A Comparative Study on Information Security Risk Analysis Methods

Vivek Agrawal*
The Norwegian Information Security laboratory – NISLAB, Gjøvik University College, Gjøvik, Indian.

* Corresponding author. Tel.: +47-46562450; email: vivek.agrawal@hig.no
Manuscript submitted October 2, 2015; accepted December 30, 2015.
doi: 10.17706/jcp.12.1.57-67

Abstract: *Background* – Risk Analysis is an integral part of management practice and an essential element of good corporate governance. There are many risk analysis methods available today, and it is a tedious task for an organization (particularly small and mid-scale company) to choose the proper method. *Problem* – Although many methods and tools are available in this domain, very few inventories do exist that are structured according to a set of common properties. There are many risk analysis methods available today, and the main task for an organization is to determine which one to use. *Contribution* – The objective of this review paper is to provide researchers, an analysis of four risk analysis methods using the Campbell *et al*. classification scheme. The major contributions of this paper are; 1) Present a summary of four Information Security Risk analysis methods using ontology, 2) Classify these risk analysis methods using Campbell *et al.* classification scheme, 3) Compare risk analysis methods based on generic attributes i.e. input, outcome, purpose, effort, scalability, methodology, etc.

Key words: CIRA, CORAS, ISRAM, IS, risk analysis.

1. Introduction

Information is a key asset for organizations, and reducing the risk of information compromise is a high priority. The primary objective of any organization involves management of business processes to use and maintain information systems. The information system must comply to the security objectives of confidentiality, integrity and availability, authentication, authorization and non-repudiation in order to ensure proper functioning of the business processes. Information security risk analysis is the basis of information protection, risk management, and risk in the process of information protection. Risk analysis is an assessment of risk management. As risk management requires accurate assessment as a condition, risk analysis is an indispensable aspect of the management of information protection. Risk analysis in particular has attracted major interest and it is evident from the fact that risk analysis is often used as the point of start for information security events. Risk analysis is an important component in the compilation of information security policy for the organization. There are many risk analysis methods available (some are free, some are paid) for use today. Every Risk analysis method is designed for a particular purpose using different approach, data, level of expertise/skill and parameters (input and output). It is important for an organization, who is interested to carry out risk analysis task, to select a proper risk analysis method to solve its purpose. The most logical way to select a specific method is the method of comparison based on certain criteria established by the organization or research community [1].

The primary objective of this study is to provide a better understanding of the fundamental differences and similarities between the various Information security Risk analysis methodologies using attribute-based comparison method. The other way of conducting a comparison i.e. forming a case-study to apply selected methods, is out of scope of this paper. This study performs a survey of some well-known risk analysis methodologies. The selected methodologies are described and analyzed to understand the underlying concepts. The analysis of the methodologies is followed by a comparison of essential features to extract differences and similarities. This paper provides comparative study of two *Qualitative* methods – CORAS [2], CIRA [3] and two *Quantitative* methods – ISRAM [4], IS Risk analysis based on business model (denoted as IS method from now onwards) [5] using Campbell *et al.* Classification scheme [6]. These four risk analysis methods are chosen for the study because they are well documented and their papers are available on the internet. These reports help to get the complete picture of all the phases and working methodology of these methods.

Unless otherwise stated, the word 'method' is used in this paper to a 'Risk Analysis' method, though often full phrase is used. The article is structured as follows: The current section introduces the scenario that helps to get the overview of this research work. *Motivation* explains the reason of carrying out this research work. *Problem Statement* is the short description of the question, unsolved queries related to a given research area and *Contribution* points out specific tasks carried out in this paper. Section 2 explains comparison works and reviews done by other authors in a recent past. Section 3 describes the working principle of the chosen risk analysis methods with the help of ontology. Section 4 compares risk analysis method using Campbell *et al*. framework [6]. Section 5 presents a discussion on the finding of the study using Campbell *et al*. framework. It describes purpose, input, outcome, etc.. of each risk analysis method. The paper ends with conclusion and Future work in Section 6.

