Buletin Teknik Elektro dan Informatika
(Bulletin of Electrical Engineering and Informatics)
Vol.1, No.2, June 2012, pp. 111~122
ISSN: 2089-3191

A Comparative Study of Risk Assessment Methodologies for Information Systems

S. K. Pandey[1], K. Mustafa [2]
[1]Department of Information Technology, Board of Studies
The Institute of Chartered Accountants of India (Set up by an Act of Parliament), Noida- 201 309
[2]Department of Computer Science
Jamia Millia Islamia (Central University), New Delhi-110 025
e-mail: santo.panday@yahoo.co.in[1], kmfaruki@yahoo.com[2]

Abstract

Today's highly vulnerable world information systems are subjected to greater risks than ever before. As a result, related officials should be in a position to identify the risks which an organization faces and its management policies have to effectively manage those risks. Risk assessment is currently used as a key technique for managing security information systems. Literature reveals various information security risk assessment methods that can be implemented by the organizations, and each has different approaches to assess the information security risks. Organizations find it difficult to select an information security risk assessment method. Therefore, there is a need for a critical review of existing risk assessment methodologies. This paper presents a brief discussion on the top risk assessment methodologies, particularly COBRA, CORAS, CRAMM, OCTAVE, SOMAP, and NIST Guide, along with its strengths and weaknesses. After that, a comparative study is also done as the basis of the review results. Further research directions may also be taken by the weaknesses section. This work provides an evaluation to determine whether an information security risk assessment method is in line with information technology governance or not. The research paper will help the senior IT personnel to provide their recommendations for using a risk assessment methodology based on the specific requirements of an organization.

Keywords: *Risk Assessment, Review of Risk Assessment Methodologies, Information Security, Comparative Study of Risk Assessment Methodologies.*

1. Introduction

Todays, business is very depending on the information systems. Computer networks have made our life very fast and easy, but along with these facilities, this rises to various threats to the information systems. Any information asset, when connected to the outside world, is vulnerable to attacks. The attacks are caused by threats which have a potential to exploit vulnerabilities. Any type of damage to these assets cause risk and it is one of the most important factors for the organization [11] [13]. This shows the requirement of a systematic approach to assess information security risks.

Over the last couple of years, information security risk assessment has become more important for organizations as a result of the release by government and industry governing bodies of risk recommendations or requirements [1][2][3]. Other pressures to implement solid risk assessment principles are the increase breaches in high-profile information technology (IT) and the security requirements of technologically integrated business partners.

Formally, risk can be defined as the potential harm caused if a particular threat exploits a particular vulnerability to cause damage to an asset, and risk analysis is defined as the process of identifying security risks and determining their magnitude and the impact on an organization [4] [12]. NIST Guide for Security Certification and Accreditation [5] expands the definition to describe the process. Risk assessment include: (i) Identification of threats to and vulnerabilities in the system; (ii) Potential impact or magnitude of harm that a loss of CIA (Confidentiality, Integrity or Availability) would have on enterprise operations or enterprise assets, should an identified vulnerability be exploited by a threat; and (iii) The identification and analysis of security controls for the information system.

Received February 24, 2012; Revised May 5, 2012; Accepted May 10, 2012

An important fact in information security is that an asset often ceases to be sensitive or critical after a certain period of time i.e. the security requirements of an asset may change with time [4]. Manual methods of risk assessment can not be so effective due to increasing complexity of possible vulnerabilities and rising threats. There are so many methodologies and tools for risk assessment which available in the literature. Currently, there is not any comparative study which shows the strengths and weaknesses of each method that will assist organizations in determining which method is the best, in terms of IT governance recommendations, to be employed within an organization. This paper is authored to answer such type of questions.

The rest of the paper is organized as follows: Section 2 presents a brief discussion of the existing Risk Assessment Methodologies, whereas in Section 3, 'Strengths and Weaknesses' of each one is discussed. In Section 4, a 'Comparative Study' is done on the basis of the critical review. Section 5 presents 'Future Research Directions' in the area. 'Conclusion and Future Work' is reported in Section 6.

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. COBRA

COBRA (Consultative, Objective and Bi-functional Risk Analysis), consists of a range of risk analysis, consultative and security review tools [6]. 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 and tools 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, and its default methodology, evolved very fast to tackle these issues properly. It was developed in full co-operation with one of the world's major financial institutions and followed by many years research. 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. A substantial number of approaches are supported. However, the default process usually consists of three stages [6]:

- Questionnaire Building
- Risk Surveying
- Report Generation

During the first stage, via module selection or generation, the base questionnaire is built to fit the environment and requirements of the user. The second stage is the survey process - *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.

