Comparative Study of Information Security Risk Assessment Model

Keerti Dixit
Institute of Computer Science
Vikram University, Ujjain

Umesh Kumar Singh, PhD
Institute of Computer Science
Vikram University, Ujjain

Bhupendra Kumar Pandya, PhD
Institute of Computer Science
Vikram University, Ujjain

ABSTRACT

Analysis of security risks is crucial to the management of information systems. The same risks brought on by information assets, their potential threats, and vulnerabilities, as well as security measures, are to be prevented by security risk analysis models. Today, the majority of these models are utilized to assess risk value without recognizing the organization's security issues. As a result, decision-makers are unable to choose the best methodology for addressing security concerns. In this research paper, we have developed a Comparative Framework to carry out a thorough comparative analysis of the various models that underpin the information risk assessment process. Next, we have evaluated existing information security risk assessment models through this framework.

Keywords

Information Security Risk Assessment, risk, threat, vulnerability

1. INTRODUCTION

Business today depends heavily on information systems. Our lives have become much faster and simpler thanks to computer networks, but these conveniences have also given rise to a number of risks to information systems [1]. Being linked with the external world, any information asset is open to attacks. Threats with the potential to exploit vulnerabilities are what lead to the attacks. One of the most crucial factors for the firm is risk, which is caused by any kind of loss to these assets [2]. This demonstrates the need for a systematic method to evaluate information security risks. Information security risk assessment has grown in importance for companies over the past few years as a result of the publication of risk recommendations or regulations by industry and government governing bodies [3]. The rise in elevated information technology security breaches and the security expectations of technologically advanced business partners are two further factors pushing organizations to use sound risk assessment techniques. Technically, risk is the potential harm that could result if a certain threat takes advantage of a specific vulnerability to harm an asset, and risk analysis is the method for recognizing security risks and gauging their significance and influence on an organization [4, 5].

There are so many methodologies and tools for information security risk assessment. We have noted the similarities among the methodology for information security risk assessments, the components that must be considered while conducting one, the methodologies' advantages, and their drawbacks [6, 7].

Hence, in order to undertake a thorough comparison examination of several approaches that support the information risk assessment process, we developed a Comparative Framework. This evaluation framework relates to a predetermined group of crucial characteristics that serve as the standards for the current information risk assessment procedures. It aids in establishing efficient approach according to evaluate that highlights similarities and dissimilarity as well as the strengths and limitations of the existing approaches.

2. CRITERIA FOR COMPARATIVE FRAMEWORK

Structure, Identification, Techniques, Training, Functionality, Guidance, Usability Consistency and, Tool support are some major criteria for the resulting requirements and characteristics.

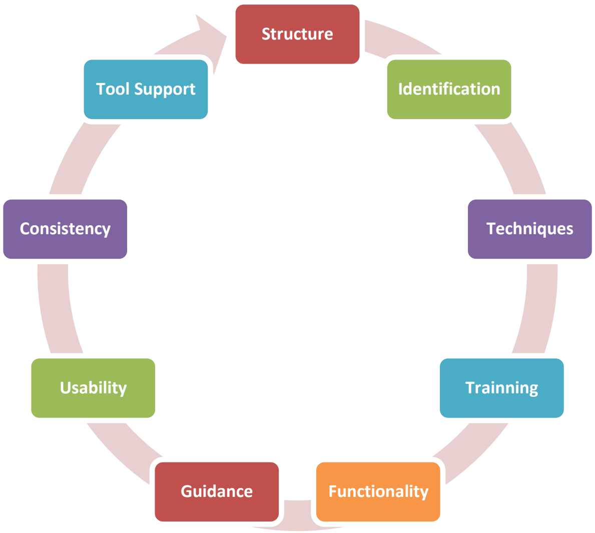


Figure 1: Criteria for Comparative Framework

Structure: This criterion describes the steps involved in carrying out a thorough assessment of the information risk in particular domain & organization. It offers stage process methodology and guides a user in an additional structured manner than instructions, benchmarks, and standards in protection and risk.

Identification: To scope the assessment, an analysis team must follow a number of specific steps, which are represented by this feature. Undoubtedly, a controlled and organized approach is needed. The methodology includes a threat index and a list of security practice areas for your convenience.

Techniques: Requirement to give proponent relevant, current, and upgrade technique for suitably gathering, analyzing, & reporting results of information risk assessment is key component of the information risk assessment methodology.

