International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-2 Issue-6, August 2013

An EISRM Frame Work - A New Approach for Embedding Information Security into the Enterprises

Kiran Kumar Kommineni, Adimulam Yesu Babu

Abstract— This paper aims at contributing to the knowledge by developing comprehensive Enterprise Information Security Risk Management (EISRM) framework that integrates typical approaches for information security risk management, and incorporates main components of key risk management methodologies. The practical evaluation, using the proposed enterprise information security readiness assessment model has been performed depending on a developed investigation form that used to investigate. The results demonstrate the effectiveness of the model in assessing and comparing enterprises information security readiness at all levels of the model, using numerical indicators and graphical representations.

Index Terms— Risk management; Assessment; Measures; Enterprise Security; Information Security;

I. INTRODUCTION

This paper aims to provide a comprehensive Enterprise Information Security Risk Management (EISRM) framework. The proposed EISRM framework is designed to incorporate the essential components of the key risk management methods on one hand, and depends on the TOPE (Technology, Organization, People and Environment) scope for its structural dimension and on the six-sigma DMAIC (Define, Measure, Analyze, Improve and Control) process for its procedural dimension on the other hand. The research also presents information security readiness indicators based on a developed analytical model that can assess numerically enterprise information security readiness. These indicators represent protection levels against possible risks, and provide an information security performance measure for future improvements. In addition, a practical cost-benefit analytical model is developed for applying the recommended protection measures cost effectively. Furthermore, for practical application of the proposed information security assessment model, the research suggests a gradual approach for the implementation of the ISO information security standards. Finally, for evaluating the EISRM framework and investigating the effective use of its associated models, practical case studies are presented and the data was analyzed using a developed computer tool. The main objectives are as follows:

- To the development of a comprehensive enterprise information security risk management framework.
- Focuses on the identification of the ISO/IEC 27002 based enterprise information security assessment measures.
- The development of an analytical model that provides integrated multi-level information security readiness indicators considering the risk controls of the ISO/IEC 27002 code of practice for information security management standard.
- The development of a practical model that provides cost-benefit trade-off between the estimated cost from applying the recommended information security protection measures and the expected benefits as a result from the protection of the information resources.
- The information security assessment model for investigating information security in different fields and presenting the assessment results numerically and graphically using a developed computer tool.
- The importance of managing information security risks and providing recommendations for improving the current situation information security management practices inside these enterprises.
- To the theory of information security management by unique analytical models via a comprehensive enterprise information security risk management framework.

II. MAIN ISSUES ABOUT EISRM FRAME WORK

This paper is concerned with introducing a comprehensive information security risk management (ISRM) framework for enterprises. The developed enterprise information security assessment model, to measure for the effectiveness of the implemented information security protection measures which considers as an essential input to the developed EISRM framework. The EISRM frame work is based on the four TOPE domains of strategy, technology, organization, people, and environment with different levels of details, associated with each domain. The framework is considered to be associated with the controls of the ISO family of information security standards.

2.1 Comparison of Proposed EISRM Framework with Other Professional Methods

The previous methods CRAMM and EBIOS have a technical nature. OCTAVE considers technical and organizational factors, while CORAS considers technical, organizational, human and environmental factors in dealing with the risk management programme. OCTAVE and EBIOS methods use the stakeholders in running the risk management programme, but CRAMM needs outsourced expertise.

Manuscript published on 30 August 2013.
***** Correspondence Author (s)
Mr. Kiran Kumar Kommineni, Assistant Professor, Department of Information Technology, Bapatla Engineering College, Bapatla - 522101, Guntur, AP,India.
Dr. Adimulam Yesu Babu, I/c Principal and Professor in Computer Science & Engineering, Sir. CR Reddy College of Engineering, Eluru -534007, West Godavari (Dt), AP., India.

Table 2-1 summarizes the main issues of the above reviewed professional organizations risk management methods that should be considered by the proposed EISRM framework. Table 2-1 summarizes and compares the main issues considered by the above reviewed risk- analysis based methodologies.

Table 2-1 Relation of professional risk management methods and the proposed EISRM framework.

Professional Method	Main Issues to be Considered by the EISRM Framework
CRAMM	Identification of IT assets. Sources of threats and vulnerabilities.
OCTAVE	Analysis team from the enterprise itself to lead the whole risk management activities. Development of security strategy and plan.
CORAS	Integration of risk management techniques. Platform for the inclusion of tools.
EBIOS	Identification of security needs by the users of the system. The analytical approach in dealing with risks. Identification of the security objectives. Identification of the security requirements.

