A Comparative Study on Information Security Risk Analysis Practices

Neeta Shukla
Deptt. of Computer Sc. & Engg., Mewar University, Chittorgarh, India

Sachin Kumar
Deptt. Of IT, Ajay Kumar Garg Engineering College, Ghaziabad, India

ABSTRACT

Information is a key asset for organizations, and reducing the risk of information compromise is a high priority. There are a lot of risk analysis methods available today, some of which are qualitative while others are more quantitative in nature. They all have the same fundamental target to estimate the overall value of risk, but most attempts to hit the target from very different approaches. Some approaches can be applied to all types of risk, while others are specific to particular risks. This work addresses some of the methodologies used currently to analyze information security risks. The main task for an organization is to determine which one to use. Since the organization will spend money on whichever method they choose, it is vital that the chosen methodology meet the requirements. The purpose of the study is to compare and clarify the different activities, inputs, and outputs required by each model of information security risk assessment and the analysis that effectively addresses the risks of information security.

Keywords-component; : information security; risk analysis; risk assessment; risk analysis models; risk analysis method; risk analysis comparison; information security risk analysis methods.

1. INTRODUCTION

Information security is often conceptualized as being the protection or preservation of four key aspects of information: availability, integrity, authenticity, and confidentiality. [4]

Availability: Accessibility of information for a purpose.

Integrity: Completeness, wholeness, and readability of information, and the quality of being unchanged from a baseline state.

Authenticity: Validity, conformance, and genuineness of information.

Confidentiality: Limited observation and disclosure of knowledge to only authorized individuals.

Using computer systems and networks and capitalizing on weaknesses in equipment and human operators, malefactors are able to strike at information assets with a whole host of attacks. The information technologies are a powerful set of enabling technologies. They confer upon their users an unprecedented capability for managing, processing, and communicating information. Securing these technologies and the information that they steward is a difficult and often expensive venture. In addition to the direct costs of planning, designing, and implementing safeguards, computer security also requires the participation of everyone in the organization but limits their freedom to use the technology to its fullest extent.

2. PROBLEM DEFINITION

A. *Risk Analysis*

The purpose of any risk analysis is providing decision-makers with the best possible information about the probability of loss. As a result, it is important that decision-makers accept the risk analysis method used, and that information resulting from the analysis should be in a useful form. There are several different approaches to risk analysis, but they can be broken down into two essential types: quantitative and qualitative.

❖ Quantitative Risk Analysis

This approach uses two basic elements: the probability of an event occurring and the losses that may be incurred.

Quantitative risk analysis uses one number produced from these elements. This is called the Expected Annual Loss (ALE) or Estimated Annual Cost (EAC). This is calculated for an event by simply multiplying by the probability of potential losses. Therefore, in theory, one may rank events in order of risk (ALE) and make decisions based on that risk.

❖ Qualitative Risk Analysis

The qualitative method rates the magnitude of the potential impact of a threat as high, medium, or low. Qualitative methods are the most common measures of the impact of risks. This method allows covered entities to assess all potential impacts, whether they are touchable or untouchable. The qualitative risk analysis methodology uses several elements such as threats, vulnerabilities and controls that are all interconnected.

Risk analysis includes processes such as the identification of activities, threat analysis, vulnerability analysis and guarantees. Risk analysis processes such as BS7799, GMIT, and CSE and explain the procedure to define the modalities for implementation.

There are several methods used for analysis: a matched comparison of dependency diagrams, asset-function assignment tables, and activities. Other models for the design of information security focus on the identification and assessment of the vulnerability of the system and the specification of counters to those vulnerabilities [7].

B. *Risk Assessment*

Risk assessment is the process of identifying, characterizing, and understanding risk; that is, studying, analyzing, and describing the set of outcomes and likelihoods for a given endeavor. These methodologies centered on fault/event trees that were used to illustrate and to capture all possible plant failure modes in a graphical representation.

C. *Risk Management*

Risk management is a policy process wherein alternative strategies for dealing with risk are weighed and decisions about acceptable risks are made. The strategies consist of policy options that have varying effects on risk, including the reduction, removal, or reallocation of risk. In the end, an acceptable level of risk is determined and a strategy for achieving that level of risk is adopted. Cost-benefit calculations, assessments of risk tolerance, and quantification of preferences are often involved in this decision-making process.

