Journal of Information Assurance and Security 6 (2011) 081-088

A Heuristic Approach for Qualitative Risk Assessment and Treatment Model

Javaria Sana[1] , M. Hasan Islam[2] and Bushra Fayyaz[3]

[1]NUST , College of Electrical and Mechanical Engineering,
Rawalpindi, Pakistan
javaria.sana@gmail.com

[2]Centre for Advance Studies and Engineering,
Islamabad, Pakistan
mhasanislam@gmail.com

[3]Centre for Advance Studies and Engineering,
Islamabad, Pakistan
Bushra.fayyaz@gmail.com

***Abstract*:** A good planning phase for development of any project includes problem identification, analysis, development and maintenance. Risk management is important in each phase but it is recommended after the plan has been detailed. Instead a technical feasibility analysis can be done to detect most of the risks. In this paper a qualitative risk assessment model is defined for managing risks. The risks related to all the assets and resources are identified and analysis is made. After finding out the criticality the countermeasures are set to mitigate risks according to the environment. The new model is compared with the commonly used approach for risk management.

1. Introduction

The prime objective of risk management process for any organization is providing information security, protecting the organization and its ability to perform their operation swiftly. It is the process of identification, assessment and taking preventive measures to lessen risk at an acceptable level. It is applicable on all types of management structures like for Information Security Management System (ISMS), Occupational Health and Safety Management System (OH&S), Environmental Management System (EMS) and Operational Management through Quality Management Process (QMS), etc. Every management system has its own agendas; therefore all of them come up with their respective objectives and end deliverables. Difference in prime objectives, also effects the point of view required to assess the risks associated with each activity. An ISMS is the most suitable management practice to provide the secure and reliable approach for risk management in IT structure.

Different [1] methodologies and tools are proposed by many researchers for assessing the risks and control measures enabling enterprises to operate in a cost efficient manner with a known and acceptable level of business risk. The methodologies involve CCTA Risk Analysis and Management Methodology (CRAMM), Fault Tree Analysis (FTA), Failure Mode and Effect Criticality Analysis (FMECA) and Hazard and Operability Study (HazOp). These existing methods encounter all types of risks and fulfill all steps in the development of system and its maintenance. Most of the methodologies among the defined are qualitative.

The paper section II describes basic concepts involved. Section III defines different methodologies used for assessing and treatment of risks Section IV is related to the comparative analysis of Commercial and Strategic organization on the basis of risk assessment. . In section V proposed qualitative model is explained. Section VI contains the comparison between CRAMM and QRATM on the basis of basic steps involved in risk management. In Section VII the results shown which are collected by applying the proposed model in both Commercial and Strategic organization

2. Basic Concepts

There are some basic components involved in process of Risk management. The basic definitions of these factors are as follows

2.1 Asset

Asset is defined [9] as any "data, device, or other component of the environment that supports information-related activities, which can be affected in a manner that result in loss".

2.2 Vulnerability

Vulnerability [9] may be defined as "the probability that an asset will be unable to resist the actions of an intruder. Vulnerability exists when this probability exceeds a given threshold".

2.3 Threat

Threat is a potential cause of an unwanted incident, which may result in harm to a system or organization.

2.4 Risk

Risk is [10] the possibility of damage or loss, is described mostly in dependencies of threat and vulnerability, or impact and probability.

3 Risk Assessment Methodology

There are hundreds of techniques that can be adopted to calculate risk rating, which is an expression that is used to give an idea or scale of risk under observation. These techniques are mostly divided into three types of assessments;

Received October 19, 2010

1554-1010 $ 03.50 Dynamic Publishers, Inc.

3.1 Qualitative Assessment

Qualitative Risk assessment [2] [6] identifies the assets and resources risk by evaluating the magnitude of risk and probability of its occurrence and how often associated risk would be thriving in exploiting vulnerability. It prioritizes risks and identifies areas for immediate development in order to tackle the vulnerabilities. Based on this it becomes justifiable from financial perspective to invest in implementing preventive measures against identified risk.

In this method, ratings are defined in terms of characteristics and when compared, always most repeated or the characteristic of highest impact is considered to be the final answer. For example: Lowest, Low, High and Highest. A Combination of two "Low" and one "High" may result in selection of "Low" at the end. But a combination of two or even three "Low" but one "Highest" will always result in "highest" as the final answer, it being the one with maximum impact. Since rankings are descriptive and are based on judgments this may also result in some confusion like in a combination of "Highest" and "Lowest", which one will be preferred, it's highly reliable on experience of the person performing the assessment.

