Information Technology Risk Assessment Methodologies: Current Status and Future Directions

Monzer Moh'd Qasem

Abstract— The spread of information technology was the foundation that led to the construction and the design and use of information systems, which can be defined as the set of elements trained human elements necessary mechanism for the collection and operation of the data for the purpose of conversion to information that will help in the decision-making This system consists of input and conversion processes and outputs and is designed information system to disclosure of the information compiled and analyzed and prepared according to the needs of the various work centers institution or company and the information system works on the circulation of information and renewed on an almost daily basis and retrieved when needed, but there are a lot of threats and vulnerabilities in formation system and IT stuff should evaluate the relative risk for each of the vulnerabilities. This process is called risk assessment. Risk assessment is a process of evaluating the relative risk for each of the vulnerabilities in the information systems at the organizations. Because of there are a various information security risk assessment methods that can be implemented by the organizations and each has different approaches to assess the information security risks. Therefore organizations find it difficult to select an appropriate information security risk assessment method. Therefore, there is a need for a critical review of existing risk assessment methodologies to help IT staff to select the best risk assessment methodology based on the specific needs of the organization. This paper presents a comparative study between the top risk assessment methodologies like CORAS, COBRA, OCTAVE , CRAMM, NIST Guide , and SOMAP, along with its strengths and weakness.

Index Terms— Auditability, Authenticity, Comparative Study, Information Security, Risk Assessment, Risk management, vulnerabilities.

1 Introduction

Risk management is the process identifying risk, as represented by vulnerabilities, to an organization's information assets and infrastructure, and taking steps to reduce this risk to an acceptable level which involves three major undertakings: (i) Risk identification, (ii)Risk assessment and (iii)Risk control. Risk identification is the examination and documentation of the security posture of an organization's information technology and the risks it faces. Risk assessment is the determination of the extent to which the organization's information assets are exposed or at risk. Risk control is the application of controls to reduce the risks to an organization's data and information systems. The purpose of this paper is to allow the following to be performed:

[1] Determination of the most appropriate risk assessment methodologies for use by organizations in a range of given circumstances; such as their business sector, size, culture, legal, regulatory and governance requirements.
[2] Discussing the Strengths and Weaknesses' of each methodology.
[3] Direct comparison between risk assessment methodologies in order to permit expert advice to be given on their suitability for use in particular circumstances.

Dr. Monzer Qasem, Assistant Professor, Computer Information Systems Department, College of Computer & Information Sciences, Princess Nora Bint Abdul Rahman University, Al-Riyadh-Kingdom of Saudia Arabiai.
Qmonzer2000@yahoo.com - Mmqaseem@pnu.edu.sa

2 A Survey of Existing Methodologies

Various risk assessment methodologies are reported in the existing literature. Some significant contributions bear weight and appear valuable among all. A selection from the trend setting research contributions in the concerned area are briefly described one by one for analysis of strengths and weaknesses, as follows:

2.1 CORAS

CORAS is technological development project, it is developing a tool supported framework for model-based security risk assessment. It provides a customized language for threat and risk modeling, and comes with detailed guidelines explaining how the language should be used to capture and model relevant information during the various stages of the security analysis [2]. The Unified Modeling Language is typically used to model the target of the analysis which makes this method has some strength and weakness, see table 1. For documenting intermediate results and for presenting the overall conclusions, a special CORAS diagrams will be used which are inspired by UML. The CORAS method provides a computerized tool designed to support documenting, maintaining and reporting analysis results through risk modeling. A security risk analysis is conducted in seven steps as follows:

- Introduction: Involves an introductory meeting. The main item on the agenda for this meeting is to get the representatives of the client to present their overall

goals of the analysis and the target they wish to have analyzed.
- o High Level Analysis: Involves a separate meeting with representatives of the client. It also involves a rough, high-level security analysis.
- o Approval: Involves a more refined description of the target to be analyzed, and also all assumptions and other preconditions being made.
- o Risk Identification: Identify as many potential unwanted incidents as possible, as well as threats, vulnerabilities and threat scenarios.
- o Risk Estimation: Focus on estimating consequences and likelihood values for each of the identified unwanted incidents.
- o Risk Evaluation: This step gives the client the first overall risk picture.
- o Risk Treatment: The last step is devoted to treatment identification.

