Enterprise Information Security Risk Management

K. Srujan Raju and M. Varaprasad Rao
Dept of CSE, CMR Technical Campus, Hyderabad - 501401

This paper presents the current approaches for enterprise information security risk management. These approaches are studied to identify basic elements, essential components and main steps of each one of them. A compiled list of high level requirements is identified from the investigated approaches that could be used as a base for the development of the target reference comprehensive enterprise information security risk management. Based on these requirements, a suitable framework for enterprise information security risk management will be developed.

KEYWORDS: Information Security, Risk Management, Enterprise

1. Introduction

An enterprise is a complex system of cultural, process and technology components engineered together to accomplish organisational goals. An enterprise is "any entity engaged in an economic activity, irrespective of its legal form". An enterprise is a complex system of people and technology organized together and working in a specific environment to achieve the strategic goals of the business. In fact, information is now becoming the lifeblood of any enterprise, and it has become the most valuable asset to any enterprise.

Information Security approaches deal with protecting and mitigating threats to the information assets and technical resources available within computer based systems. Information security is defined as "preservation of confidentiality, integrity and availability of information". The modern information security definition extends the previous definition to include authentication and non-repudiation, but they are not included in the ISO standard definitions till now, and throughout this thesis the standard ISO definitions will be used. Confidentiality of information is "the property that information is not made available or disclosed to unauthorised individuals, entities or processes". Integrity is "the property of safeguarding the accuracy and completeness of asset". Availability is "the property of being accessible and usable upon demand by an authorized entity". Information security requirements are concerned with the amount and specifics of security required for effective protection of the information resources.

From the above definitions one can conclude that the aim of enterprise information security is to achieve the protection of the enterprises" information and information systems from unauthorized access, use, disclosure, modification, disruption or destruction of information and information resources whether accidental or deliberate.

2. Literature Review

So many workers proposed different approaches for enterprise information security risk management, some of them are Katina Michael [1] reported the security risk management by building an information security risk management program from the Ground Up. Tony Jeffreek [2] presented the provision of management facilities within large networks based on the use of OSI protocols to ensure the long-term success of OSI as a vehicle for global communication. Gang Ma and Liping Sun [3] studied the main target of FPSO assets management is to control risk of operation, assure security of production, maintain integrity of equipment, collect assets information, assure capital operation, arrange human resources and logistics. Mohamed S. Saleh., Abdulkader, A [4] presented the comprehensive ISRM framework that enables the effective establishment of the target safe environment. Robert M. Gellman [5] reported the Securities and Exchange Commission's new EDGAR (Electronic Data Gathering, Analysis, and Retrieval) database of prospectuses, securities registration statements. Richard P. O'Neill et al [6] analysed the regulation of electric power and natural gas in the USA, its potential for enhancing or degrading efficiency in the gas industry. Ritu Agarwal et al [7] proposed a number of approaches that allow for the consideration of corporate goals and objectives in prioritizing information systems using both financial and non-financial criteria. Kenneth Baum et al [8] described a first generation, farm level recursive interactive programming model for analysing the impacts of commodity farm programs on typical farms (FLIPRIP). Guillermo A. Calvo., Enrique G. Mendoz [9] reported that globalization may promote contagion by weakening incentives for gathering costly information and by strengthening incentives for imitating arbitrary market portfolios. Pullen Troy., Maguire Heather [10] proposed that the management of organizational records, irrespective of format needs to be considered a component of information quality. Mohamed S. Saleh.,

Abdulkader Alfantookh [11] presented a comprehensive ISRM framework that enables the effective establishment of the target safe environment. Robert E. Crossler et al [12] proposed the future highlighted directions for data collection and measurement issues in behavioural Information Security research.

3. Risks to Information Security

The definition of risk varies based on different businesses and environments. Within information security context, risk is defined by ISO as "the combination of the probability of an event and its consequence". Threat is "a potential cause of an incident that may result in harm to a system or organization". Threat is defined also as "any person or object that presents danger to an asset". Depending on this, risks to information security can result from processes of modification, destruction, fabrication, disclosure, interruption, denial of service and theft of hardware, software or data. In order to manage these risks effectively, each enterprise must run a regular and effective risk management exercise to understand the nature of these risks.