1.1. Motivation

The IT Audit Benchmarking survey report [7] created by Protiviti, shows that almost 37% of small companies do not conduct an IT risk analysis tasks. In the case of small companies, selection of improper risk analysis method also results in poor risk analysis. It has been argued that the above mentioned problem can be addressed up to a certain extent using proper risk analysis strategy. There are many risk analysis methods available today, and the main task for an organization is to determine which one to use. The best way to choose among methodologies is to compare them, e.g. using its approach, level of expertise required, input parameters, and outcome. If the criteria that are used are applicable to all risk analysis methodologies, the organization can compare different methodologies objectively, and decide on the best one.

1.2. Problem Definition

Risk Analysis is an integral part of management practice and an essential element of good corporate governance. A wide variety of methodologies available to manage, assess and treat risks evidently be a great use to business. By having numerous choices, organizations can adopt one, or a combination of methods that best addresses their needs and fits their respective company structure and culture. Different methods will have varying uses, approach, purpose, and may stress a dissimilar set of aspects. There are many risk analysis methods available today, and the main task for an organization is to determine which one to use.

1.3. Contribution

This research work targets information security risk analysis methods used currently to analyze information security risks. There are four different security risk analysis methods analyzed, and the way in

which each of them analyze risk is investigated using ontology. The main contribution of this review is to conduct an analysis of four risk analysis methods and compare these methods using Campbell *et al.* classification scheme [6]. We also compared the risk analysis methods on the basis of purpose, input and output parameters, methodology used, scalability and effort required to conduct the analysis.

2. Related Work

The content of this section consists of several works that suggest the framework for comparing information security risk analysis methodologies while assessing the way risks are valued and prioritized.

Behnia *et al.* [8] and **Shukla *et al.*** [9] presented studies to compare several Information Security Risk Analysis methods. They selected some Qualitative methods and some Quantitative methods to draw their comparison study. They claim in their paper that the given framework for comparison makes the procedure of the selection of risk analysis methodologies easier and more prompt. However, their studies mainly presents summary of selected Risk Analysis methods and compare them on the attributes like 'languages', 'price', 'country of origin', 'vendor name', etc.. The reader learns nothing about the particular benefits, performance, input, output, effort associated with these methods.

Vorster & Labuschagne [1] identified the problem of selection of risk analysis methods and compared various risk analysis methods to address this issue. They used several criteria to compare different methods e.g. main formulae, number of people involved in the analysis, number of assets considered in the risk analysis, etc.. Authors indicated the difference in the formula of risk valuation used by CORAS and ISRAM processes i.e. CORAS prefers simplicity and thus provide a simple 'impact and probability' approach to determine loss, whereas ISRAM employs a complicated, all inclusive formula to value risk, thereby stressing accuracy over simplicity. The main limitation of this approach is the assumption while deciding simplicity and accuracy. There is no proven fact that a complex calculation/formula necessarily be accurate.

Badenhorst *et al.* [10] proposed a comparison framework using the criteria that focus on information technology, information security and risk approach completeness. The framework proposed by Badenhorst *et al*. indicates whether a methodology addresses a criterion or not. It does not use scales, or trade-offs that can aid the organization in choosing a methodology that will best meet their needs.

There is a well-known report on inventories for risk management and risk assessment methods and tools, published by **ENISA** [11] in June 2006. This paper provides a generic description of processes and activities implementing information Security Risk Management (RM) /Risk assessment (RA). The ENISA working group has defined attributes in order to classify Information Technology RM/RA method, process or standard. These attributes are categorized as A. Product Identity card, B. Product Scope, C. Users viewpoint. However, the report doesn't include newly suggested major Risk analysis methods as the report was written in 2006.

Paintsil compares four classic risk analysis methods, namely Mehari, AICPA/ CICA, CIRA, EM-BRAM in the report [12]. The author mentioned that the two classic risk analysis methods (Mehari, AICPA/ CICA) are useful for determining administrative and management controls for Identity Management Systems. They are expensive because their main inputs for the analysis are obtained from extensive assessment of an organization and collaboration with system stakeholders. The comparison framework used by the author is based on three distinct categories. It compares risk analysis methods on the basis of 'Applicable Approaches', 'levels of Expertise', 'Method Types'.

Campbell *et al.* [6] presented a classification scheme for risk analysis methods. This scheme provides meaning by imposing a structure that identifies relationships. Their scheme is based on two orthogonal aspects-level of detail and approach. A risk analysis method can take three approaches in order to serve its purpose i.e. Temporal, Functional and comparative. Level of detail can be categorized into Abstract,

mid-level and Concrete. They presented their scheme through 3×3 matrix..