Table 1: CORAS methodology (Strength and Weakness)

Strength	Weakness
o IT's for model-based risk assessment integrating aspects from partly complementary risk assessment methods and state-of-the-art modeling methodology applies the standardized modeling technique UML to form input models to risk analysis methods that are used in a risk management. o A UML based specification language targeting security risk assessment is used, which increases its applicability. o There are so many automated procedures which also increases its uses. o This is very useful for Object Oriented Projects. [2]	o Is a generalized one; hence, there is still a need to develop or extend the methodology for particularly requirements phase. o The participants of the meeting may or may not be well aware with the recent developments in the concerned area. o Not mentioned the accuracy level. o Does not clearly talk about the security attributes. [3]. o How the severity of threats and vulnerabilities is mapped', is not clear. Quantitatively risk assessment cannot be provided by CORAS.

2.2 COBRA

COBRA (Consultative, Objective and Bi-functional Risk Analysis), consists of a range of risk analysis, consultative and security review tools [4]. These were developed largely in recognition of the changing nature of IT and security, and the demands placed by business upon these areas.

The first, such undercurrent of change, was the growing acceptance that IT security was a business issue. It was, and is, becoming largely expected that security reviews should be business related, with cost justified solutions and recommendations. Another issue, most of the late 90s, is the search by many organizations for a better and more visible return on their security budgets. To achieve this, many organizations adopt new approaches to the traditional constraints of lack of expertise, time and finance. Oftentimes, a formal risk analysis technique is employed. However, conventional methods simply do not address the new demands placed by business management. Some go part of the way, but tend to introduce their own drawbacks and difficulties. COBRA, methodology, evolved very fast to tackle these issues properly, see table 2. It was recognized that business users should be involved from the outset. This carries a number of advantages, and shapes the entire review. In addition, a number of other radical departures were called for. The result was a risk analysis methodology and tool that will meet the most stringent of requirements, fully satisfying the changing demands placed upon the security or audit team. The risk assessment process, using COBRA, is extremely flexible. However, the default process usually consists of three stages; Questionnaire Building, Risk Surveying and Report Generation [4].

During the first stage, via module selection, the base questionnaire is built to fit the environment and requirements of the user. The second stage risk consultant questions are answered by appropriate personnel and the information is securely stored. For the third stage, risk assessments and 'scores' are produced for individual risk categories, individual recommendations are made and solutions offered, and potential business implications are explained.

Table 2: COBRA methodology (Strength and Weakness)

Strength	Weakness
o COBRA provides a variety of tools for risk assessment, which means most of the processes are automated. This makes the risk assessment process very easy. o The methodology has very simple steps and hence this is very easy for implementation perspective.	o Is based on the various questionnaire or survey i.e. opinion based; the participants may or may not be well aware with the recent developments in the concerned area. o Is a generalized one; hence, there is still a need to develop or extend the methodology for particularly requirements phase. o What is the accuracy level of this methodology is also not mentioned. o Risk assessment tech-

	nique is not clearly mentioned. o COBRA does not clearly talk about the security attributes. [3]. o Threats and vulnerabilities play an important role in the process of risk assessment; but how these are taken into consideration, is not clearly given in the methodology.

2.3 OCTAVE

The Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) define the essential components of a comprehensive, systematic, context-driven information security risk evaluation [5]. By following the OCTAVE Method, an organization can make information protection decisions based on risks to the CIA of critical information technology assets. The operational and the IT department work together to address the information security needs of the enterprise. Using a three-phase approach, OCTAVE examines organizational and technology issues to assemble a comprehensive picture of the information security needs of the enterprise which it some strength and weakness, see table 3. The Phases of OCTAVE are [5]:

Phase 1: Build Asset-Based Threat Profiles: This is an organizational evaluation. Key areas of expertise within the organization are examined to identify important information assets, the threats to those assets, the security requirements of the assets, what the organization is currently doing to protect its information assets, and weaknesses in policies and practice. The processes for this phase are: Identify Senior Management Knowledge, Identify Operational Area Knowledge, Identify Staff Knowledge and Create Threat Profiles.