4. Importance of Risk Management

The importance of managing information security risks continues to grow worldwide, as a result of the increasing breaches that affect the protection of information resources and consequently the business activities. The lack of properly implemented security measures to mitigate the rising information security risks has been reflected in recommendations by the governments and industry requirements for enterprises in running regular and effective risk management programs. One of the main responsibilities of agencies under the FISMA (Federal Information Security Management Act) of the USA is to perform a regular risk assessment exercise (FISMA 2002). The enterprises are potentially losing profit as a result of the absence of effective information security risk management programs that proactively share in the protection of the enterprises" information resources. Therefore, enterprises are required to acquire and run effective information security risk management program to not only achieve better protection of their information resources and consequently reduce the financial losses, but also to comply with the governmental laws and mandatory regulations which was applied in their environments.

5. Existing Risk Management Approaches

Today, there are various information technology and information security risk management methodologies; each of these methods has a different view and steps for identifying, analysing, evaluating, controlling and monitoring risks to information systems and information security. The risk-analysis approach for EISRM is concerned with the systematic in depth identification and valuation of assets, the assessment of threats to those assets, the assessment of vulnerabilities and the use of different risk analysis techniques to calculate the value of risk. The results from these activities are then used to assess the identified risks and to recommend justified protection measures. The main characteristics of this approach are accurate results, appropriate identification of protection measures and detailed documentations that could be used in the management of security changes. Examples of methodologies under this approach include CRAMM, CORAS, EBIOS and OCTAVE (CRAMM 2001; CORAS 2003; EBIOS 2004; OCTAVE 2005).

On the other hand, the best practice approach for enterprise information security risk management was developed to solve the major practical problems which appeared with the application of risk analysis based methodologies. The main idea behind this approach is to use the best practice documents to standardize the security controls and to achieve a fast basic level of security inside the concerned enterprises. This approach utilizes the checklist technique to achieve its objectives, and it depends mainly on the compliance and certification processes to examine the existence of the required protection controls according to a specific standard. The main goal of this paper is to show that combining these two approaches in an integrated comprehensive enterprise information security risk management framework shall benefit the information security risk management results.

5.1 The Risk-Analysis Approach

The enterprise information security risk-analysis approach has many different methods; these methods are standard, professional and research methodologies. Selective key methods from each group will be discussed in terms of their objectives, structure, content, basic elements, essential components, steps and their ability to integrate technological, organizational, human and environmental components in studying enterprises" information security risks. The technological view in dealing with information security risk management is not sufficient for the development of comprehensive EISRM framework. Organization, people and environment issues should also be addressed in the framework to ensure that it is comprehensive. These methods are selected because they are issued by well-known national and international standard organizations used internationally and often referenced in other methods.

5.1.1 Standard Risk Management Methods

National and International standard organizations suggested a number of risk management methods.

AS/NZS 4360

It is considered one of the first risk management standards to define a complete risk management method. The standard is very generic and independent of any industry or economic structure. The AS/NZS 4360 defines risk management process as the total process of identifying, controlling and eliminating or minimizing uncertain events that may affect IT system resources, which are often best carried out by a multi-disciplinary team. The AS/NZS 4360 standard includes five main steps and defines two parallel processes. Table 1 summarizes the issues considered by each step and process.

■

Table 1: The generic risk management steps & process of AS/NZS 4360

S. No.	Steps	Issues Considered
1	Establish the context: Define the basic parameters & set the scope for the rest of risk management process	1) External environment: Business, social, regulatory, cultural, competition, financial, political / Stakeholders & key business drivers /Organization's: strengths, weaknesses, opportunities, threats. 2) Internal environment: Stakeholders/Organization's: strategy, goals, structure, resources (people, system, processes, capital), decision making 3) Risk management: The depth and breadth of the needed risk management activities. 4) Risk criteria: Risk evaluation issues: environmental, legal, financial, social, humanitarian, operational, technical. 5) Analysis: Define the structure of the analysis.
2	Identify risks	What can happen, when and where, why and how: events that could prevent, degrade or delay the achievement of objectives.
3	Analyze risks	Existing risk controls / Likelihood of occurrence of identified risks and their potential consequences / Levels of risks.
4	Evaluate risks	Levels of risk versus risk criteria considering risk treatment: balancing adverse outcomes with potential benefits of treatment, setting priorities and making decisions.
5	Treat risks	Specific cost-effective strategies and action plans for risk treatment: development and implementation (options, treatment, residual risk).

The parallel process

S. No.	Steps	Issues Considered
1	Communicate and consult	Plan / Consultative team / Stakeholders perceptions of risk / Understanding the basis of decision.
2	Monitor & review	The effectiveness of all steps for continuous improvement.