Training: Focusing on obtaining the necessary grip and fundamental expertise is a crucial need in the information risk assessment process, including information risk analysts, must meet in order to allow them to successfully complete the tasks associated with information risk-assessment. Increased member awareness of their level of security understanding is outcome of information risk assessment carried out within an organization.

Functionality: In order to successfully complete the difficult tasks of recognition, data gathering, evaluation, verification, reporting, and result presenting, information risk assessment processes and tasks must offer effective functionalities. Information risk-assessment approach's main goal is to give the evaluation team the flexibility to carry out various tasks in line with predetermined specifications.

Guidance: This criteria highlights the direction the approach offers in order to secure organizational support, that is a critical key factor for successful in carrying out a thorough information risk assessment in a specific scenario and organization.

Usability: It measures methodology's usability and the extent to which the analysis team can utilize it to carry out information risk assessment effectively, efficiently, and to the necessary satisfaction levels.

Consistency: This criterion speaks about the uniformity with which various team members apply the methodology. Setting definitions of terms used in information risk assessment is one strategy that works well for achieving uniformity.

Tool Support: The approach is considerably simpler to apply if it is accompanied by tools that carry out the necessary activities and allow for simple customization in accordance with organizational requirements.

3. COMPARATIVE FRAMEWORK

Despite their similarities, existing ISRA models have unique traits as well as unique advantages and disadvantages. Based on these specifications and traits, we created a comparative framework to compare the operations, procedures, and techniques associated with each information risk assessment approach.

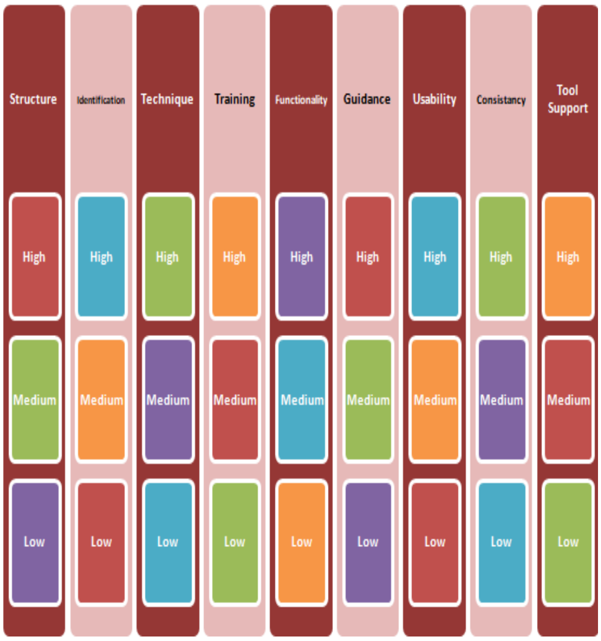
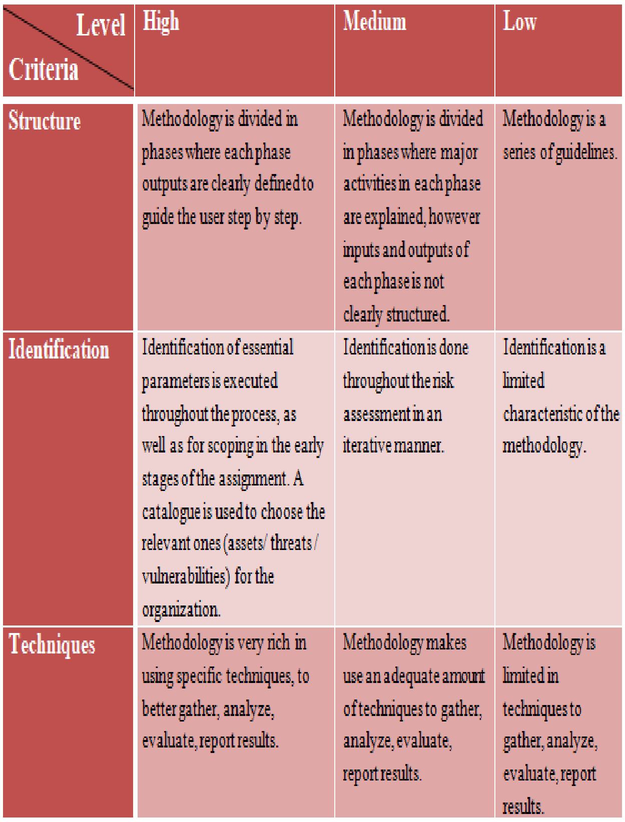
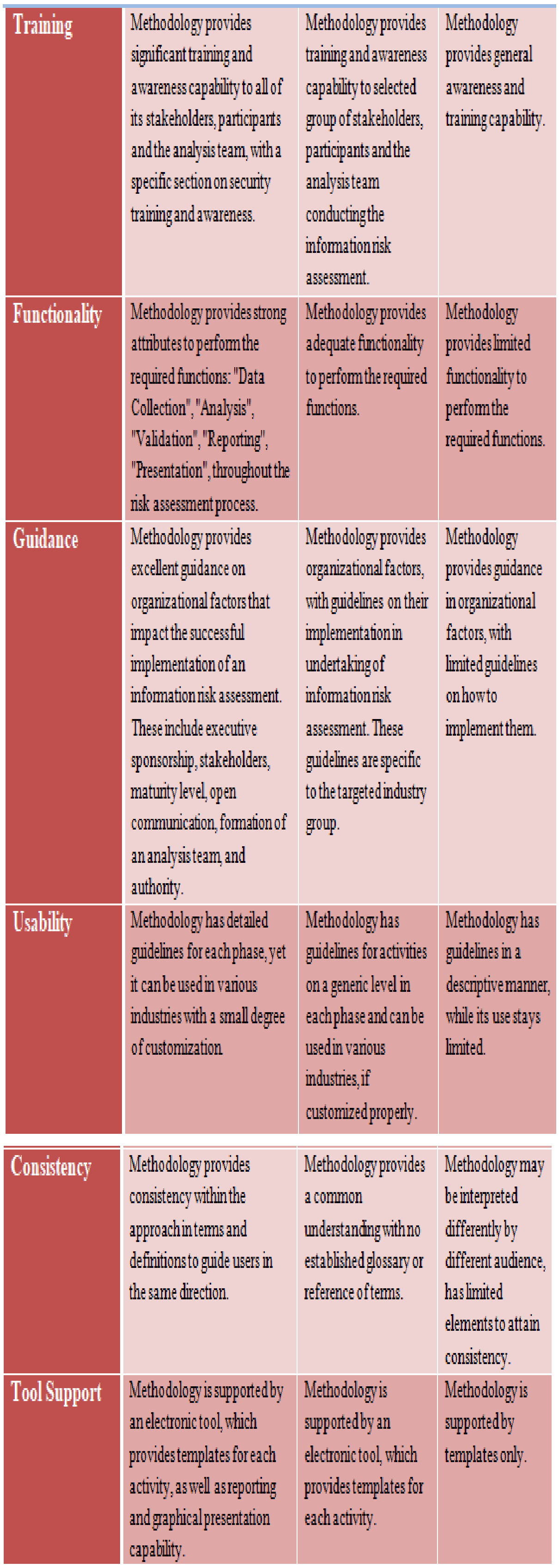