Phase 2: Identify Infrastructure Vulnerabilities: This is an evaluation of the information infrastructure. The key operational components of the information technology infrastructure are examined for that can lead to unauthorized action. The processes for this phase are: Identify Key Components and Evaluate Selected Components.

Phase 3: Develop Security Strategy and Plans: Risks are analyzed in this phase. The information generated by the organizational and information infrastructure evaluations (Phases 1 and 2) are analyzed to identify risks to the enterprise and to evaluate the risks based on their impact to the organization's mission. In addition, a protection strategy for the organization and mitigation plans addressing the highest priority risks is developed. Each phase of the OCTAVE method contains two or more processes. The processes for this phase are: Conduct Risk Analysis and Develop Protection Strategy [5].

Table 3: OCTAVE methodology (Strength and Weakness)

Strength	Weakness
o In this methodology, all the operational critical threats, assets, and vulnerabilities are taken into consideration; this increases the accuracy of the risk assessment. o The methodology not only provides risk assessment value, but it also provides some security strategy and plans which increases the applicability of the process.	o Risk evaluation criteria are based on a qualitative scale (high, medium, low). o This methodology is a generalized one; hence, there is still a need to develop or extend the methodology for particularly requirements phase. o It considers only the CIA attributes. There are some other attributes like Authenticity, Non repudiation [3], Accountability, and Auditability [6] which may also be taken into this list for risk calculation factors. o The accuracy level is not mentioned. Therefore, one may validate this methodology and discuss the results by applying the same. o It is opinion based; the participants of the workshop may or may not be well aware with the recent developments in the concerned area.

2.4 CRAMM

CCTA (Central Communication and Telecommunication Agency) Risk Analysis and Management Method (CRAMM) includes a comprehensive range of risk assessment tools that are fully compliant with ISO 27001and which address tasks such as [7]:

- Asset dependency modeling,
- business impact assessment,
- identifying and assessing threats and vulnerabilities,
- assessing levels of risk.
- identifying required and justified controls on the basis of the risk assessment.

CRAMM provides a staged and disciplined approach embracing both technical and non-technical aspects of security, which it has some strength and weakness, see table 4. In order to assess these components. It is divided into three stages as shown below:

(a) Asset identification and valuation: CRAMM enables the reviewer to identify the physical, software, data and location assets that make up the information system. Each of these assets can be valued. Physical assets are valued in terms of the replacement cost. Data and software assets are valued in terms of the impact that would result if the information were to be unavailable, destroyed, disclosed or modified.

(b) Threat and vulnerability assessment: Having understood the extent of potential problems, the next stage is to identify just how likely such problems are to occur. CRAMM covers the full range of deliberate and accidental threats that may affect information systems including: Hacking, Viruses, Failures of equipment .

(c) Countermeasure selection and recommendation: CRAMM software uses the measures of risks determined during the previous stage and compares them against the security level in order to identify if the risks are sufficiently great to justify the installation of a particular countermeasure. CRAMM provides a series of help facilities including backtracking. What If? prioritization functions and reporting tools to assist with the implementation of countermeasures and the active management of the identified risks.

Table 4: CRAMM methodology (Strength and Weakness)

Strength	Weakness
o CRAMM provides a variety of tools for risk assessment, which means most of the processes are automated. This makes the risk assessment process very easy. o This methodology is fully compliant with ISO 27001, which also increases its applicability.	o Is a generalized one; hence, there is still a need to develop or extend the methodology for particularly requirements phase. o Quantitatively risk assessment cannot be provided by CRAMM. o For list of vulnerabilities, source is not clearly mentioned. o CRAMM does not clearly talk about the security attributes e.g. Confidentiality, Integrity, and Availability etc. [3]. o How the severity of threats and vulnerabilities is mapped', is not clearly given in CRAMM. Hence, there is a need to re-look in this perspective.

