security risks"; and it uses the ontology principles of the "Unified Problem-solving Method Development Language (UPML)" for this purpose. The ontology of UPML is seen as a flexible way to reduce design complexities. The target risk management of the paper is divided into three parts: "domain", which is associated with knowledge acquisition and modeling of organizational data valuation and security flaws and threats; "task", which is related to establishing risk rating and management; and "resolution", which is concerned with problem solving and minimizing the risk considered, using the ontology principles.

Further related information is given in Table 3. In spite of the importance of the above methods and techniques, none of them was successful in introducing a comprehensive approach for enterprise information security risk management. This is addressed in the next sections.

ENTERPRISE ISRM FRAMEWORK

The framework described below 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.

- 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.

Figure 2 illustrates the structure of the proposed framework. Further explanations of both its structural view and procedural view, are given in the next sections.

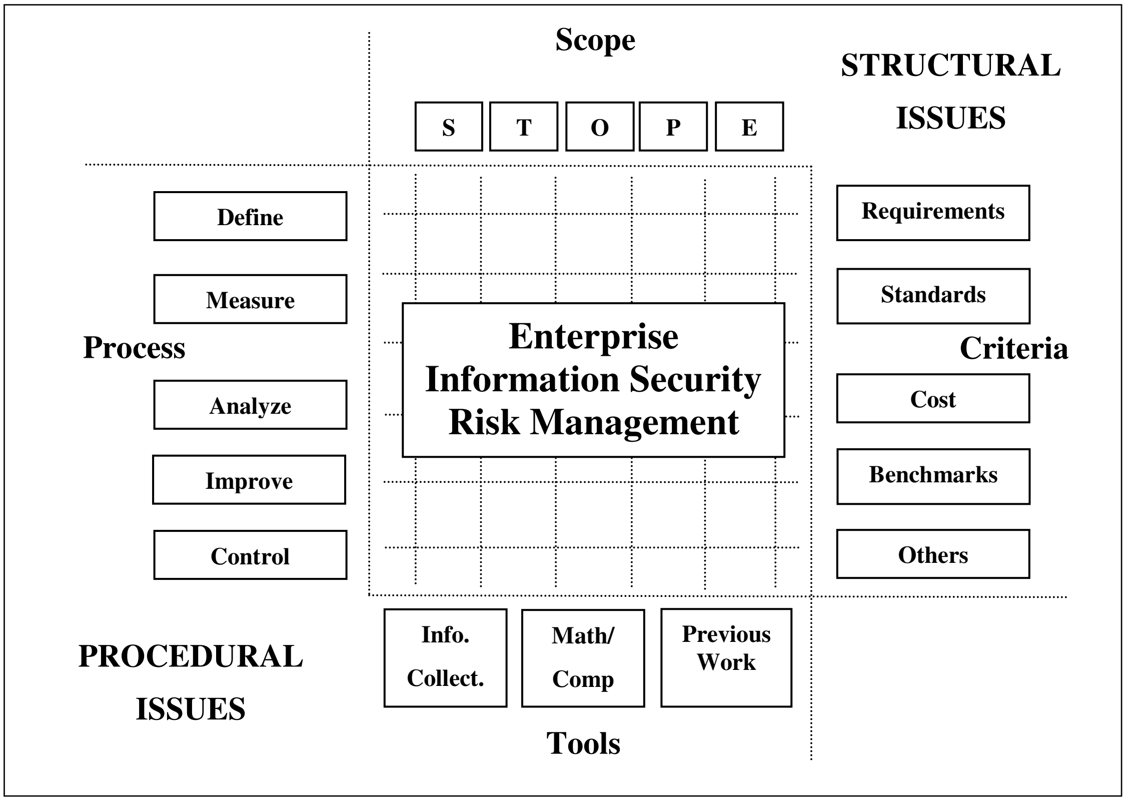

Figure 2. The structure of the proposed enterprise ISRM framework

THE STRUCTURAL VIEW

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

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 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.

Assets

One of the main clauses of ISO 17799 is "asset management", which has two objectives: “responsibility of assets” and “information classification”. ISO defined 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 4 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.