3. Summary of Risk Analysis Methods

This section explains the main principle of CIRA, CORAS, ISRAM and IS methods in a brief but comprehensive manner. An ontology is also presented for each Risk analysis method to present definitions of basic concepts in the domain of risk analysis and relations among them [13]. Ontology also helps to share common understanding of the structure of information among people or software agents [14], [15].

3.1. CORAS

CORAS [16], [17] is a model-based method for conducting security risk analysis. It uses a qualitative approach to address Information security risks [18]. CORAS was developed under the Information Society Technologies (IST) program. One of the main objectives of CORAS is to develop a framework that exploits methods for risk analysis, semi-formal methods for object orienting modeling and computerized tools for precise, unambiguous and efficient risk assessment of security critical systems. The methodology is based on UML, a language that uses diagrams to illustrate relationships and dependencies between users and the environment in which they work. In the CORAS method, a security risk analysis is conducted in eight steps. In step 1 to 4, a common understanding of the target of the analysis is established. This includes determining the scope and the focus of the analysis and giving the overall description of the target, which will serve as a basis for the subsequent risk identification. The remaining four steps are devoted to the actual detailed analysis. These steps include identifying concrete risks and their risk level as well as identifying and assessing potential treatments for unacceptable risks. An overview of the elements of the CORAS ontology is presented in Fig. 1. The ontology depicts that the Target contains Assets having some Value and has its Security requirements. Security requirements leads to Security policy that helps to reduce Vulnerabilities and protect Assets. An Asset can have one or many Vulnerabilities that can be exploited by Threats. Every Threat has some specific Source and Intent. Threat and Vulnerability may give rise to Risk that has a certain Likelihood and Frequency.

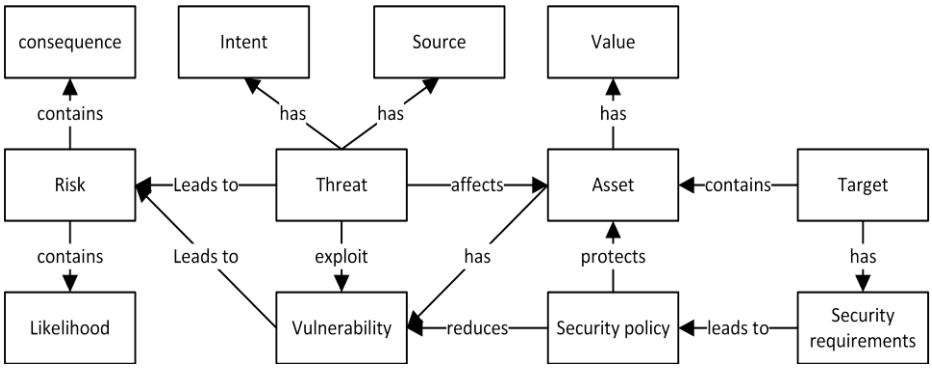

Fig. 1. Basic Ontology of CORAS, based on [18].

3.2. CIRA

Conflicting Incentives Risk Analysis (CIRA) was developed in January 2014 in Gjøvik University College in Norway by Rajbhandari and Snekkenes [3]. This method is based on the idea of qualitative analysis. CIRA method identifies stakeholders, actions and perceived expected consequences that characterize the risk situation. In CIRA, a stakeholder is an individual that has some interest in the outcome of actions that are taking place within the scope of the significance. There are two classes of stakeholders: the strategy owner and the risk owner. Strategy owner is the stakeholder who is capable of triggering an action to increase his perceived benefit. Typically, each stakeholder has associated a collection of actions that he owns. The risk

owner is the stakeholder whose perspective is considered when performing the risk analysis, i.e., he is the stakeholder at risk. CIRA focuses on the human-related risks. This corresponds to understanding the incentives of the stakeholders that influence their actions. An incentive is something that motivates a stakeholder to take action to increase his expected/ predicted utility. Utility is the benefit as perceived by the corresponding stakeholder. Utility comprises of utility factors. Each factor captures a specific aspect of utility, e.g., prospect of wealth, reputation, ego. Thus, utility can be approximated as the sum of weighted values for utility factors using Multi-Criteria Decision Analysis. An overview of the elements of the CIRA ontology is presented in Fig. 2. The ontology states that Risk Owner and Strategy Owner has a certain Description that defines them. Strategy Owner performs some Strategy that modifies the Utility Factors of both Risk Owner and Strategy Owner. Utility Factor uses Utility Metric that consists of Weight and Scale, to compute its value. The change in Utility Factors is perceived as Incentive that generates Risk in the system. The Risk can be treated by Risk Treatment methods.