2.5 NIST Guide

Risk is the net negative impact of the exercise of vulnerability, considering both the probability and the impact of occurrence [8]. Risk management is the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level. NIST (National Institute of Standards and Technology) guide provides a foundation for the development of an effective risk management program, containing both the definitions and the practical guidance necessary for assessing and mitigating risks identified within IT systems. The ultimate goal is to help organizations to better manage IT-related mission risks. It has some strength and weakness, see table 5 [8].

Risk assessment is the first process in the risk management methodology. Organizations use risk assessment to determine the extent of the potential threat and the risk associated with an IT system throughout its SDLC. The output of this process helps to identify appropriate controls for reducing risk. The risk assessment methodology encompasses nine primary steps, which are given as follows:

- Step 1: System Characterization
- Step 2: Threat Identification
- Step 3: Vulnerability Identification
- Step 4: Control Analysis
- Step 5: Likelihood Determination
- Step 6: Impact Analysis
- Step 7: Risk Determination
- Step 8: Control Recommendations
- Step 9: Results Documentation

Steps 2, 3, 4, and 6 can be conducted in parallel after Step 1 has been completed.

Table 5: NIST methodology (Strength and Weakness)

Strength	Weakness
o This guide highly recommends the integration of risk assessment into SDLC [8]. Risk assessment is an iterative process that can be performed during each major phases of SDLC. This indicates that risk assessment process must be embedded in the early phases of SDLC i.e. Requirements phase itself. o The methodology has very simple steps and hence this is very easy for implementation perspective.	o Is a generalized one i.e. for all the major phases of SDLC. o The likelihood of the vulnerabilities is described as high, medium, or low; but at what basis, these levels are allocated, is not clearly mentioned. o For list of vulnerabilities, source is not clearly mentioned. o It does not talk about the quantification of the risk. o In the step 3, i.e. Vulnerability Identification, there is a step System Security Testing which cannot be followed at the requirements level. o Impact analysis is performed on the basis of

o The methodology uses a step 'Control Analysis', in which existing control analysis is done in various detailed steps, which improves the accuracy of methodology.	CIA attributes. There are some other attributes like authenticity, non-repudiation [3] [6].

2.6 SOMAP

The Security Officers Management and Analysis Project (SOMAP.org) presents Open Information Security Risk Assessment Guide which contains detailed information about security risk management and it has some strength and weakness, see table 6 . The current version of the SOMAP.org Guide describes two methodologies to analyze risk: qualitative methodology and quantitative methodology. Depending on the goals, which should be achieved when doing the risk Assessment, the one method is better suited than the other. So, the decision, which method to use, should be evaluated in front of the risk assessment.

The Risk Assessment Workflow helps in completing a structured risk assessment and analysis. The Workflow leads the security officer through five phases. Every such phase consists of multiple activities which sometimes can be done in parallel, sometimes need to be done sequentially. The activities are small pieces of work which can either be done by the security officer or which can be delegated. Depending on the activity in question, multiple persons need to give their input in order to finish an activity. This process consists of the following steps: Collect data, Threat Analysis, Vulnerability Analysis, Risk Retention and Risk Treatment [6].

In Risk Retention, there are four sub activities: Risk Identification, Risk Estimation, Risk Evaluation, and Risk Financing. Further, Risk Estimation can be done by both qualitatively way and quantitatively way. There are some risk calculation formulas for both the methods.