These methodologies, as shown in Table 2-2, have the following main limitations:

- Most of these methods are country based and devoted for specific domain.
- In general, these methodologies lack definite framework or common approach for running enterprise's wide risk management programme that is based on effective Information Security Management System (ISMS) .
- Most of these methods are complex and depend on manual processes, and their results are informal most often in natural language.
- The assessment of the current state information security is not addressed by all of these methods.
- The results of these methods are not reusable to achieve continuous monitoring of the information security improvements.
- No reference standard economic model for the analysis of the proposed mitigation plans.

Table 2-2 Comparison of the risk-analysis based methods

Issue	Risk Analysis Method			
	CRAMM	OCTAVE	CORAS	EBIOS
Origin	UK	USA	Europe	France
Target sector	Business	Industry	Industry	Military
Domain	Information technology systems	Security critical systems	Security critical systems	Information systems security
Standard terminologies	No	No	No	No
Users of the method	Outside Expert	Stakeholders	Outside Expert	Stakeholders
Standard ISMS	No	No	No	No
Type of results	Reports	Reports	Reports & Graphs	Reports
Comprehensiveness	T	TO	TOPE	T
Assess current state	No	No	No	No
Economic analysis	No	No	No	No
Type of analysis	Qualitative	Qualitative	Qualitative	Qualitative
Software tool	Yes	Yes	Yes	Yes

2.2 Researchers Risk Management Methods and Techniques

The management of information security risks has not only been the concern of standard or professional organizations, but they are also the concern of individual researchers and research projects. Key methods of this type are introduced in Table 2-3. The main steps that are considered by these methods also appeared in the same table. Most of the researchers" methods concentrated only on improving techniques for calculating the risk value.

2.3 An Approach for EISRM framework

The best-practice approach for information security risk management depends mainly on the information security management best-practice standard documents in assessing enterprises " information security according to the requirements of these standards. The best-practices are the combined experiences of several companies that have already had great influence in the information security environment. Recently, there are many different information security standards and recommended security best-practice documents that evolved to address the issues of enterprise's information security risk management from different perspectives. National and international organizations, such as International Standards Organizations (ISO), the German Bundesamt fur Sicherheit id der Information stechnik (BSI Germany) and the Information Security Forum (ISF), have published information security management standards (ISO/IEC 2005; BSI-Germany 2004; ISF 2007). Two of the above mentioned best-practice standards will be presented in the following sections.

Table 2-3 Key researchers risk management methods and techniques

	Method / Title	Author/Year/Description/Steps/Technique
1	RAMeX	Kaily and Jarrah (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	RiMaHCoF	Smith and Eloff (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 technique.
3	BPIRM	Robert and Rolf (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.
4	Ontology-based	Liu (2007) • Ontology is a collection of concepts, which represent higher level knowledge in the knowledge hierarchy in a given enterprise. • 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 modelling; "task" related to risk rating &management; and "resolution" concerned with minimising SCM information security risks using problem solving method based on ontology.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

2.3.1 The Standard of Good Practice for Information Security

The ISF is an international independent organisation dedicated to benchmarking and best practices in information security. It was established in 1989 as a European security forum, and then expanded its mission and membership in the 1990s. Nowadays, it includes hundreds of members, including a large number of 300 leading organizations concerned with information security from all over the world. The ISF published the first issue of the Standard Of Good Practice (SOGP) for information security in 1996. The SOGP standard is based on the extensive knowledge and expertise of ISF members, the views of other national and international standard organizations and the results of earlier ISF information security status surveys. The standard is free for the members and the most recent version of the SOGP standard was published in 2007. Participants can make a comprehensive assessment of how well their enterprises are conforming to the standard (ISF 2007).

Table 2-4 The standard of good practice for information security aspects, areas and sections.