A formal risk framework can be a useful tool for decomposing the problem of risk management. In such a framework, risks are assessed by evaluating preferences, estimating consequences of undesirable events, predicting the likelihood of such events, and weighing the merits of different courses of action. In this context, risk is formally defined as a set of ordered pairs of outcomes (O) and their associated likelihoods (L) of occurrence.

$$Risk \equiv \{(L1, O1)\ldots(Li, Oi)\ldots(Ln, On)\}^{\wedge}3$$

3. COMMON FRAMEWORK

In 1979, the National Bureau of Standards published its Federal Information Processing Standard (FIPS) 65, *Guideline for Automatic Data Processing Risk Analysis*.4 The document set the risk assessment standard for large data-processing centers and also proposed a new metric for measuring computer-related risks: Annual Loss Expectancy (ALE).

$$ALE = \sum_{i=1}^{n} I(O_i)\mathrm{F_i}$$

where:

$\{O_1 ,......, O_n\}$	= Set of Harmful Outcomes
$I(O_i)$	= Impact of Outcome i in dollars
F_i	= Frequency of Outcome i

The metric's appeal rests in its combination of both risk components into a single number. Unfortunately, this blending of quantities has the disadvantage of being unable to distinguish between high-frequency, low-impact events and low-frequency, high-impact events. In many situations, the former may be tolerable while the latter may be catastrophic.

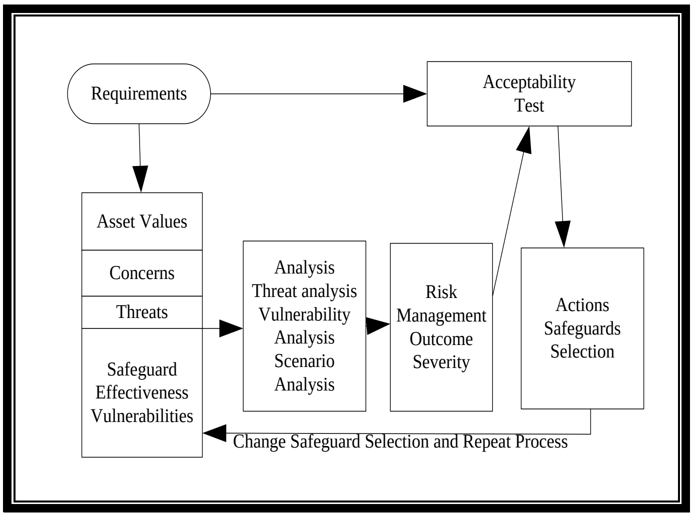
Requirements
Acceptability Test
Asset Values
Concerns
Threats
Safeguard Effectiveness Vulnerabilities
Analysis Threat analysis Vulnerability Analysis Scenario Analysis
Risk Management Outcome Severity
Actions Safeguards Selection
Change Safeguard Selection and Repeat Process

Figure 1: Common Framework Process Diagram

The framework had seven basic elements:

Requirements: **R** □□ [R1, R2, . . . , Rj]

e.g., expected loss < $100K, expected loss < $1M

Assets: **A** □□ [A1, A2, . . . , Ak]

e.g., hardware, software, data

Security Concerns: **C** □□ [C1, C2, . . . , Cs]

e.g., confidentiality, integrity, authenticity

Threats: **T** □□ [T1, T2, . . . , Tm]

e.g., human, natural

Safeguards: **S** □□ [S1, S2, . . . , Sp]

e.g., physical, system, communication, admin.

Vulnerabilities **V** □□[V1, V2, . . . , Vq]

e.g., physical, software, hardware, administrative

Outcomes: **O** □□[O1, O2, . . . , Or]

e.g., combinations of A, C, T, S, V

The framework also included three associated quantities:

Asset Values: **Aval** □□[A1val, A2val, . . . , Akval]

Safeguard Effectiveness: **Seff** □□[S1eff, S2eff, . . . , Speff]

Outcome Severity **Osev** □□[O1sev, O2sev, . . . , Orsev]

e.g., ALE of the outcome, qualitative judgment

The framework called for an assessment of the above quantities in an iterative process as diagrammed in Figure 1. First, identification of security requirements, assets for consideration, security concerns, possible threats, vulnerabilities, and safeguards takes place. Next, a series of analyses ensues.