Table 6: SOMAP methodology (Strength and Weakness)

Strength	Weakness
ɒ The proposed methodology describes both the methods for risk assessment, qualitative, and quantitative. Users of this methodology can use any one depending upon the type of project. ɒ The methodology has a factor 'Control Effectiveness' that means 'how effective a Control when it is implemented'. Any control may have different effectiveness for different type of projects. This factor increases the accuracy level of the methodology.	ɒ Is a generalized one; hence, there is still a need to develop or extend the methodology for particularly requirements phase. ɒ Considers five key attributes for risk assessment: Confidentiality, Integrity, Availability, Accountability, and Auditability. Other attributes like authenticity, non-repudiation [3] which may also be taken into this list for risk calculation factors. ɒ Talks about the 'Cost of Control'; but about how this factor will be calculated. ɒ On which basis, all the ranks or values of components are defined, is not mentioned . ɒ What is the accuracy level of this methodology is also not mentioned. Therefore, one may validate this methodology and discuss the results by applying the same. ɒ Threats and vulnerabilities play important role in risk assessment process, but in the calculation part, only likelihood and impact of vulnerabilities are taken into consideration.

3 METHODOLOGY

Research methodology relies on a set of criteria to measure risk identification methodologies already been talk about previously which are: Model-based risk assessment :Providing descriptions of the target of assessment at the right level of abstraction., it acts as a medium for communication and interaction between different groups of stakeholders involved in a risk analysis and to document results and the assumptions on which these results depend [14]. The Unified Modeling Language: is a standardized general-purpose modeling language originally designed for the object-oriented paradigm. UML has also been suggested for the design of embedded and real-time systems [15]. Quantification: For the accuracy of the results, quantification of any process is highly required. Most of the methodologies provide various mathematical formulas for assessing the correct value. Moreover, quantification increases the reliability of the process [16]. Standard Compliance: If any methodology is relevant standard compliance, it increases the trust level. Therefore, suitable standards' compliance must be achieved to extend the level of usability. Supporting Tools: Automation of any process makes the steps easier; therefore, tools support is highly recommended [17]. Integration of Security Attributes: Confidentiality, Integrity, and Availability are the basic pillars of information security. Preservation of these attributes must be considered in any process. Integration of Threats and Vulnerabilities: Vulnerabilities are the weaknesses of the software, which causes threats. There are various databases worldwide, which

maintain the list of these vulnerabilities in details along with their countermeasures. Therefore, it is highly desirable to address the same [18].

Table 7: Criterias that have been applied on methodologies

Criteria	CORAS	COBRA	OCTAVE	CRAMM	NIST	SOMAP
Model-based risk assessment	Yes					
A UML based specification language	Yes					
Automated procedures	Yes	Yes		Yes		
Very useful for Object Oriented Projects	Yes					
Easy for implementation perspective		Yes			Yes	
Applicability	Yes		Yes	Yes		
Accuracy			Yes		Yes	Yes
Integration of risk assessment					Yes	
Quantification						Yes
Integration of Threats and vulnerabilities	Yes		Yes	Yes	Yes	
Supporting Tools	Yes	Yes		Yes		
Standard compliance				Yes		

After the applying the criteria's on risk identification methodologies, see table 7, Can draw the following:

In case of CORAS, it is better to include the: 1) Inclusion of Confidentiality, Integrity and Availability. 2) Quantitatively risk assessment cannot be provided. 3) Consideration of threats and vulnerabilities in the process. 4) Extension with requirements phase perspective. 5) Validation and presentation for a live project

In case of COBRA, it is better to include the: 1) The accuracy level of this methodology is also not mentioned. 2) Increase the usability and the accuracy. 3) Quantification of the risk assessment. 4) Inclusion of Confidentiality, Integrity and Availability. 5) Add threats and vulnerabilities in the process. 6) making the methodology more specific for requirements phase, along with a validation report.

In case of OCTAVE, is better to include the: 1) Undertaken for the quantification of steps. 2) Inclusion of other attributes like Authenticity, Non-repudiation, Accountability, and Auditability. 3) The accuracy level of this methodology is also not mentioned.

In case of CRAMM, is better to include the: 1) Throwing light on the mapping of threats and vulnerabilities. 2) Quantification of risk value. 3) Inclusion of CIA.

In case of NIST, is better to include the:1) Throwing the light on the likelihood of the vulnerabilities, base of the levels of vulnerabilities. 2)Inclusion of other security attributes, like authenticity, non-repudiation, making the process more specific for requirements perspective.