Figure 2: Comparative Framework

Table 1: Criteria Description of Comparative Framework



Level / Criteria	High	Medium	Low
Structure	Methodology is divided in phases where each phase outputs are clearly defined to guide the user step by step.	Methodology is divided in phases where major activities in each phase are explained, however inputs and outputs of each phase is not clearly structured.	Methodology is a series of guidelines.
Identification	Identification of essential parameters is executed throughout the process, as well as for scoping in the early stages of the assignment. A catalogue is used to choose the relevant ones (assets/ threats / vulnerabilities) for the organization.	Identification is done throughout the risk assessment in an iterative manner.	Identification is a limited characteristic of the methodology.
Techniques	Methodology is very rich in using specific techniques, to better gather, analyze, evaluate, report results.	Methodology makes use an adequate amount of techniques to gather, analyze, evaluate, report results.	Methodology is limited in techniques to gather, analyze, evaluate, report results.



Training	Methodology provides significant training and awareness capability to all of its stakeholders, participants and the analysis team, with a specific section on security training and awareness.	Methodology provides training and awareness capability to selected group of stakeholders, participants and the analysis team conducting the information risk assessment.	Methodology provides general awareness and training capability.
Functionality	Methodology provides strong attributes to perform the required functions: "Data Collection", "Analysis", "Validation", "Reporting", "Presentation", throughout the risk assessment process.	Methodology provides adequate functionality to perform the required functions.	Methodology provides limited functionality to perform the required functions.
Guidance	Methodology provides excellent guidance on organizational factors that impact the successful implementation of an information risk assessment. These include executive sponsorship, stakeholders, maturity level, open communication, formation of an analysis team, and authority.	Methodology provides organizational factors, with guidelines on their implementation in undertaking of information risk assessment. These guidelines are specific to the targeted industry group.	Methodology provides guidance in organizational factors, with limited guidelines on how to implement them.
Usability	Methodology has detailed guidelines for each phase, yet it can be used in various industries with a small degree of customization.	Methodology has guidelines for activities on a generic level in each phase and can be used in various industries, if customized properly.	Methodology has guidelines in a descriptive manner, while its use stays limited.
Consistency	Methodology provides consistency within the approach in terms and definitions to guide users in the same direction.	Methodology provides a common understanding with no established glossary or reference of terms.	Methodology may be interpreted differently by different audience, has limited elements to attain consistency.
Tool Support	Methodology is supported by an electronic tool, which provides templates for each activity, as well as reporting and graphical presentation capability.	Methodology is supported by an electronic tool, which provides templates for each activity.	Methodology is supported by templates only.

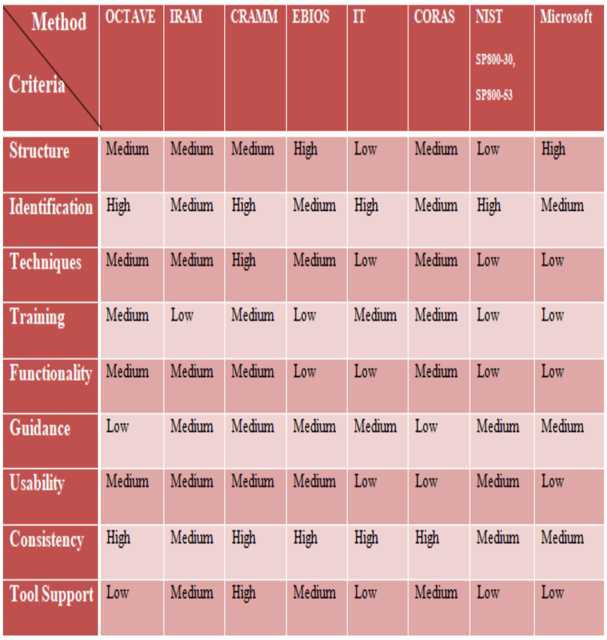
The comparative framework shown above illustrates the broad standards by which we evaluate the current approaches. Each methods enacts and consolidates a series of steps, activities, or processes, including the identification of personal information, threat and security risk, risk analysis, evaluating solutions to meet current, knowing the level of information police, security training and education, correspondence planning, and road mapping, at various levels.

These actions are frequently seen to have a significant impact on how successfully an information risk assessment turns out. The presence of fundamental functionalities, such as data collection, analysis, validation, reporting and presentation, is a characteristic shared by these frameworks. In order to comprehend the information risks facing the organization, there is a general trend towards developing and putting into practice standardized frameworks for information risk assessment. At every stage of information risk assessment, the proper actions are taken in order to achieve the end result of creating a risk profile for information security within the firm.

4. COMPARATIVE STUDY OF ISRA MODELS THROUGH PROPOSED COMPARATIVE FRAMEWORK

We have compared Octave [8], IRAM [9], CRAMM [10], EBIOS [11], IT-Grundschutz [12], NIST [13], CORAS [14], and Microsoft Security Risk Management [15] models through proposed comparative framework. Table 2 shows the results of comparative study.

Table 2: Comparative study of ISRA Methodologies



Method / Criteria	OCTAVE	IRAM	CRAMM	EBIOS	IT	CORAS	NIST SP800-30, SP800-53	Microsoft
Structure	Medium	Medium	Medium	High	Low	Medium	Low	High
Identification	High	Medium	High	Medium	High	Medium	High	Medium
Techniques	Medium	Medium	High	Medium	Low	Medium	Low	Low
Training	Medium	Low	Medium	Low	Medium	Medium	Low	Low
Functionality	Medium	Medium	Medium	Low	Low	Medium	Low	Low
Guidance	Low	Medium	Medium	Medium	Medium	Low	Medium	Medium
Usability	Medium	Medium	Medium	Medium	Low	Low	Medium	Low
Consistency	High	Medium	High	High	High	High	Medium	Medium
Tool Support	Low	Medium	High	Medium	Low	Medium	Low	Low

Structure: Information risk assessment methodologies enable the performance of various steps, including Identification of assets, evaluation of the organization's security awareness, evaluation of threats and vulnerabilities, impact evaluation, and risk evaluation, through phases consisting of several activities. Although structure is essential for directing user in the execution of information risk assessment, it limits the flexibility of the method's customization, which may be needed to use the approach across various sectors.