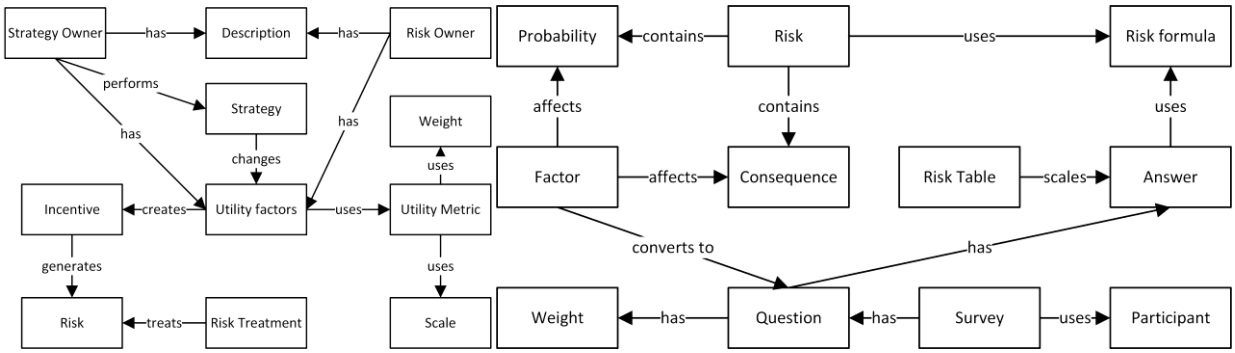

Fig. 2. Ontology of CIRA.

Fig. 3. Ontology of ISRAM.

3.3. ISRAM

Information Security Risk Analysis Method (ISRAM) [4] was developed in December 2003 at the National Research Institute of Electronics and Cryptology and the Gebze Institute of Technology. It is a quantitative approach to risk analysis and a survey based model used to analyze risk in information security. The method includes two major attributes of risk i.e. probability and consequence to conduct two separate and independent surveys. The method is based on risk being modeled as a combination of probability and consequence of a security breach. The risk factor in ISRAM approach is a numerical value between 1 and 25. This numerical value corresponds to a qualitative, high, medium or low value, and it is this qualitative value on which risk management decisions are based. ISRAM is proposed for Information Security risk analysis. It is designed for analyzing the risks at complex information systems by allowing the participation of managers and staff. It consists of seven steps, the first four steps are the preparation phase where the surveys are constructed. During step 5 the surveys are completed and risk analysis is performed during step 6. The final step is the assessment of the result. An overview of the elements of the ISRAM ontology is presented in Fig. 3. The ontology identifies Risk that contains Probability and Consequence. There are a certain Factors that affect Probability and Consequence of Risk. These Factors are converted into Questions of Survey done by Participants. The Question uses Weight to find Answers. Risk Table scales the survey Answers and with the help of a given Risk Formula, Answers are converted into a numeric value of Risk.

3.4. IS Risk Analysis Based on Business Model

The IS method, is a quantitative method, developed at the Korea Advanced Institute of Science and Technology in 2002 [5]. This model was developed because traditional IS risk analysis methods do not adequately reflect the loss from disruption of operations in determining the value of Information Systems'

assets. There are four stages of this method. In the first stage, it uses AHP (Analytic Hierarchy Process) for determining the relative necessity and importance of certain business functions. In second stage, a "`traditional"' risk analysis process is conducted: Assets are identified and assigned to the business functions, resulting in the relative necessity of assets. The third stage includes a threat and vulnerability assessment resulting in the determination of risk probability. In fourth stage, annualized loss expectancy (ALE) calculation is conducted to assess the overall loss due to business discontinuity. This proposal does not include any means for revising suitable safeguards for risk mitigation. An overview of the elements of the IS ontology is presented in Fig. 4. According to the given ontology, Asset is the first significant point of contact. An organization owns several Assets where each Asset is related to some Business function of the Organization. The identification of Risk involves an analysis of the Vulnerability in Assets, and the Threats that has a certain Source and Intent. A Risk can cause Injury in the system that can hampers the Asset of the Organization. The Injury needs a Recovery time, but it creates an Income loss. A Risk has a Probability that can affect the Control requires to mitigate Vulnerability.