The threat analysis involves an examination of possible threats to each asset. The threats might include human actors, natural catastrophes, unintentional errors, etc. The vulnerability analysis looks at the weaknesses in security that might enable a successful attack against the assets. The scenario analysis requires a detailed evaluation of assets, security concerns, threats, and vulnerabilities to generate all possible scenarios whereby security compromises could occur. The acceptability test compares the risk measured for a given asset with the established requirements. Safeguard selection decisions are then made to close the gap between the required and measured risk levels. The entire process is then repeated under the new safeguard regime, resulting in a new risk measurement for each asset. These risk measurements along with assessments of safeguard costs are then used to generate cost-benefit analyses for each safeguard.

4. COMPARING INFORMATION SECURITY RISK ANALYSIS METHODOLOGIES

As stated earlier there are two fundamental types of risk assessment. Quantitative risk analysis applies mathematical and statistical tools to represent risk.

Qualitative risk analysis methods perform risk analysis with the help of adjectives, not mathematics.

The common framework was quite generic in its specification and therefore broad in its potential application. The methodology can be adapted to either qualitative or quantitative risk assessment. The scenario analysis and subsequent risk-measurement activity are specifically well-suited to qualitative assessment. In a quantitative risk assessment, both tasks could be automated calculations, based on asset values, frequency of vulnerability exploitation, and probability of successful attack.

Despite the best efforts of those involved, the common framework and other ALE-based approaches are not suitable for intensive analysis of today's information security risks. Unlike the past decade, information systems today have a complicated structure and are heavily used.

The qualitative approach does not utilize any mathematical tools or statistics for the risk model, so therefore the outputs of the remote method depend on the ideas of those who undertake risk analysis. There can be a subjective decision about risk when the risk was analyzed with a qualitative method [6].

Comparison frameworks use criteria that focuses on information technology, information security and a complete approach to risk, such as that proposed by Badenhorst et al. (1993). The framework proposed by Badenhorst et al. indicates whether or not a method meets a criterion. It does not use ladders, or trade-offs that can help the organization in choosing a methodology that will best meet their needs. This shows the need for more superior comparatives.

A comparison of different methodologies is made. Each time a methodology is mentioned by an author, they receive a check mark and one point. OCTAVE ranks the first on a score of 11 points out of 14, followed by CRAMM which scores a 7. CORAS which scores a 6, and then is followed by ISRAM, CORA, and IS.

A comparison is made by analyzing mutual aspects of the different methodologies. For this reason a brief overview is given of each.

- OCTAVE

OCTAVE was developed at the CERT Coordination Center by Carnegie Mellon Software Engineering Institute. It is a technique for performing risk analysis. It considers both technological and organizational issues. Octave looks at the daily usage of organization’s computing infrastructure [14]. This approach focuses on activities, threats, and vulnerabilities. One of the main concepts of OCTAVE is self-direction. This means that people within the organization must practice information security risk assessment [10].

The OCTAVE methodology uses an Expected Value Matrix to determine a risk's expected value. The impact values and probability values are subjective and are then applied mostly to the Expected Value Matrix to get an overall value. The main formula is:

Loss = Impact/consequence x Probability

OCTAVE implements no mathematical computations and thus it catches a value of 3 for simplicity and a value of 1 for precision. If an organization is concerned with simplicity rather than accuracy, OCTAVE is a good fit [5].

- CORAS

CORAS [12] was developed using information society technologies (IST). One of the main objectives of CORAS is to develop a structure that uses the methods of risk analysis, semi-formal methods for object-oriented modelling, and computer tools for an accurate and unambiguous assessment of risk, and efficient critical safety systems [14]. The methodology is based on Unified Modelling Language (UML), a language that uses diagrams to illustrate relationships and dependencies between users and the environment in which they work.

The framework has four main pillars, of which risk management is one. In CORAS, the decisions made can be based on UML class diagrams of each asset [17, 18, 25,].

Loss = Impact x Probability

CORAS applies no mathematical computations, consequently it obtains a value of 3 for simplicity and a value of 1 for precision. The CORAS method also employs the impact and probability method [5].