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

Table 4. Enterprise assets considered by different references (ISO/IEC TR 13335, 1998; CRAMM, 2001) mapped on the STOPE domains

Challenges

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 5 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).

Controls

ISO defines controls as "means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be of administrative, technical, management or legal nature". Table 6 maps ISO information security clauses, objectives and controls (ISO/IEC 17799, 2005) to the five STOPE domains.

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. For further information on this work, readers are referred to the papers (Saleh et al., 2006, 2007, 2008).

It should be noted that the framework would not be limited to the issues of the assets, threats, vulnerabilities, and controls considered by ISO, as it would be open to all other and potential issues.

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

Table 5. Threats and vulnerabilities considered by different references (ISO/IEC TR 13335, 1998; CRAMM, 2001) mapped on the STOPE domains

The Management Criteria

The management criteria dimension appears 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.

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

The adoption of six-sigma five-phase cyclic process DMAIC by the proposed framework is addressed here. 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.

The Six-Sigma Process and Other Methods

Table 7 maps the processes of key risk management methods, reviewed 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 function of each phase, in the process, as summarized in Table 8, and explained in the following.

STOPE		**ISO 17799:2005 BASIC PARTS**				
		Part No.	**Clause**	**No. of Objectives**	**No. of Controls**	**No of Factors**
S	**Strategy**	5	Security Policy	1	2	15
T	**Technology**	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	**Organization**	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	**People**	8	Human Resources Security	3	9	30
E	**Environment**	9	Physical and Environmental Security	2	13	59
		15	Compliance	3	10	39
Total objectives, controls and measures				**39**	**133**	**682**

Table 6. ISO information security clauses, objectives and controls (ISO/IEC 17799, 2005) mapped on the STOPE domains

The "Define" Phase

The main function of this phase is to specify 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 of 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

The main function of this phase is to assess the basic elements of the framework according to a specified criteria. It will receive 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.

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

The main function of this phase is to analyze 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

This 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

This phase considers the improvement plan and performs the following main steps:

- implementation of the plan;
- monitoring the changing state;
- documenting the work; and
- re-initiating the DMAIC process.

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

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, as given in section two. The tools would include, but not limited to, information collection and survey management tools, modeling and mathematical analysis, computational methods and software packages, in addition to other related tools.

Six-Sigma	**Key risk management methods**					
	AS/NZS:4360:2004	**ISO/IEC TR 13335-3**	**NIST 800-30:2002**	**OCTAVE**	**CRAMM**	**Microsoft**
Define	Communicate & consult Establish the context	Risk analysis	System characterizations	Management knowledge Operational area management knowledge Staff knowledge Create threat profile	Asset identification	Assessing risk
Measure	Identify risks		Threat identification Vulnerability identification	Identify key components Evaluate selected components	Asset valuation Threat and vulnerability assessment	
Analyze	Analyze risk Evaluate risk		Control analysis Likelihood determination Impact analysis Risk determination			
Improve	Treat risk	Safeguards selection Policy & plan Plan implementation	Recommended controls Risk assessment report Cost-benefit analysis and selection of controls Implementation	Develop protection strategy	Countermeasure selection and recommendation	Conducting decision support Implement controls
Control	Monitor and review	Follow-up	Test and evaluate			Measuring risk management program effectiveness

Table 7. Mapping the processes of key risk management methods to the adopted DMAIC phases of the six-sigma

DMAIC	Explanation		Output
Define	**Objective**: Specify current state enterprise information security		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 and 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	
	Vulnerabilities / assets	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 the current state from the "measure" phase; and the "required security protection criteria" of the enterprise concerned.		
	Model	development of an analytical model for gap analysis	
	Evaluation	using the model to evaluate the current state of security versus the 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, understanding and 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	

Table 8. The use of six-sigma five phase cyclic process DMAIC for ISRM

CONCLUSIONS

This paper has introduced a new framework for enterprise ISRM that enjoys attractive features for future use. From a structural viewpoint, the "STOPE-scope" of the framework enables it to accommodate the wide range of issues associated with ISRM in, a well structured and comprehensive manner. This has been illustrated in two main ways. It has been shown that the assets, vulnerabilities and threats considered by different risk management methods can be accommodated by the STOPE scope. In addition, ISO 17799 clauses and controls, that provide risk management criterion, have also been mapped on the STOPE scope.