Each of these stages is managed by its corresponding system component: Questionnaire Builder, Risk Surveyor and Report Generator.

2.2. CORAS

CORAS is a European research and technological development project, it is developing a tool supported framework for model-based security risk assessment. CORAS 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 [7]. In this respect, CORAS is model-based. The Unified Modeling Language (UML) is typically used to model the target of the analysis. For documenting intermediate results and for presenting the overall conclusions, we use special CORAS diagrams which are inspired by UML. The CORAS method provides a computerized tool designed to support documenting, maintaining and reporting analysis results through risk modeling. In the CORAS method, a security risk analysis is conducted in seven steps which are shown in Figure 1 [7]:

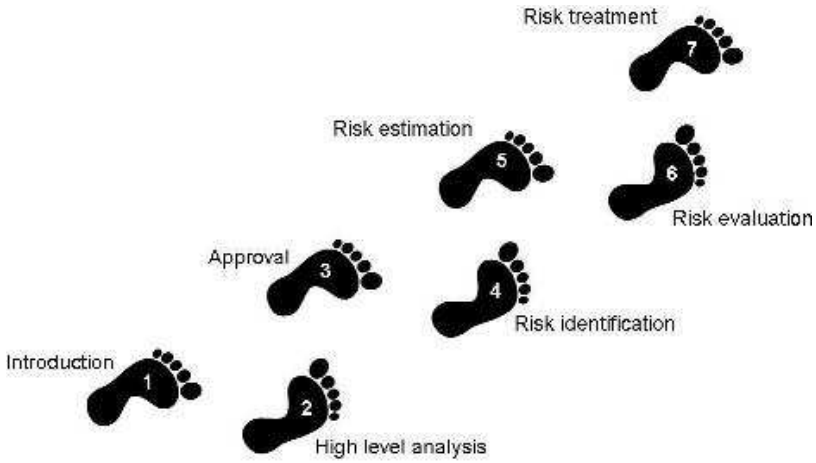

Figure 1: Steps of CORAS Method [7]

- **Step 1**: The first step 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. Hence, during the initial step the analysts will gather information based on the client's presentations and discussions.
- **Step 2**: The second step also involves a separate meeting with representatives of the client. However, this time the analysts will present their understanding of what they learned at the first meeting and from studying documentation that has been made available to them by the client. The second step also involves a rough, high-level security analysis. During this analysis the first threats, vulnerabilities, threat scenarios and unwanted incidents are identified. They will be used to help with directing and scoping the more detailed analysis still to come.
- **Step 3**: The third step involves a more refined description of the target to be analyzed, and also all assumptions and other preconditions being made. Step three is terminated once all this documentation has been approved by the client.
- **Step 4**: This step is organized as a workshop, drawn from people with expertise on the target of the analysis. The goal is to identify as many potential unwanted incidents as possible, as well as threats, vulnerabilities and threat scenarios.
- **Step 5**: The fifth step is also organized as a workshop. This time with the focus on estimating consequences and likelihood values for each of the identified unwanted incidents.
- **Step 6**: This step gives the client the first overall risk picture. This will typically trigger some adjustments and corrections.
- **Step 7**: The last step is devoted to treatment identification, as well as addressing cost/benefit issues of the treatments. This step is best organized as a workshop.

2.3. 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 [8]:

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

CRAMM provides a staged and disciplined approach embracing both technical (e.g. IT hardware and software) and non-technical (e.g. physical and human) aspects of security. In order to assess these components, CRAMM is divided into three stages as shown in Figure 2 [8]:

Figure 2. Steps of CRAMM Method [8]

(a) Asset identification and valuation: CRAMM enables the reviewer to identify the physical (e.g. IT hardware), software (e.g. application packages), data (e.g. the information held on the IT system) 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 or software
- Willful damage or terrorism
- Errors by people

This stage concludes by calculating the level of the underlying or actual risk.

(c) Countermeasure selection and recommendation: CRAMM contains a very large countermeasure library consists of over 3000 detailed countermeasures organized into over 70 logical groupings. The CRAMM software uses the measures of risks determined during the previous stage and compares them against the security level (a threshold level associated with each countermeasure) 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.