- CRAMM

The CCTA Risk Analysis and Management Method (CRAMM) is a qualitative risk analysis and management tool developed by the UK Government Central Computer and Telecommunications Agency in 1985 to provide government departments with a method for revisions to the security of information systems. CRAMM can be used for all types of organizations.

Demonstrating acquiescence with BS7799 (British standard for information management) during a certification process. It can also be regarded as a benchmark for organizational risk and emergency management considering input from a number of public and private sector experts in the security instrument.

The crucial essentials of data collection, analysis and output results that should be present in a programmed risk analysis tool are covered in the three stages of a CRAMM review:

Recognizing and valuing assets.

Recognizing threats and vulnerabilities, computing risks.

Recognizing and prioritizing countermeasures.

CRAMM computes risk for each group of assets versus the threats to which it is vulnerable on a scale of 1 to 7 utilizing a risk matrix with the default values by comparing it with the activity level of threat and vulnerability. On this scale, 1 implies a fundamental requirement of safety and 7 shows a very high safety requirement [28].

- ISRAM

ISRAM was improved in December 2003 at the CNR Institute of Electronics and Cryptology and Gebze Institute of Technology in Turkey. It was marketed as a quantitative approach to risk analysis, which allows the participation of the Director and staff of the organization. ISRAM is poll-based model. Two separate and independent investigations are established for the two attributes of risk, whose names are probability and consequence. ISRAM does not implement techniques such as single occurrence losses (SOL) or annual loss expectancy (ALE). However, the risk factor is a number between 1 and 25. This numerical value keeps in touch with a high, average or low qualitative assessment, and this quality value is based on risk management decisions. The ISRAM methodology has seven steps [6].

The original risk model of ISRAM is based on the below formula [6]:

Risk = Probability of SB . Consequence of SB where SB means the occurrence of security breach. The risk model of ISRAM, which is realized from a formula, consists of two main parts, which are the projections of two basic parameters in a formula:

$$Risk = \left(\frac{\sum_m T1\left(\sum_i wipi \right)}{m} \right) \left(\frac{\sum_n T2\left(\sum_j wjpj \right)}{n} \right)$$

In this equation, i is the number of questions for the survey of probability of occurrence. j is the number of applications for the detection of the consequences of occurrence. m is the number of participants who participated in the survey about possibilities of occurrence. n is the number of participants who participated in the survey of consequences of occurrence. wi and wj are the weight of questions i and j. pi and pj are the numerical values of the selected answer choice for question I and j. T1 is the table risk of the investigation of probability of occurrence. And finally, T2 is the table of risk for the study of the consequences of an occurrence.

If an organization is interested in simplicity, ISRAM is not the proper choice. But it does accurately evaluate the security risks in an organization. Two processes of separate and independent surveys were conducted for two risk parameters in the formula. The preparation and flow of the survey is done in steps to produce well-defined risks [29].

- CORA

International Security Technology, Inc. (ICT) has developed Cora, a system for estimating and analyzing the cost of risk.

Cora risks using data collected on the threat, functions, and assets, and weaknesses of the functions and assets to the threats to calculate the consequences. That is, the losses due to incidents of threats. It is a method in which the parameters specified in quantitative risks and where the loss is expressed in terms of quantitative finance. Cora uses a two-step process to support risk management. The parameters of the threat, the functions and assets, are verified and refined until the best values are determined. Cora then calculates SOL and ALE for each identified threat. The total losses to the organization are evaluated for each threat, and then this value is multiplied by the frequency of threats. [30]. CORA employs the following:

ALE = Consequence x Frequency

where the result equals Sn(individual SOLs) n the number of SOLs, and SOL = loss potential (worst case monetary value) x vulnerability. Cora utilizes some mathematical computations, but they are not extensive. It earns a value of 2 for both simplicity and accuracy [5].

- IS Risk Analysis Based on a Business Model

Based on a business model, IS Risk Analysis has been developed at the Korea Advanced Institute of Science and Technology (KAIST) in 2002. They developed this model owing to some limitations of traditional risk analysis methodologies. An asset's value is taken by this model and then not only supports the analysis on its replacement cost, but also its tangible asset's value from the viewpoint of the operational continuity measured. The methodology is comprised of four stages. By this method, the significance of various business functions of the business model and the necessity of various IS assets are determined. Mathematical formulae are applied to compute ALE for a single threat occurrence of the organization. The end result is a quantitative monetary value [7].