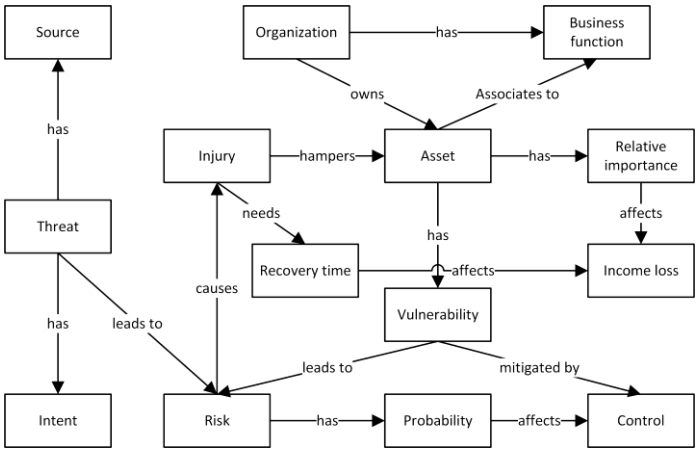

Fig. 4. Ontology of IS.

4. Classification of Risk Analysis Methods

In this section, we compare the risk analysis methods to identify characteristics shared by the methods. It is done in this paper using Campbell *et al*. classification scheme [6]. This classification scheme is based on two orthogonal aspects *Approaches, Level of Detail*. The approaches can be temporal, functional, or comparative. A temporal approach focuses on technical security. It depends on an understanding of the system, being investigated and may require formal system modeling. It estimates risk based on the actual system tests and analysis. A functional approach is between the temporal approach and a comparative approach. It has less focus on technical security than the temporal approach but requires more system-specific understanding than the comparative approach. The functional approach focuses on understanding threats to the system and how to mitigate these threats. It employs threat models rather than formal system models to analyze risk. The comparative approach focuses on management or non-technical security. It represents an explicit risk analysis standard. The standard or procedure is then compared with that of a system owner. The categories of levels determine the capabilities or skills required to execute a risk analysis method and the extent to which a risk assessor need to understand the system under investigation. The following sections show how the classification scheme is applied to compare the risk analysis methods discussed in this paper.

4.1. Approach

This section compares the approaches used by the methods discussed under Section 3. Table 1 shows the classification of the approaches used by the four methods discussed in the paper.

The CORAS [18], CIRA [3], and the IS method [5] come under *Functional* approach where the understanding of the technical system or model is less important. Functional approaches is mainly based on risk models rather than a technical system model or specification to determine the necessary security controls for a system or an organization. Risk assessors or system stakeholders play a keen role to estimate a risk in this approach. Administrative, policies and management procedures are the primary focus of the analysis. CORAS, CIRA and IS consider specific threats, vulnerabilities, assets and countermeasures. The outcome of functional risk analysis approaches is useful for 'management level' and 'operational level' decision making in organizations but less useful for 'technical level'.

Table 1. Approaches of Risk Analysis Methods

	Approach	
Temporal	Functional	Comparative
-	CORAS, CIRA, IS	ISRAM

The ISRAM [4] method falls under the *Comparative* approach. Method follows comparative approach implement an explicit risk analysis standard such as ISO 27005 [19]. ISRAM implements ISO/IEC 17799 [20] and ISO/IEC 13335 [21] standards. There is no explicit system model or list of threats, assets involved in the comparative approach. The model and the lists are only implicitly present in generic form. ISRAM allows the participation of manager and staff of the organization to conduct risk analysis process. One of the strengths of this approach is its simplicity. Comparative methods can be ideal for organizations as they begin to focus attention on security. The risk assessors estimate risk based on their subjective intuition and employ no formal approach to reduce the subjectivity in the risk estimation. Comparative approaches are less useful for 'technical level' details but useful for 'Management level' and 'operational level' decision making.

4.2. Levels of Expertise

This section compares the expertise/skills needed to use the risk analysis method discussed above. *Abstract* methods have broad application but require a high level of expertise. *Concrete* methods have a narrow application but require only a low level of expertise. The methods that are a mix of abstract and concrete are referred as *mid-level*. Abstract method is often conducted by an *expert*[1] person e.g. risk analyst.