2.4. OCTAVE

The Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) define the essential components of a comprehensive, systematic, context-driven information security risk evaluation [9]. 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 or business units 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. The Phases of OCTAVE are [9]:

- **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 (protection strategy practices), and weaknesses in organizational policies and practice (organizational vulnerabilities).
- **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 weaknesses (technology vulnerabilities) that can lead to unauthorized action.
- **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 following list includes the processes for each phase of OCTAVE [9]:

- Phase 1: Build Asset-Based Threat Profiles
  - Process 1: Identify Senior Management Knowledge
  - Process 2: Identify Operational Area Knowledge
  - Process 3: Identify Staff Knowledge
  - Process 4: Create Threat Profiles
- Phase 2: Identify Infrastructure Vulnerabilities
  - Process 5: Identify Key Components
  - Process 6: Evaluate Selected Components
- Phase 3: Develop Security Strategy and Plans
  - Process 7: Conduct Risk Analysis
  - Process 8: Develop Protection Strategy

2.5. 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. 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 [10]. 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 [10]:

- Step 1: Collect data

- Step 2: Threat Analysis
- Step 3: Vulnerability Analysis
- Step 4: Risk Retention
- Step 5: Risk Treatment

In the step 4, 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.

2.6. NIST Guide

Risk is the net negative impact of the exercise of vulnerability, considering both the probability and the impact of occurrence [5]. 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 [5]. The ultimate goal is to help organizations to better manage IT-related mission risks [5].

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 or eliminating risk during the risk mitigation process.

Risk is a function of the likelihood of a given threat-source's exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization [5]. The risk assessment methodology encompasses nine primary steps (as shown in Figure 3), 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.

3. Strengths and Weaknesses

After a critical review of mentioned risk assessment methodologies above, we have noted some strengths and weaknesses of each one, which are given in the different sub-sections.

3.1. COBRA

After going through this methodology, we listed some strengths and weaknesses, which are given as follows:

(a) Strength(s):

The major strengths of this Risk Assessment methodology are as follows [6]:

- 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.
- The methodology has very simple steps and hence this is very easy for implementation perspective.