Aspect		Description	Area	Section
1	Security management	Covers topics relating to high-level direction for information security, arrangements for information security across the organisation and establishing a secure environment.	7	36
2	Critical business applications	Covers topics relating to requirements for securing business applications, identifying information risks and determining the level of protection required to keep information risks within acceptable limits.	6	25
3	Computer installations	Covers topics relating to the design and configuration of computer systems, management activities required to establish a secure computer installation and maintain service continuity.	6	31
4	Networks	Covers topics relating to network design and implementation, management activities required to run and manage secure networks including: local and wide area networks and voice communication networks.	5	25
5	Systems development	Covers topics relating to the application of information security during all stages of systems development including: design, build, testing and implementation.	6	23
6	End user environment	Covers topics relating to local security management, protecting corporate and desktop applications, and securing portable computing devices.	6	26
Total areas and sections			36	166

2.3.2 The ISO/IEC 27002 standard

The ISO/IEC 27002 is a management standard providing a code of practice for information security management. The standard was originated from the British standard BS 7799 and was first issued in 2000. It was revised and reissued in 2005. It is used by enterprises in managing their information systems security. The standard is adopted by various countries and used as a base for their regional information security standards. The ISO/IEC 27002 standard, as shown in Table 2-5, states 11 clauses, 39 security objectives and provides 133 controls to achieve those objectives.

A practical approach for information security management system implementation. The escape velocity concept is defined as the momentum a project must have in order to escape resisting forces without reverting back and failing. The approach is simple and straightforward in applying ISO/IEC 27002 to the enterprises using a computer tool. The adopted Key Performance Indicators (KPIs) of COBIT (Control Objectives for Information and related Technology) by this approach do not appear to be effective in measuring the performance of ISO/IEC 27002.

Table 2-5 The ISO/IEC 27002 clauses, objectives and controls

Clause		Description	Objective	Control
1	Security Policy	Aims to provide management direction and support for information security.	1	2
2	Organisation of information security	Organisation of the process implemented to manage information security.	2	11
3	Asset Management	Concentrate on asset inventories, information classification and labeling.	2	5
4	Human resources security	Considers permanent, contractor and third party user responsibilities.	3	9
5	Physical and environmental security	Controls the allowance of only authorised access to facilities and secure areas.	2	13
6	Communications and operations management	Focus on the correct and secure operation of information facilities.	10	32
7	Access control	Manage user access to information and include clear desk, network access and operating system access principles.	7	25
8	Information systems acquisition development and maintenance	Ensure the security of user-developed and the information system products.	6	16
9	Information security incident management	Ensures that incidents are communicated in a timely manner and that corrective action is taken.	2	5
10	Business continuity management	Focuses on business continuity plans and testing.	1	5
11	Compliance	Achieve it accordance with statutory, regulatory or contractual requirements or obligations, laws, audit and policy.	3	10
Total objectives and controls			39	133

III. INFORMATION SECURITY MANAGEMENT METHODS

Researchers also suggest a number of information security management methods, two of these methods are presented in the following:

3.1 The PROTECT Information Security Management Method

A comprehensive approach towards information security, namely PROTECT, which is an acronym for Policies, Risks, Objectives, Technology, Execute, Compliance and Team.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

The seven components of the PROTECT method are aimed at implementing and managing an effective information security program from technology to people perspective. They are summarized below:

- Policy component includes information security policies, procedures and standards, as well as guidelines.
- Risk methodologies such as CRAMM and OCTAVE, as well as automated tools to identify system vulnerabilities.
- Objective component refers to implementation of controls by considering the risk environment of the enterprise and not implementing more or less controls than what is required.
- Technology component includes hardware, software and systems‟ product components of the IT infrastructure.
- Execute component refers to a proper information security management system environment.
- Compliance component covers both internal compliance, with the enterprise's policies, and external compliance, with information security expectations set by outside parties.
- Team refers to the people component, i.e. all the employees of the enterprise, where each has a responsibility towards securing information.

3.2 The Capability Maturity Model Security Management Method

The Capability Maturity Model (CMM) methodology provides components used to protect information assets against unauthorized access, modification or destruction. The method is based on a holistic view of information security and it encompasses seven main components, as follows:

- Security leadership by means of an executive level security representative and an information security strategy.
- A security programme with defined roles and responsibilities for information security tasks.
- Security policies, standards and guidelines that are used to direct information security tasks.
- Security management that constitutes day-to-day operations and monitors users and technology.
- User management that focuses on awareness of policies and manages user profiles.
- Information asset security that encompasses the technology aspects of information security.

Technology protection for the environment and continuity, which focuses both on business continuity and disaster recovery.