ISO/IEC TR 13335-3

It is the third part of five series technical reports, which adopts a more holistic approach for enterprises information security management. This technical report provides guidance on the management of IT security presenting a foundation to assist enterprises in developing and enhancing their internal security architecture, and to establish commonality between enterprises. The document also provides guidance on the selection and use of safeguards which addresses the vulnerabilities of a particular network and its associated security risks. The IT security risk management method of ISO/IEC 13335-3 has five basic steps. Table 2 presents the issues associated with each of these steps.

Table 2: IT risk management steps & process of ISO/IEC TR 13335-3

S. No.	Steps	Issues Considered
1	Risk analysis	1) Boundaries: Technology & information / People: staff, subcontractors & others / Environment: building facilities / Activities: operations. 2) Threats & vulnerabilities: Identifying both: accidental and deliberate risk sources / Assessing the likelihood of the occurrence of risk / Identifying weaknesses in: technology, people, physical environment, activities & procedures. 3) Safeguards: Identifying existing and planned safeguards. 4) Risks: Assessing the risks to which assets are exposed.
2	Safeguards selection	Constrains / Security architecture / Risk acceptance & residual risk
3	Policy & plan	Policy: Why selected safeguards are necessary. Plan: How safeguards can be implemented.
4	Plan implementation	Practical implementation of safeguards according to plan / Awareness & training / Approval of plan.
5	Treat risks	Maintenance / Checking compliance / Monitoring / Incident handling / Change management.

5.1.2 Professional Risk Management Methods

Professional organizations also suggest a number of risk management methods from four which are presented in the following.

CRAMM

CRAMM (CCTA Risk Analysis and Management Method) is a qualitative risk analysis and management method developed by the UK government's central computer telecommunication agency. The method had undergone major revisions and is finally being distributed by a private company. CRAMM method has three main steps and shown in Fig.1.

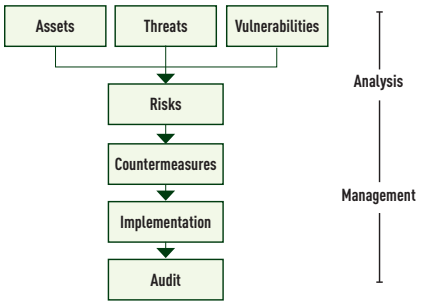

Fig. 1 : CRAMM risk management process

One of the main features of CRAMM is the identification of the IT assets. The information is gathered through interviewing the owners of the assets, the users of the system, the technical support staff and the security manager. The method neither helps in the calculation of return on investment for the proposed controls nor helps in the monitoring the effectiveness of these controls. CRAMM does not assist in risk management improvement inside the considered enterprises, so no training, meetings or workshops are utilised. No steps in CRAMM are concerned with implementation and follow-up.

OCTAVE

The Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE) method was developed at the Computer Emergency Response Team Coordination Center. The method is considered as human centric qualitative risk analysis methodology. The main objective of this method is to examine enterprises' organizational and technological issues for developing a comprehensive picture for information security needs. The method produced by OCTAVE has the following three main phases as shown in Fig. 2.

The method collects the required information at phase one through two workshops; the first with the senior management to define the scope of the analysis, while the second with the staff that has more technical expertise. One of the main concepts of OCTAVE is self-direction. This concept means that people from various hierarchical levels of the enterprise are responsible to lead the information security risk evaluation program.

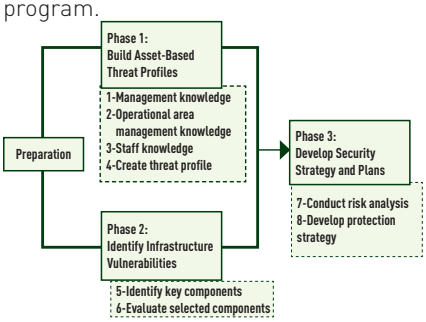

Fig. 2 : OCTAVE risk management process

CORAS

The CORAS (Consultative Objective Risk Analysis System) project was developed and aims at addressing security-critical systems in general, but places particular emphasis on IT security.