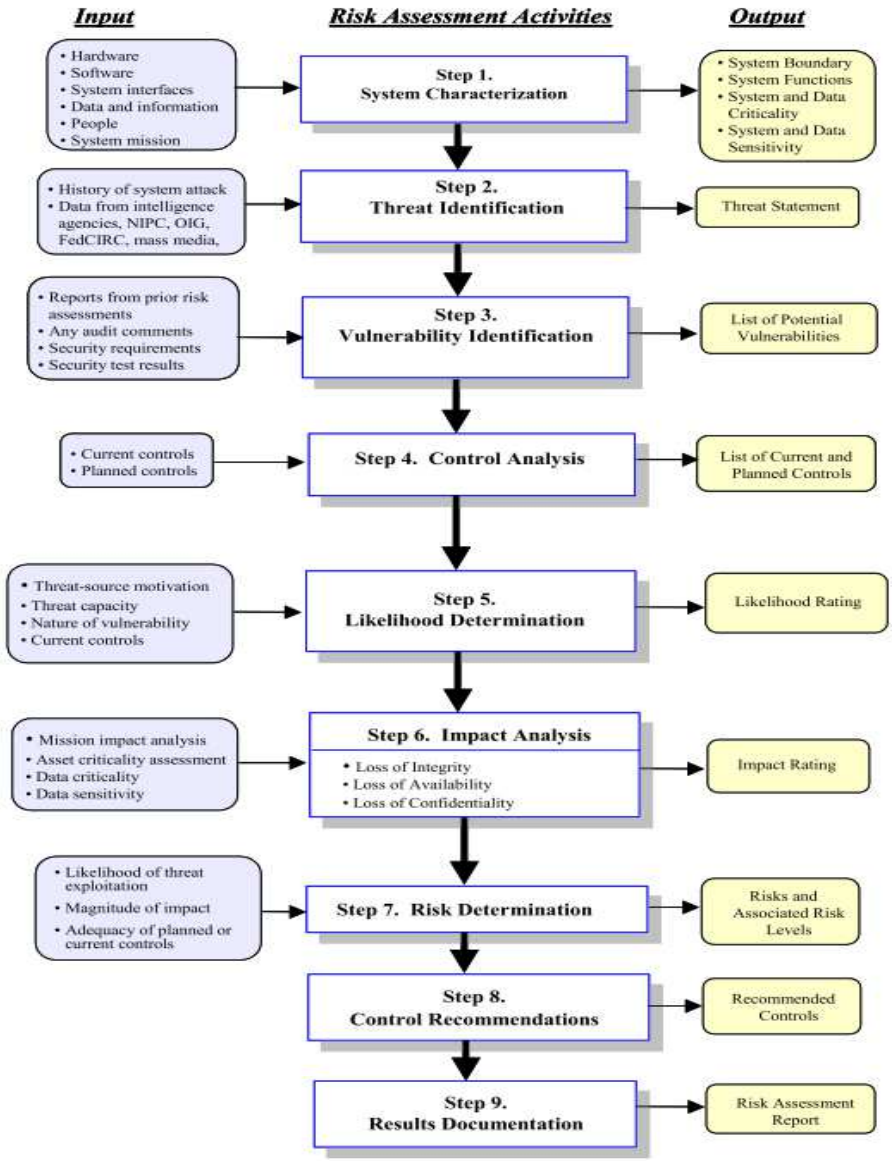

Figure 3. Risk Assessment Methodology Flowchart [5]

(b) Weaknesses:

The major weaknesses of this Risk Assessment methodology are as follows [6]:

- This methodology 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. Hence, there is a need to quantify a maximum number of steps.
- This methodology is a generalized one; hence, there is still a need to develop or extend the methodology for particularly requirements phase.
- 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.
- Risk assessment technique is not clearly mentioned; hence, there is need to extend this methodology in this direction.
- COBRA does not clearly talk about the security attributes e.g. Confidentiality, Integrity, and Availability etc [4]. Hence, this point can also be taken into consideration.
- Threats and vulnerabilities play a very important role in the process of risk assessment; but how these are taken into consideration, is not clearly given in the methodology. Hence,

further work may be done in this direction to increase the useability and accuracy of COBRA.

3.2. CORAS

After going through this methodology, we listed some strengths and weaknesses, which are given as follows:

(a) Strength(s):

The major strengths of this Risk Assessment methodology are as follows [7]:

- This methodology for model-based risk assessment (MBRA) 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.
- A UML based specification language targeting security risk assessment is used in the CORAS, which increases its applicability.
- There are so many automated procedures which also increases its uses.
- This is very useful for Object Oriented Projects.

(b) Weaknesses:

The major weaknesses of this Risk Assessment methodology are as follows [7]:

- This methodology is a generalized one; hence, there is still a need to develop or extend the methodology for particularly requirements phase.
- The methodology is much opinion based; the participants of the meeting or workshop may or may not be well aware with the recent developments in the concerned area. Hence, there is a need to quantify a maximum number of steps.
- 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.
- CORAS does not clearly talk about the security attributes e.g. Confidentiality, Integrity, and Availability etc [4]. Hence, this can also be taken into consideration.
- 'How the severity of threats and vulnerabilities is mapped', is not clearly given in CORAS. Hence, there is a need to re-look in this perspective.
- Quantitatively risk assessment can not be provided by CORAS. Hence, there need to extend this methodology in this direction.

3.3. CRAMM

After going through this framework, we listed some strengths and weaknesses, which are given as follows:

(a) Strength(s):

The major strengths of this Risk Assessment methodology are as follows [8]:

- 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.
- This methodology is fully compliant with ISO 27001, which also increases its applicability.

(b) Weaknesses:

The major weaknesses of this Risk Assessment methodology are as follows [8]:

- This methodology is a generalized one; hence, there is still a need to develop or extend the methodology for particularly requirements phase.
- Quantitatively risk assessment can not be provided by CRAMM. Hence, there is need to extend this methodology in this direction.
- For list of vulnerabilities, source is not clearly mentioned. Hence, some work may be done for identifying the source and also for ensuring the update of this list of vulnerabilities.
- CRAMM does not clearly talk about the security attributes e.g. Confidentiality, Integrity, and Availability etc [4]. Hence, this can also be taken into consideration.
- '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.

3.4. OCTAVE

After going through this guide, we listed some strengths and weaknesses, which are given as follows:

(a) Strength(s):

The major strengths of this Risk Assessment methodology are as follows [9]:

- In this methodology, all the operational critical threats, assets, and vulnerabilities are taken into consideration; this increases the accuracy of the risk assessment.
- The methodology not only provides risk assessment value, but it also provides some security strategy and plans which increases the applicability of the process.