IV. RISK MANAGEMENT MAIN REQUIREMENTS

A thorough investigation of the main applied information security risk management approaches highlighted the need for a new comprehensive information security risk management framework that enables enterprises to address all aspects of information security risk management in an effective and efficient manner. Therefore, an information security risk management framework should consider the following main requirements:

- Incorporate the basic elements of the risk management methodologies.
- Possess a comprehensive scope in that not only limit the analysis of the information security risk management on the technical issues, but also include organisation, people and environment issues as well.
- Depend on a management process that integrates the main approaches for information security risk management and incorporates the essential components of the risk management methodologies.
- Assess numerically the current situation enterprise information security using valid and reliable modelling technique.
- Base the selection of the recommended ISO/IEC 27002 security protection measures on an economical analysis.

In addition to the previous main requirements, a well defined information security policy, a trained supporting team from inside enterprises and a clear identification of risk management terms and concepts play a crucial role in successfully developing an effective information security risk management framework.

V. CONCLUSION

The conclusion from reviewing the key enterprise information security risk management standard, professional and researchers methods is that they provide different tools and techniques for reaching generally the same goal of protecting enterprises information resources by defining suited security protection measures with the help of a risk management approaches. However, these methods achieve this goal by different approaches: risk-analysis approach and best-practice approach, and have different levels: some methods are high-level just for providing guidelines, while others are more detailed and concentrate mainly on achieving better risk analysis results. Most of the available risk management methods have technical nature and ignore the assessment of the current state enterprise information security. In addition, these methods are not depending on standard economical approach in selecting the relevant security protection measures. Each method has its own strengths and weaknesses, and it is believed that integrating these methods in a reference comprehensive enterprise information security risk management framework will achieve better results.

REFERENCES

[1]. Katina Michael “Security Risk Management: Building an Information Security Risk Management Program from the Ground Up” Computers & Security,Volume 31, Issue 2, Mar2012, pp 249–250.

[2]. Tony Jeffreek “A review of OSI management standards” Computer Networks and ISDN Systems, Volume 16, Issues 1–2, September 1988, pp 167–174

[3]. Chunlin Liu., Chong-Kuan Tan., Yea-Saen Fang., Tat-Seng Lok “The Security Risk Assessment Methodology” Procedia Engineering, Volume 43, 2012, pp 600–609.

[4]. Serap Atay & Marcelo Masera “Challenges for the security analysis of Next Generation Networks” Information Security Technical Report, Vol.16, Issue 1, 2011, pp 3–11.

[5]. Shuzhen Wang., Zonghua Zhang., Youki Kadobayashi “Exploring attack graph for cost-benefit security hardening: A probabilistic approach” Computers & Security, Volume 32, February 2013, pp 158–169.

[6]. Romain Jallon., Daniel Imbeau., Nathalie de Marcellis-Warin “Development of an indirect-cost calculation model suitable for workplace use” Journal of Safety Research, Volume 42, Issue 3, June 2011, pp 149–164.

[7]. Pullen Troy., Maguire Heather "The information management risk construct: identifying the potential impact of information quality on corporate risk" International Journal of Information Quality, Vol. 1 (4), 2007, pp. 412-443.
[8]. Feng-Ming Tsai., Chi-Ming Huang "Cost-Benefit Analysis of Implementing RFID System in Port of Kaohsiung" Procedia- Social and Behavioral Sciences, Volume 57, October 2012, pp 40 -46.
[9]. Daniel Mellado., Eduardo Fernández-Medina., Mario Piattini "A common criteria based security requirements engineering process for the development of secure information systems" Computer Standards & Interfaces, Volume 29, Issue 2, February 2007, pp 244–253
[10]. Shaun Posthumus., Rossouw von Solms "A framework for the governance of information security" Computers & Security, Volume 23, Issue 8, December 2004, pp 638–646.

Mr. KIRAN KUMAR KOMMINENI Pursuing Ph.D in Computer Science & Engineering from Monad University, Pilakhwa, Dist. Hapur(U.P), India. Received Master of Engineering in Computer Science & Engineering from RMK Engineering College, Chennai affiliated to Anna University. Presently working as an Assistant Professor in Information Technology Department of Bapatla Engineering College, Bapatla, Guntur (Dt), AP

Dr. ADIMULAM YESU BABU received Ph.D in Computer Science & Systems Engineering from Andhra University, Visakhapatnam. Dr. Babu having 23 years of Academic & Academic Administration experience and presently working as a I/c Principal and Professor in Computer Science & Engineering, Sir. CR Reddy College of Engineering, Eluru -534007, West Godavari (Dt), AP.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)