In case of SOMAP, is better to include the: 1)Throwing light on 'cost of control' and the base of the ranks or values of components. 2) Inclusion of other attributes like Authenticity, Non-repudiation, Accountability. 3) The accuracy level of this methodology is also not mentioned.

4 Conclusion

This paper presents a comparative study between the top risk assessment methodologies like CORAS, COBRA, OCTAVE, CRAMM, NIST Guide , and SOMAP, along with its strengths and weaknesses which can be easily done by the Senior IT Personnel by going through the results, derived in the paper.

On the other hand, this paper may help to provide effective and efficient ways to incorporate security right from the beginning in the development life cycle.

References

[1] Principles of Information Security, Fourth Edition, Michael E. Whitman and Michael E. Whitman, Course Technology, 20 Channel Center, Boston, MA 02210, USA.

[2] CORAS: A Platform for risk analysis of Security Critical Systems. IST-2000-25031. 2000. Available on: http://www2.nr.no/coras/

[3] Chandan Mazumdar, Mridul Sankar Barik, Anirban Sengupta. Enterprise Information Security Risk Analysis: A Quantitative Methodology. Proceedings of the National Workshop on Software Security (NWSS 2007), N. Delhi, India. 2007: 1-12.

[4] COBRA: Introduction to Security Risk Analysis. Available on: http://www.security-risk-analysis.com/

[5] Alberts C, Dorofee A. An Introduction to the OCTAVE Method, Software Engineering Institute. Carnegie Mellon University. 2001. Available on: http://www.cert.org/octave/methodintro.html

[6] Open Information Security Risk Assessment Guide Version 1.0. available on: www. SOMAP.org

[7] CRAMM: Information Security Risk Assessment Toolkit, http://www.cramm.com.

[8] Gary Stoneburner, Alice Goguen, Alexis Feringa. Risk Management Guide for Information Technology Systems. NIST Special Publication 800-30. July 2002.

[9] Corey Hirsch, Jean- Noel Ezingeard. Perceptual and cultural aspects of risk management alignment: a case study. Journal of Information Systems Security, JISSec. Jan 2008; 4(1): 3-20.

[10] Abdullah Tahir, Mateen Ahmed, Sattar Ahsan Raza, Mustafa Tasleem. Risk analysis of various phases of software development models. European Journal of Scientific Research. 2010; 140(3): 369-376.
[11] Allen C Johnston, Ron Hale. Improved security through information security governance. ACM Communications., January, 2009; 52(1): 126-129.
[12] Mustafa K, Pandey S K, Rehman S. Security assurance by efficient access control and rights. CSI Communication. September, 2008; 32(6): 29-33.
[13] Pandey S K, Mustafa K. Risk Assessment Framework (RAF). International Journal of Advanced Research in Computer Science. Sep-Oct, 2010; 1(3): 423-432.
[14] Jan Aagedal, Folker den Braber, Theo Dimitrakos, Bjørn Axel Gran , Dimitris Raptis, Ketil Stølen, Model-based Risk Assessment to Improve Enterprise Security, Copyright IEEE 2002. Published in the Proceedings ofthe Fifth International Enterprise Distributed Object Computing Conference, (EDOC 2002), pp. 51-62, September 17-20, 2002, Lausanne, Switzerland
[15] L. Lavagno, G. Martin, and B. V. Selic. UML for Real: Design of Embedded Real-Time Systems. Springer-Verlag, Secaucus, NJ, USA, May 2003.
[16] Allen C Johnston, Ron Hale. Improved security through information security governance. ACM Communications., January, 2009; 52(1): 126-129.
[17] Mustafa K, Pandey S K, Rehman S. Security assurance by efficient access control and rights. CSI Communication. September, 2008; 32(6): 29-33.
[18] Pandey S K, Mustafa K. Risk Assessment Framework (RAF). International Journal of Advanced Research in Computer Science. Sep-Oct, 2010; 1(3): 423-432.