(b) Weaknesses:

The major weaknesses of this Risk Assessment methodology are as follows [9]:

- Risk evaluation criteria are based on a qualitative scale (high, medium, low); hence, further work may include its extension for quantitative scales also.
- This methodology is a generalized one; hence, there is still a need to develop or extend the methodology for particularly requirements phase.
- The methodology considers only three attributes for risk assessment: Confidentiality, Integrity, and Availability. There are some other attributes like Authenticity, Non-repudiation [4], Accountability, and Auditability [10] which may also be taken into this list for risk calculation factors. This will improve the accuracy of the risk assessment.
- 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.
- The methodology is much opinion based; the participants of the workshop may or may not be well aware with the recent developments in the concerned area. Hence, there is a need to quantify a maximum no. of steps.

3.5. SOMAP

After going through this guide, we listed some strengths and weaknesses, which are given as follows:

(a) Strength(s):

The major strengths of this Risk Assessment methodology are as follows [10]:

- 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.
- 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.

(b) Weaknesses:

The major weaknesses of this Risk Assessment methodology are as follows [10]:

- This methodology is a generalized one; hence, there is still a need to develop or extend the methodology for particularly requirements phase.
- The methodology considers five key attributes for risk assessment: Confidentiality, Integrity, Availability, Accountability, and Auditability. There are some other attributes like authenticity, non-repudiation [4] which may also be taken into this list for risk calculation factors. This will improve the accuracy of the risk assessment.
- The method talks about the 'Cost of Control'; but this is not mentioned that how this factor will be calculated. Hence, there is a need to describe the same in detail.
- On which basis, all the ranks or values of components are defined, is not mentioned in the report. Hence, there is a need to clearly mention the base in this formula.
- 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.
- Threats and vulnerabilities play a very important role in risk assessment process. Although the method considers both the things in the beginning, but in the calculation part, only likelihood and impact of vulnerabilities are taken into consideration. Hence, threat related values may also be incorporated in the formula to increase the accuracy level.

3.6. NIST Guide

After going through this guide, we listed some strengths and weaknesses, which are given as follows:

(a) Strength(s):

The major strengths of this Risk Assessment methodology are as follows:

- This guide highly recommends the integration of risk assessment into SDLC [5]. 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.
- The methodology has very simple steps and hence this is very easy for implementation perspective.
- The methodology uses a step 'Control Analysis', in which existing control analysis is done in various detailed steps, which improves the accuracy of methodology.

(b) Weaknesses:

The major weaknesses of this Risk Assessment methodology are as follows [5]:

- This methodology is a generalized one i.e. for all the major phases of SDLC; hence, there is still a need to develop or extend the methodology for particularly requirements phase.
- The likelihood of the vulnerabilities is described as high, medium, or low; but at what basis, these levels are allocated, is not clearly mentioned in the report. Hence, this step may be revisited.
- For threat sources, all types of threats are taken into consideration. But from security perspective, some threats like natural threats e.g. floods, earthquakes, tornadoes, landslides etc. are not much relevant. Hence, this step also requires reconsideration with security points of view.
- For list of vulnerabilities, source is not clearly mentioned. Hence, some work may be done for identifying the source and also for ensuring the update of the list of vulnerabilities.
- This methodology does not talk about the quantification of the risk. Although some calculation is done, but it is not the accurate; because the values of high, medium, and low impact is fixed as 100, 50, and 10. Therefore, further research is required to quantify the entire calculation.
- In the step 3 of the report i.e. Vulnerability Identification, there is a step System Security Testing which can not be followed at the requirements level. Hence, for requirements level risk assessment, the methodology may be revisited.
- Impact analysis is performed on the basis of three attributes: confidentiality, integrity, and availability. There are some other attributes like authenticity, non-repudiation [4] [10] which may also be taken into this list for performing impact analysis. This will improve the accuracy level of the risk assessment.

4. Comparative Study

For accomplishing a comparative study of the aforementioned methodologies, some attributes have been identified based on the well known practices with similar cases. These are described as follows:

- **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 [14]. Moreover, quantification increases the reliability of the process.
- **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 [16].
- **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.
- **Requirements Phase Perspective**: Requirements phase is the backbone of any software to be developed [15]. As it is already discussed that this phase must be considered very seriously, it is necessary for any methodology to consider this perspective.
- **Accuracy level/ Validation**: Any methodology is only useful when it is well supported by the tryouts of a large sample of live projects. Therefore, this attributes is also desired.
- **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 useability.

- **Supporting Tools:** Automation of any process makes the steps easier; therefore, tools support is highly recommended.

On the basis of these review results i.e. strengths and weaknesses, a comparative study of the mentioned methodologies above is done. A table is made for the comparative study at- a-glance. If the methodology *fully satisfies* an attribute, a mark √ is drawn against the column, otherwise **×** is marked.