The discussed approaches are divided up into stages and tasks. We have evaluated steps of each methodology. While the order of the tasks may vary from one methodology to another, the tasks themselves that are carried out in the various phases are constant. The phases can be thought of as being misplaced as a result. The French government and the defense industry were the primary drivers behind the development of EBIOS' structure. Additionally, Microsoft's organizational design is particularly flexible for IT businesses like Microsoft., adding a level of specificity.

Identification: Each phase's characteristic varies depending on the methodology, which affects how they go about determining scope. The initial scoping of the effort must include identification. OCTAVE includes a validation component while iteratively scoping the effort in the first stage. This is accomplished by identifying inputs (assets, problem areas, and organizational security requirements) in the first 3 processes, beginning with management, moving through functional management, and finishing at the staff. Prior to completing a business impact analysis, the organization's important assets are determined. Typically, this task is completed in the first stage of the other techniques. A greater range of analysis is provided by the inclusion of risk management in NIST and Microsoft. The criticality establishes the assessment's scope. The scope is adjusted when the risk assessment identifies the essential information assets and their dependencies. As a result, it is best to create a rough draught of the project's scope at the start and then amend it when new information becomes available.

Techniques: Several methodology and stages of the project for information risk assessment use various techniques. They have offered a list of risks from which to choose the ones that are right for the company. A threat inventory is not provided by Microsoft or OCTAVE. A starting list is helpful for firms performing their initial information risk assessment because each organization's list of threats is unique.

In terms of presentation, CORAS employs visual methods, OCTAVE makes use of threat tree diagrams, and CRAMM uses approaches for greater visibility and collaboration, including reporting into its software and the graphical display of the results. While the other techniques offer templates, they do not offer any particular visual aids or graphical results depiction for simpler management evaluation. Most important steps in current approaches are risk appraisal. The fact that risk assessment is heavily influenced by participants' subjectivity is another issue. Iteration, evaluation, and validation of the outcomes help to some extent reduce this ambiguity, and participant involvement in the process encourages them to assume responsibility for the observations activity. Open communication, knowledge sharing, and change management are therefore crucial organizational elements in the process.

Training: The first step in assisting a specific organization in lowering and effectively responding to information risks is information risk assessment. To support the process of managing information security risks, a training programme is required for the research team conducting the evaluation, as well as an employee information security education and awareness practice. Although information security is thought to be primarily the duty of the information technology personnel, since the majority of threats are internal to the company, everyone must contribute. Majority of methodologies incorporate industry-recognized best practices for information security, such as those found in ISO 17799, which can be used to create surveys and provides a list of these practices. This survey is essential to judge participants' knowledge of information security risks and practices, but it also serves as a tool for raising awareness. When developing survey questions to evaluate participants' security awareness, it is essential to take the organization's unique control environment into account. Those organizations that understand the importance of information security employ separate training programmes on a larger scale.

Functionality: While some methodologies focus on these elements more than others, "Data Collection," "Analysis," "Validation," "Reporting," & "Presentation" are each primary steps in every method. CRAMM enhances capability of automated reporting with its software. CORAS utilizes the visual tools that are beneficial for data presentation. At the end of each phase in OCTAVE, the results are validated. Guidelines are provided by EBIOS, NIST, ITGrundschutz, and Microsoft methods. The phase of threat and vulnerability assessment, which is primarily technical and carried out by information security specialists who have received specialized training in this area, is one of the features. In contrast to inspection, "analysis" refers to interpretation by many members.

Guidance: Approaches under study offer the user instructions and a framework to adhere to. They don't fully explain on the project management needs crucial information risk assessment procedure. Despite the fact that the exercise appears to be primarily a technical one, getting the organization's employees to work together and implement the necessary adjustments to the controls in order to make them more robust to security incidents is more of an art than a science. The suggested techniques fall short in addressing the organizational change needed to instill a risk aware culture. The approaches are not explicitly described in the tasks that show how to maintain sponsorship, keep stakeholders interested, encourage open communication, and provide the analytic team enough authority. Although it is not specifically included in the techniques, training and awareness are crucial components in risk recognition.