The *owner*[2] is involved to the extent that an expert needs information about the system, but the owner does not drive the method. Concrete methods are executed by the owner and do not require an expert to be explicitly involved during the assessment (though the expert is implicitly involved to the extent that the owner follows the expert's direction as described by the method). Mid-level methods are driven by both expert and owner. Mid-level methods can thus be referred to as *collaborative*. Table 2 shows the classification of the levels of expertise required for various risk analysis methods.

The IS method [5] requires thorough understating of organization's mission, development of the business model, identification of asset and evaluation, threat and vulnerability assessment. An expert is required to execute the method therefore it falls under the abstract or expert levels. The expert must be having specialist level of knowledge. This also implies that IS method could be expensive as it needs an expert and thorough knowledge of all the business process and entities. However, IS method reduces cost by adopting mathematical approach to assess risk and loss. The method also leads to the involvement of various field

[1]an outside consultant who is knowledgeable in risk analysis methods but unfamiliar with the target system
[2]someone who is not knowledgeable in Risk analysis methods but is familiar with the target system

managers as well as the IS manager, increasing all managers' understanding of the risks and threats.

Table 2. Level of Expertise Needed for Risk Analysis Methods

Level of Expertise		
Abstract (Expert)	Mid-level (collaborative)	Concrete (Owner)
IS Specialist	CORAS & CIRA	ISRAM Standard

Table 3. Comparison Summary of Risk Analysis Methods

Criteria	CORAS	CIRA	ISRAM	IS
Methodology	Qualitative	Qualitative	Quantitative	Quantitative
Purpose	model-based method to conduct risk analysis through strong business and asset orientation	Non-Technical risk analysis and decisions	Analyze the risks at complex information systems by allowing the participation of managers and staffs	calculate Annual loss expectancy
Input	Direct asset, vulnerability, threat scenario, risk, risk evaluation matrix, likelihood scale	Stakeholders, strategies, utility factors, weight, initial values	questions for the survey, weight of the question, risk table	business function, assets, importance of asset
Effort	Specialist level and time-consuming	Specialist level and time-consuming	Standard level, less time-consuming	Specialist level and time-consuming
Outcome	identify potential risks and assess potential treatments for unacceptable risks	Strength of Stakeholders incentive or changes in utility	single numeric value for representing the risk, Annual loss expectancy	calculation of loss from disruption of operations in determining the value of IS assets
Scalability	Yes	No	Yes	No
Pros	Free tool support, Facilitates iterative communication and collaboration between various stakeholders, suitable for security-critical systems and large organizations	tool support, useful for both small and large organizations, Detects human risks in Information security	It is self-directed i.e. can be carried out by small teams of the organization's own employees, Ease of use, does not require dedicated tools	based on a business model where importance of business functions and assets are evaluated, especially useful for large enterprise organizations
Cons	Requires expert knowledge from various backgrounds, extra efforts required, Time-consuming	Expert knowledge required, Full assessments of the method can be time-consuming and overly-complex	preparation phase and initial data collection phase can be time-consuming, absence of any expert can make the whole task complex	Expert knowledge required, Full assessments can be an extremely lengthy process and time-consuming

The CORAS and CIRA methods are mid-level or collaborative. This means that system stakeholders and experts need to work together to execute this method. The participants must be having specialist level of knowledge to conduct the analysis. In a large system or organization, obtaining the initial input could be time consuming and expensive. Thus, the CIRA and CORAS methods require extensive expertise 'to introduce' the method while the IS may require little preparation. In addition, effective risk communication is required to get the best out of the method because experts and non-experts speak different languages.

ISRAM [4] method is Concrete as it does not require any high level of expertise to execute it. In this

method, staff and manager (owner) participate to conduct a survey in order to identify potential risk in the business. Participants need to have standard level of skills to conduct the analysis. Participants identify potential list of factors that can affect the probability of security breach and consequence of a security breach to conduct risk analysis. This method is not costly as it doesn't require expert or any special skills.

5. Discussion

This section discusses risk analysis methods based on Methodology, purpose, input, effort, outcome, scalability, pros, and cons. The findings of this comparison study is presented in Table 3.