From a procedural viewpoint, it has been shown that the six-sigma "DMAIC process", considered by the framework, can accommodate the processes of various risk management methods. The framework also considers the use of "support tools" for performing the various phases of the process efficiently; and in this respect it allows the use of any available or future tools for this purpose.

The comprehensive and flexible nature of the framework makes it a candidate to become an "open reference" for ISRM that can be used by enterprises seeking safe environment for their e-based business. In the future, the authors intend to provide future illustrative applications of the framework, in order to support its hoped wide-scale use.

REFERENCES

1. AS/NZS 4360 (2004) Risk Management Third Edition *Standards Australia/Standards New Zealand*, Sydney, Australia, Wellington, New Zealand.
2. 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.
3. CRAMM user guide (2001) Risk analysis and management method, *United Kingdom Central Computer and Telecommunication Agency (CCTA)*, UK.
4. HB231 (2004) Information Security Risk Management Guidelines, *Australia/New Zealand*, Sydney, Australia, Wellington, New Zealand.
5. ISO/IEC Guide 73: (2002) Risk Management-Vocabulary-Guidelines for Use in Standards; *International Standards Organization*, Geneva, Switzerland.
6. ISO/IEC TR 13335 (1998) Information Technology-Guidelines for the Management of IT Security- Part 3, *International Standards Organization*, Geneva, Switzerland.
7. ISO/IEC 17799: (E) (2005) Information Technology-Security Techniques-Code of Practice for Information Security Management; *International Standards Organization*, Geneva, Switzerland.
8. Kailay, M. P. and Jarratt, P. (1995) RAMeX a prototype expert system for computer security risk analysis and management, *Computer & Security*, vol. 14, pp. 449-463.
9. Liu, F. H. (2007) Constructing enterprise information network security risk management mechanism by using Ontology, *21 st International Conference on Advanced Information Networking and Applications Workshops (AINAW'07)*, IEEE computer society.
10. Microsoft, (2006) The security risk management guide, Microsoft solutions for security and compliance & Microsoft security center of excellence, *Microsoft Corporation*, USA.
11. NIST SP800-30 (2002) Risk management guide for information technology systems, *National Institute of Standards and Technology*, USA.
12. OCTAVE, (2005) Managing information security risk, *Carnegie Mellon*, USA.
13. Pyzdek T. (2003) The Six Sigma Handbook; *McGraw-Hill*: New York.
14. Raptis, D., Dimitrakos, T., et al. (2002) The COARS approach for model-based risk analysis applied to the e-commerce domain, *In Proc. Communication and Multimedia Security (DMS-2002)*, pp. 169-181, Kluwer.
15. Robert, C., and Rolf, M. (2003) Operationalizing IT risk management, *Computer & Security*, Vol. 22, No. 6, pp. 487-493.
16. Saleh M.S., Alrabiah, A., and Bakry, S.H. (2006) Using ISO 17799-2005 security management standard: “A STOPE view with six sigma approach, *International Journal of Network Managemen*t, Wiley, Vol. 17, Issue 1, p 85-97.

17. Saleh M.S., Alrabiah A., and Bakry S.H. (2007) A STOPE model for the investigation of compliance with ISO 17799-2005 *J Information Management & Computer Security*, Emerald, 15(4): 283-294.
18. Saleh M.S., Alrabiah A., and Bakry S.H. (2008) STOPE approach for ISO 17799 S-readiness assessment case-studies. *Computer & Security*, Elsevier science direct; (under review)
19. Saleh, M.S., and Bakry, S.H. (2008) An overview of key IT risk management methods, *Saudi Computer Journal*, (to appear).
20. Smith, E., and Eloff, J.H.P. (2002) A prototype for assessing information technology risks in health care, *Computer & Security*, Vol. 21, No. 3, pp.266-284.