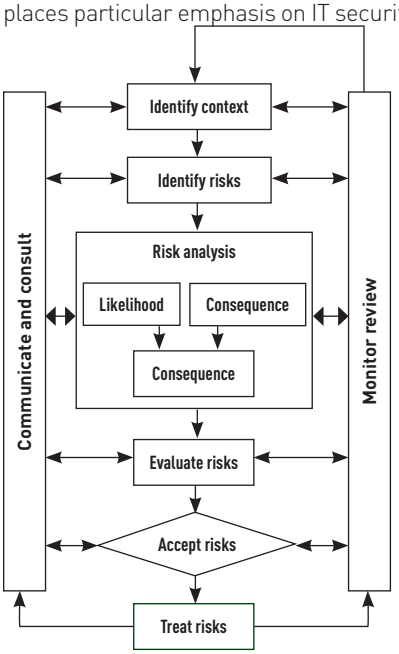

Fig. 3 : CORAS risk management process

The main objective of CORAS is to improve the traditional risk assessment methodologies to get better results by gathering well-known risk analysis techniques into an integrated security risk analysis method. The CORAS method considers a broad view to security that includes not only the technological aspects, but also the human interactions with technology and all relevant issues of the surrounding organization and environment. The CORAS risk management process, as shown in Figure 3, adopts the risk assessment process of the AS/NZS 4360 risk management standard. The CORAS 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. The method has a scientific origin and depends on its own terminology for risk management process, which is considered as one of its main weaknesses. In addition, the method adopts the risk management process of the AS/NZS 4360 standard which is a generic risk management process and is not dedicated for information security.

6. Conclusions

The conclusion from the above is 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. Most of the available risk management methods have technical nature and ignore the assessment of the current state enterprise information security. 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.

7. 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] Gang Ma and Liping Sun "The Design and Implement of FPSO Assets Management System" Procedia Environmental Sciences, Volume 12, Part A, 2012, pp 484–490

[4] Mohamed S. Saleh., Abdulkader Alfantookh "A new comprehensive framework for enterprise information security risk management" Applied Computing and Informatics, Volume 9, Issue 2, July 2011, pp 107–118

[5] Robert M. Gellman "Authorizing EDGAR: Information policy in theory and practice" Government Information Quarterly, Volume 5, Issue 3, 1988, pp 199–211

[6] Richard P. O'Neill., Charles S. Whitmore., Gary J. Mahrenholz "A comparison of electricity and natural gas markets and regulation in the USA" Utilities Policy, Volume 2, Issue 3, July 1992, pp 204–227

[7] Ritu Agarwal., Linda Roberge., Mohan R. Tanniru "MIS planning: A methodology for systems prioritization" Information & Management, Volume 27, Issue 5, November 1994, pp 261–274

[8] Kenneth Baum., James Richardson., Lyle Schertz "A stochastic recursive interactive programming model for farm firm policy analysis" Computers & Operations Research, Vol. 11, Iss2, 1984, pp 199–222

[9] Guillermo A. Calvo., Enrique G. Mendoz "Rational contagion and the globalization of securities markets" Journal of International Economics, Volume 51, Issue 1, June 2000, pp 79–113

[10] 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.

[11] Mohamed S. Saleh., Abdulkader Alfantookh "A new comprehensive framework for enterprise information security risk management" Applied Computing and Informatics, Volume 9, Issue 2, July 2011, pp 107–118

[12] Robert E. Crossler., Allen C. Johnston., Paul Benjamin Lowry., Qing Hu., Merrill Warkentin., Richard Baskerville "Future directions for behavioural information security research" Computers & Security, Volume 32, February 2013, pp 90–101

■

About the Authors

Dr. K. Srujan Raju is the Professor and Head, Department of CSE, CMR Technical Campus, Hyderabad, India. Prof. Raju earned his PhD in the field of network security and his current research includes computer networks, information security, data mining, image processing, intrusion detection and cognitive radio networks. He has published several papers in refereed international conferences and peer reviewed journals and also he was in the editorial board of CSI 2014 Springer AISC series; 337 and 338 volumes. In addition to this, he has served as reviewer for many indexed journals. Prof. Raju is also awarded with Significant Contributor, Active Member Awards by Computer Society of India (CSI) and Past Secretary of CSI Hyderabad Chapter.

Dr. M Varaprasad Rao obtained Doctorate in CSE from SVU. He has 17 years of teaching experience. He worked for various capacities in various institutions. He has published 16 papers in reputed/peer reviewed indexed international journals. He also contributed 3 book chapters for IGI global publications. He is an editorial/reviewer member of Springer journal: IJU and IJMPICT. He is a life member of UNI-IT, CSI, ISTE, IAEng.