The **CORAS** method is model-based risk analysis method to conduct risk analysis through strong business and asset orientation. CORAS is also available as a tool viz. CORAS editor V.1.1 developed by European commission in Jan 2001. It is compliant to standards AS/NZS 4360, ISO/IEC 17799. The level of specialist skill is needed to introduce, use and maintain this method. The input of this method is decided at various meeting conducted among analysis leader, representative of customer, decision makers and technical experts. This method needs expertise, and it is time consuming, as they need to identify assets, vulnerability, threat scenario, risk. Vraalsen *et al*. [22] argued that it is difficult to assess the scalability[3] of the CORAS framework, but it does not give any indications that it doesn't scale well.

The **CIRA** method focuses on non-technical security risk analysis. The inputs of the method are stakeholders' incentives, utility factors, etc. Understanding such non-technical procedures in an organization could be more time consuming and requires more effort than obtaining a technical specification. In addition, none of the inputs for CIRA method is predetermined. CIRA method could be expensive as it requires an expert to lead the risk analysis. The risk analysis results of a particular department/group cannot be reused to other departments or the whole organization because requirements are specific to each group, its stakeholders and their interests. The output of the method is non-technical security risks and control decision. The major disadvantage of the CIRA method is that it is not compliant to any regulation or IT standard.

The **ISRAM** method is a survey based quantitative approach proposed to analyze security risks of information technologies by allowing the participation of the manager and staff of the organization. It is compliant to standards ISO/IEC 17799 and ISO/IEC 13335. The input of this method comes from the discussions among risk analysis team. The team decides relevant factors that may affect probability and consequence of the occurrence of a security breach along with weights of each factor. ISRAM doesn't require any expert to carry out analysis as the OWNERS of the organization are adequate to assess risk factors. The outcome of the analysis is a numeric value of risk that is calculated using formula [4]. This method is scalable as the inputs are not group/scenario specific and can be reused with minor adjustment.

The **IS** method is introduced to reflect the loss from the disruption of operations in determining the value of IS assets. It focuses on the calculation of annual loss expectancy. The input of the method is decided through policies, processes in the meeting among risk analysts, manager. It depends on the mission and objectives of the organization. This method requires an expert to make a judgment at each stage of the analysis. The output is the calculation of loss from the disruption of operations. The output is this method cannot be reused at it is specific to the department and organization. A change in the asset can bring major change in the business function associated with it. Therefore, the analysis done on a particular asset-business function cannot be extended. The major downfall of the IS method is that it is not compliant to any regulation or IT standard.

6. Conclusion and Future work

[3]We are considering a method scalable if the input values can be reused without making significant change

There are many risk analysis methods exist today, and it is a tedious task for an organization (particularly small and mid-scale company) to choose the proper method. This study aims to analyze and compare the four information security risk analysis methods. The classification scheme of Campbell *et al.* is used to stabilize the analysis as it classifies risk analysis methods into approach and level of expertise. This analysis will be helpful for the companies, risk experts to find major attributes related to each method. The procedure of selecting a method can become easier and more prompt. Instead of going through the original report of a risk analysis method, anyone can directly check this paper to find information given in the most relevant attributes to make any decision. For instance, if an organization is interested in a method that strictly follows IT standards then CIRA and IS method are obviously not a good choice. Similarly, when the requirement is to get a numerical value of the risk instead of some subjective classification, then ISRAM is a good candidate to consider. From the Table, it is evident that ISRAM does not include any expert to carry our risk analysis task where as CIRA, IS, CORAS need an expert. If an organization is looking for a method that doesn't need any expert and can be conducted by the internal staff and managers then ISRAM is a good candidate for the selection.

For future work, the above approach will be explored with a comprehensive case study. An example risk analysis of a use case will be performed with all the risk analysis methods such that the results of the methods in use can be compared to each other. Moreover, the study will also include new developments in risk analysis standards i.e. ISO/IEC 27005:2011 – Information security risk management [19]; ISO/IEC 27002:2005 – Code of practice for Information Security Management [23]; ISO/IEC 13335-1:2004 – Concepts and models for information and communication technology security management [21]. Additionally, after including other well-known methods into the analyis, the summary of the comparison presented in the section 5 will be converted into a guideline to present a picture to the readers about the selection of Risk analysis process.

Ackowledgment

The author recognizes the contribution of comment and instruction from Einar Arthur Snekkenes and Gaute Wangen. We also thank the anonymous reviewers for their contributions to this manuscript.