Usability: This quality measures how much an information risk assessment approach may increase its applicability. Regarding its natural language, company standards, regional best practices, and regulatory context, information risk assessment is mainly employed in particular location. While the EBIOS and NIST frameworks were developed specifically for defense organizations, the Microsoft and IRAM framework are exceptional in that they offer characteristics designed to facilitate technology organizations. OCTAVE, on the other hand, was primarily developed for defense organizations but can be appropriately described as having a general use.

Consistency: When choosing the best technique that may be customized to the demands of the company, misunderstanding is greatly reduced by consistency in the description and understanding of these terms. To improve communication, it is helpful to create a shared understanding of terminology before attempting to discover common terms. The approaches define the words, and some include glossaries.

Tool Support: It's important to highlight that the ISRA approach described here pay minimal attention to crucial elements like modelling and risk quantification, which have an impact on the outcomes and the process's effectiveness. Another problem is that while the frameworks offered contain electronic-tools, reporting is not available outside of the excel sheets and other tool-provided templates. Hence, the process of capturing, reporting, and maintaining the records involves a sizeable administrative component. CRAMM's software minimizes this strain. The time required to use software products properly and efficiently during the process is the problem.

5. CONCLUSION

In this research paper we have developed a comparative framework to perform a comprehensive comparative evaluation of various information risk assessment approaches. With the help of proposed framework we have compared 8 methodologies of information security risk assessment

With this comparative research, we observed that no model could provide the fundamental characteristics needed by a well-structured information security risk assessment methodology. As a result, we realized that in order to secure organizations, there is a need for an integrated information security risk assessment method that meets the aforementioned criteria.

This framework also supports the development of an efficient approach dependent on examination of parallels & divergences, as well as the advantages and disadvantages, of the existing techniques.

6. REFERENCES

[1] Danial F. Gareia and Adrian Fernandez, “Effective Methodology for Security Risk Assessment of Computer Systems”, International Journal of Computer, Electrical, Automation, Control and Information Engineering, vol. 7, no. 8, 2013.

[2] Wang, J., Neil, M., & Fenton, N., “A Bayesian network approach for cybersecurity risk assessment implementing and extending the FAIR model” Computers and Security, 89, 101659, 2020. https://doi.org/10.1016/j.cose.2019.101659

[3] Hiller, J. S., & Russell, R. S., “The challenge and imperative of private sector cybersecurity : An international comparison. Computer Law & Security Review”, 29(3), 236–245, 2013. https://doi.org/10.1016/j.clsr.2013.03.003

[4] K.V.D. Kiran, L.S.S. Reddy, Velagapudi Pavan Kumar, Kalluri Krishna Sai Dheeraj, “Security Risk Management in critical Informative Systems”, conference on IT in Business, Industry and Government, 2014.

[5] Piya Shedden, Atif Ahmad, Wally Smith, Heidi Tscherning, Rens Scheepers, “Asset identification in information security risk assessment: A business practice approach”, Communications of the Association for Information System, vol. 30, 2016

[6] Keerti Dixit, “Information Security Risk Assessment in Higher Educational Institutions-Issues and Challenges” presented in 36th M.P. Young Scientist Congress, March 23 - 26, 2021

[7] K. Dixit, U. K. Singh, B. K. Pandya, “Comparative Framework for Information Security Risk Assessment Model”, ICCIDS-2022 International Conference on Computational and Intelligent Data Science (Elsevier) 21 May 2022.

[8] Muhammad Asif Kha, “Efficacy of OCTAVE Risk Assessment Methodology in Information Systems Organizations”, International Journal of Computer Applications Technology and Research Volume 6–Issue 6, 242-244, 2017, ISSN:-2319–8656

[9] ISF: Information Security Forum. 'TRAM: Information Risk Analysis Methodologies Project Control Selection", January 2006.

[10] Insight Consulting, "Managing Risk in Your Organization, Achieving True Corporate Governance through the Management of Risk", 2005.

[11] DCSSI Advisory Office, "EBIOS - Section 2: Approach", 2004.

[12] Federal Office for Information Security, Germany, "IT-Grundschutz Catalogues", 2005.

[13] P. Bowen, J. Hash, M. Wilson, "NIST Special Publication 800-53: Recommended Security Controls for Federal Information Systems", National Institute of Standards and Technology, December 2007.

[14] K. Stolen, "Security Analysis: CORAS in Seven Steps", Sintef & University of Oslo, 2007.

[15] Microsoft Solutions for Security and Security Center of Excellence. "The Security Risk Management Guide" Version 1.1, 2004.