IS Risk Analysis Based on a Business Model uses the following:

$$ALEij = (RCij + ILij)XPj$$
$$Where: ILij = AIi \times I / BD \times RTij$$
$$AIi = \sum\nolimits_{alli} (FIi \times Nij)$$

Extensive mathematical calculations are employed in the IS model. It is awarded a value of 1 for simplicity and a 3 for precision [5].

5. THE FRAMEWORK FOR COMPARISON

Table 1 shows the framework based on the six methodologies was evaluated during this research and values of each criteria.

Table 1: A Framework For The Comparison Of Risk Analysis Methodologies

CRITERIA	QUALITATIVE			QUANTITATIVE		
	OCTAVE	CORAS	CRAMM	ISRAM	CORA	IS
Method/Tools	Method/Tools	Tools	Method/Tools	Method/Tools	Tools	Method/Tools
Method/Tool Name	OCTAVEv2.0 OCTAVE – S v1.0	CORAS Editor v.1.1	CCTA Risk Analysis and Management Method	ISRAM	CORA 5.0	IS Risk Analysisbased on a Business Model
Vendor Name	Carnegie Mellon University, SEI(Software Engineering Institute)	European Commission	Insight Consulting	National Research Institute of Electronics and Cryptology and the Gebze Institute of Technology	International Security Technology, Inc	Korea Advanced Institute of science and Technology

Country of Origin	USA	Intracom(Greece)
		Solinet(Germany)
		Telenor(Norway)
			United Kingdom	Turkey	New York	Seoul, Korea

Date of First Release	Version 0.9 1999	January 2001	1985	December 2003	1978	2002
Languages	English	English	English, Dutch, Czech	English	English	English
Price	Free	Free	Unknown	Free	$ 7000- $85000	Free
Compliance to IT Standards	N/A	ISO 31000 ISO/IEC17799 AS/NZS 4360	ISO/IEC17799	NIST SP 800-30 ISO/IEC17799 ISO/IEC13335	N/A	N/a
Skills Needed	Standard	Standard	Specialist	Standard	Standard	Standard
Availibility	Trial version available, registration required	Trial version available, registration required	Registration required	Open	Licensing organisation without limit	Open
Tools Supporting the Method	Commercial Tools - Licensed materials - Trainings	An XML Mark-up for exchange of risk assessment data -A UML based specification language targeting security risk assessment	Commercial Tools -CRAMM Expert (Insight) -CRAMM Express(Insight)	Key Risk Management Tools for Information	N/A	N/A

6. CONCLUSION

At the moment, copious methodologies exist and many organizations are confronted with the frightening task of choosing one. The framework was developed with the aim of analyzing six methodologies in detail and recognizing some common criteria.

With the aid of providing such a framework, the procedure of picking a choice of a methodology can become easier and more prompt. The chief profit is involved in the ability to remove the majority of methodologies that are inappropriate and to only further investigate the few that remain. Information security risk analysis methodologies expand in an effort to differentiate themselves from competitors. Organizations are then presented with more choices but it becomes the proverbial double-edged sword, in that more choice brings more complexity in choosing. It is essential to keep remembering that the methodology chosen should hold up to all information security requirements and that it should fit into existing corporate and IT domination configurations.

7. REFERENCES

[1] K. P. Badenhorst, J. H. P. Eloff and L. Labuschagne, “A comparative framework for risk analysis methods,” Computers & Security, vol. 12, no. 6, pp. 597-603, 1993.

[2] Casualty Actuarial Society CAS, Overview of Enterprise Risk Management.

[3] A. Bayaga, Institutional risk management: analysis of factors associated with the extent of monitoring and reporting of Risk. The Journal of International Social Research, vol (3)10, pp. 77-89, October 2010.

[4] S. Lund, F. D. Braber, K. Stolen and F. Vraalsen, “A UML profile for the identification and analysis of security risks during structured brainstorming,” SINTEF Technical report STF40 A03067, 2004.

[5] A. Vorster and L. Labuschagne, “A framework for comparing different information security risk analysis methodologies,” University of Johannesburg, 2005.

[6] B. Karabacaka and I. Sogukpinar, “ISRAM: information security risk analysis method,” 2004.