Table 1. Comparison of risk assessment methodologies

Attribute	COBRA	CORAS	CRAMM	OCTAVE	SOMAP	NIST Guide
Quantification	×	×	×	×	√	×
Integration of Security attributes	×	×	×	×	×	×
Integration of Threats and vulnerabilities	×	√	√	√	×	√
Requirements phase perspective	×	×	×	×	×	×
Accuracy level/ Validation	×	×	√	×	×	×
Standard compliance	×	×	√	×	×	×
Supporting Tools	√	√	√	×	×	×

5. Future Research Directions

Based on this critical review, strengths, and weaknesses of existing risk assessment methodologies, we have collected some future research directions which are given as follows:

- In COBRA, further research may be done for the quantification of the risk assessment, addition of CIA, threats and vulnerabilities in the process, making the methodology more specific for requirements phase, along with a validation report.
- In case of CORAS, future work may include the inclusion of CIA, quantification of the risk value, consideration of threats and vulnerabilities in the process, extension with requirements phase perspective, validation and presentation for a live project.
- Future research in CRAMM may include throwing light on the mapping of threats and vulnerabilities, quantification of risk value, inclusion of CIA, making more useful for conceptual phases of SDLC e.g. requirements phase.
- In OCTAVE, further research may be undertaken for the quantification of steps, inclusion of other attributes like Authenticity, Non-repudiation, Accountability, and Auditability, making the process more specific for requirements phase, along with a validation report.
- Further work may be done in SOMAP for throwing light on ‘cost of control’ and the base of the ranks or values of components, inclusion of other attributes like authenticity, non-repudiation, incorporating threat related values in the formula, making the methodology more specific for requirements phase, along with a validation report.
- In case of NIST guide, future research may be done for throwing the light on the likelihood of the vulnerabilities, base of the levels of vulnerabilities, inclusion of other security attributes, like authenticity, non-repudiation, making the process more specific for requirements perspective.

6. Conclusion

The paper presented a comparative study, strengths and weaknesses of the existing risk assessment methodologies along with the future research directions. Decision making for selecting a risk assessment methodology can be easily done by the Senior IT Personnel by going through the results, derived in the paper. Research community has made significant progress along with many fronts in the area of risk assessment. At the same time, the demands placed on computing and the cyber infrastructure has increased dramatically, raising many new critical research questions. Keeping in view, we presented a number of research areas in which

further work is required, based on the existing or published work. The major need is to make all the methodologies more specific for the requirements phase because requirements are considered as foundation stone on which the entire software can be built and the requirements phase is the foremost opportunity for the product team to consider how security will be integrated into a development process. This work may help to provide effective and efficient ways to incorporate security right from the beginning in the development life cycle. Possible future extension of the work has already been discussed exhaustively in the section above.

References

[1] King Committee on Corporate Governance, King II Report – 2002, Institute of Directors (IOD), South Africa, 2002.
[2] Sarbanes-Oxley Act of 2002, United States Congress. (H.R. 3763), (23 January 2002).
[3] Internal Control – Guidance for Directors on the Combined Code, The Institute of Chartered Accountants in England & Wales. (September 1999).
[4] 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.
[5] Gary Stoneburner, Alice Goguen, Alexis Feringa. Risk Management Guide for Information Technology Systems. NIST Special Publication 800-30. July 2002.
[6] COBRA: Introduction to Security Risk Analysis. Available on: http://www.security-risk-analysis.com/
[7] CORAS: A Platform for risk analysis of Security Critical Systems. IST-2000-25031. 2000. available on: http://www2.nr.no/coras/
[8] CRAMM: Information Security Risk Assessment Toolkit, http://www.cramm.com.
[9] 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
[10] Open Information Security Risk Assessment Guide Version 1.0. available on: www. SOMAP.org
[11] Douglas A Ashbaugh. Security Software development, Assessing and Managing Security Risk. CRC Press. 23rd Oct 2008.
[12] 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.
[13] 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.
[14] Allen C Johnston, Ron Hale. Improved security through information security governance. ACM Communications., January, 2009; 52(1): 126-129.
[15] Mustafa K, Pandey S K, Rehman S. Security assurance by efficient access control and rights. *CSI Communication*. September, 2008; 32(6): 29-33.
[16] Pandey S K, Mustafa K. Risk Assessment Framework (RAF). *International Journal of Advanced Research in Computer Science*. Sep-Oct, 2010; 1(3): 423-432.