References

[1] Vorster, A., & Labuschagne, L. (2005). A Framework for comparing different information security risk analysis methodologies. *Proceedings of the Annual Research Conference of the South African Institute of Computer Scientists and Information Technologists on IT Research in Developing Countries* (pp. 95-103).

[2] Stolen, K., den Braber, F., Dimitrakos, T., Fredriksen, R., Gran, B. A., Houmb, S.-H., *et al.* (2002). Model-based risk assessment-the coras approach. *Proceedings of iTrust Workshop*.

[3] Rajbhandari, L., & Snekkenes, E. (2013). Using the conflicting incentives risk analysis method. *Security and Privacy Protection in Information Processing Systems, 405,* 315-329.

[4] Karabacak, B., & Sogukpinar, I. (2005). ISRAM: Information security risk analysis method. *Computers & Security*, *24*, 147-159.

[5] Suh, B., & Han, I. (2003). The \IS\ risk analysis based on a business model. *Information & Management, 41*, 149-158.

[6] Philip, J. E. S., & Campbell, L. (2004). A classification scheme for risk assessment methods. SANDIA National Laboratories.

[7] Protiviti, (2012). 012 IT audit Benchmarking survey.

[8] Behnia, A., Rashid, R. A., & Chaudhry, J. A. (2012). A survey of information risk analysis methods. *Smart Computing Review,* 2, 79-94.

[9] Shukla, N., & Kumar, S. (2012). Article: A Comparative study on information security risk analysis practices. *Special Issue on Issues and Challenges in Networking, Intelligence and Computing Technologies,* 28-33.

[10] Eloff, J. H. P., Labuschagne, L., & Badenhorst, K. P. (1993). A comparative framework for risk analysis methods. *Comput. Secur., 12*, 597-603.

[11] Marinos, L. (2006). Risk Management — Principles and inventories for risk management / risk assessment methods and tools.

[12] Paintsil, E. (2014). *Risk Methods and Tools for Identity Management Systems.*

[13] Nurse, J. C., & Sinclair, J. (2009). Supporting the comparison of business-level security requirements within cross-enterprise service development. *Business Information Systems*, *21,* 61-72.

[14] Noy, N. F., & Mcguinness, D. L. (2001). *Ontology Development 101: A Guide to Creating Your First Ontology.*

[15] Chandrasekaran, B., Josephson, J. R., & Benjamins, V. R. (1999). What Are ontologies, and why do we need them? *IEEE Intelligent Systems, 14*, 20-26.

[16] den Braber, F., Hogganvik, I., Lund, M. S., Stølen, K., & Vraalsen, F. (2007). Model-based security analysis in seven steps — A guided tour to the CORAS method. *BT Technology Journal, 25*, 101-117.

[17] Lund, M., Solhaug, B., & Stølen, K. (2011). A guided tour of the CORAS method. *Model-Driven Risk Analysis*, 23-43.

[18] Aagedal, J. O., den Braber, F., Dimitrakos, T., Gran, B. A., Raptis, D., & Stolen, K. (2002). Model-based risk assessment to improve enterprise security. *Proceedings of Sixth International Enterprise Distributed Object Computing Conference* (pp. 51-62).

[19] ISO. (2008). ISO/IEC 27005 Information technology-security techniques-information security risk management.

[20] Wiander, T. (2008). Implementing the ISO/IEC 17799 standard in practice: Experiences on audit phases. *Proceedings of the Sixth Australasian Conference on Information Security: Vol. 81* (pp. 115-119).

[21] ISO. ISO/IEC 13335 Information technology — guidelines for the management of IT security. International Standards Organisation, Geneva, Switzerland.

[22] Vraalsen, F., den Braber, F., Hogganvik, I., *et al.* (2004). *The CORAS Tool-Supported Methodology for UML-Based Security Analysis*.

[23] SO/IEC 27002: 2005 - information technology - security techniques - code of practice for information security management.

Vivek Agrawal received the MS degree in information and communication systems security from Royal Institute of Technology, Sweden, in 2013. He is currently working toward the Ph.D. degree in migration of risk analysis tool to the cloud computing at University College Gjøvik, Norway. His general interests are in the field of Information security, risk management, vehicular communication, network security. His specific interests include software engineering, secure cloud computing, risk analysis methods and tools.