[7] S. Goel and V. Chen, “Information security risk analysis – a matrix-based approach,” University at Albany, 2005.

[8] Z.Yazar, “A Qualitative Risk Analysis and Management Tool – CRAMM,” SANS Institute InfoSec Reading Room, 2011.

[9] N. Mayer, “Managing security IT risk: a goal-based requirements engineering approach,” in Proceedings of Doctoral Consortium in conjunction with the 13th IEEE International Requirements Engineering Conference, Aug. 2005.

[10] G. Bornman and L. Labuschagne, L, “A comparative framework for evaluating information security risk management methods,” in Proceedings of the Information Security South Africa Conference, 2004.

[11] B. Jung, I. Han, and S. Lee, “Security threats to Internet: a Korean multi-industry investigation,” Information & Management, Vol. 38,2001, pp.487–498.

[12] K. Stolen, F. D. Braber, S. Lund and J. Aagedal, “Model-based risk assessment – the CORAS approach,” 2002.

[13] S. Hariri, Q. Guangzhi, T. Dharmagadda, M. Ramkishore, and C. Raghavendra, “Impact analysis of faults and attacks in large-scale networks,” IEEE Security and Privacy, vol. 1 (5), pp. 49–54, September/ October 2003.

[14] R. Fredriksen, M. Kristiansen, B. A. Gran, K. Stølen, T. A. Opperud and T. Dimitrakos, “The CORAS framework for a model-based risk management process,” in Proceedings of the 21st International Conference on Computer Safety, Reliability and Security, 2002.

[15] NISER, Information Security Management System (ISMS) Survey, 2003.

[16] S. Hariri, Q. Guangzhi, T. Dharmagadda, M. Ramkishore, and C. Raghavendra, “Impact analysis of faults and attacks in large-scale networks,” IEEE Security and Privacy, vol. 1 (5), pp. 49–54, September/ October 2003.

[17] D. Raptis, T. Dimitrakos, A. Gran and K. Stolen, K, “The CORAS approach for model-based risk management”. Applied to Ecommerce Domain, 2002.

[18] A. Sunyaev, M. Hansen and H. Krcmar, “Method engineering: a formal description,” Technische Universität München.

[19] N. Mayer, “Managing security IT risk: a goal-based requirements engineering approach,” in Proceedings of Doctoral Consortium in conjunction with the 13th IEEE International Requirements Engineering Conference, Aug. 2005.

[20] J. M. Stanton, K. R. Stam, P. Mastrangelo, and J. Jolton, “Analysis of end user security behaviors,” Computers & Security, vol. 24, pp. 124–133, March 2005.

[21] Arthur Jung-Ting Chang and Quey-Jen Yehr, “Coping With Systems Threats: A Study of the Adequacy of Security in Taiwan,” IEEE International Conference on Management of Innovation and Technology, 2006 pp.689–693.

[22] S. Hariri, Q. Guangzhi, T. Dharmagadda, M. Ramkishore, and C. S. Raghavendra, “Impact analysis of faults and attacks in large–scale networks IEEE Security & privacy, pp. 49–54, 9 2003.

[23] R. V. Solms, "Information security management (2): guidelines to the management of information technology security (GMITS)," Information Management & Computer Security, vol. 6 (5), pp. 221-223, 1998

[24] M. T. Siponen, "A Conceptual Foundation for Organizational Information Security Awareness,"Information Management & Computer Security, vol.8, p. 31, 2000.

[25] J. Aagedal, F. Den Braber, and K. Stolen, “Model-based risk assessment to improve enterprise security”.

[26] J. Backhouse and G. Dhillon, “Structures of responsibility and security of information systems,” European Journal of Information Systems, vol. 5, no. 1, pp. 2-9, 1996.

[27] F. Vraalsen, F. D. Braber, I. Hogganvik and K. Stolen, “The CORAS tool-supported methodology for UML-based security analysis,” Sintef report, ISBN 82-14-0336, 2004.

[28] Z.Yazar, “A Qualitative Risk Analysis and Management Tool – CRAMM,” SANS Institute InfoSec Reading Room, 2011.

[29] D.Wawrzyniak, “Information security risk assessment model for risk management,” 2006.

[30] International Security Technology Inc (IST Inc), “A brief history of CORA,”.