3.2 Quantitative Assessment

Quantitative assessment [2] [6] provides a measurement of the risk's magnitude, which can be used in the cost-benefit analysis of recommended controls. It assigns values to information, systems, processes, recovery costs, impact, and therefore risk, can be measured in terms of direct and indirect costs.

Ratings are defined in the form of numbers which actually represent "Qualities" of the risk being assessed. Numerical values can easily be added or multiplied therefore the resulting figure comes out as a numerical score which makes the comparison of two or more risks very easy. Which ever scores the highest is considered to be most critical. For example: "Lowest – 1", "Low – 2", "High – 3" and "Highest – 4". This methodology only requires a person who understands "when to assign which number" as a score. In most cases, following good practices, these grades are defined in detail so that anyone who wants to perform risk assessment can easily do so without any lengthy experience outside his/her own field. This is by far the most popular methodology due to its flexible nature and also due to the fact that "not everything can be measured in amounts of money".

3.3 Monetary Assessment

Monitory Assessment requires to evaluate assets / services in terms of their monetary value, it also involves monetary values of organization's value of goodwill (based on market standing and share prices, etc.) and value of information and agreements involved in the operational activities (contractual values of projects, etc.). In case of tangible assets, [2] their depreciations may also be considered. But this may be the most complex approach, but only applies to organizations with higher concerns over their profit earnings and expenses incurred.

Therefore, only commercial organizations go for this method, and strategic does not as their assets and operations are impossible to measure in terms of money.

All other methodologies are either based on these techniques or simply a combination of any two or all three. But all of these rely on solid facts of past activities before assessment criteria is fulfilled and considered for risk rating input.

4 Comparative Analysis of Risk Assessment in Strategic and Commercial Organizations

The organizations whether Commercial or Strategic using the same equipment and technology but the difference should be in their objectives. With the enhancement in technology immediate communication becomes the basic need of any organization but the way to communicate varies from organization to organization.

Before performing Risk Assessment of any organization and its practices, there is need to understand their objectives and operations. Following is a comparison between Risk Management of Strategic and Commercial Organizations; there is need to assess their similarities and differences for understanding of their risk assessment process.

Strategic Organization	**Commercial Organization**
Not-for-profit	Works for Profit
No Competition and not part of market as the services are unique and cannot be commercialized	Have to compete with competitors, therefore biggest threats are competitors and their activities that can affect their profits
Risks and their impacts can effect national causes and eventually can effect commercial setup as well	Risks and their impacts will affect organization's assets/resources and/or services only, and shall not effect strategic organizations
Information of all levels are not shared with anyone not concerned with the organization	Information is shared among public sectors and customers, to gain market trust
All the documents and information are classified to some level according to its nature and not open to public	There is no such strict compliance to the information as mostly it is for public
Less third party involvement	Links to the third party are important for better competition and profit earning

Table 1. Differences of Commercial and Strategic Organizations.

The Strategic organizations are more interested in achieving the confidentiality and integrity of the information rather than earning profit and commercializing them in the market. The basic aim of the Commercial organizations is to earn profit and remain popular in the market.

The similarities among the organizations involve the hierarchy, methodology and working environment according to the circumstances of the organization.

S.No.	Similarities
1	Use of assets is same, e.g. use of servers, workstations and applications remain the same, i.e. to perform operations required to fulfill organization's objectives
2	Human Resource perform using the assets / applications, using the universal methodologies defined by software developers and hardware designers
3	Threats and vulnerabilities are in most cases same
4	Loss or disclosure of critical information can have major effect on the existence of organization and its position in the region
5	All Legal requirements are applicable

Table 2. Similarities of Commercial and Strategic Organizations.

5 Risk Assessment Methodology

The basic steps for risk management are same but can be used in different scenarios according the environment and structure of the organization. These steps are identifying threats, vulnerabilities and risks and the measures to mitigate them. The goal of proposed model is to provide organizations with a qualitative approach to implement risk management process. The Strategic organization is considered not for profit organization but is based on providing secure and reliable information.

There are some heuristic values taken based on significant factors involved in identification of risk and calculating its rating value. The values are decided as per criteria of working environment and objectives of the organization. The values are divided to granular level so that the importance of each factor is properly utilized for calculation and identification of the risk value. Figure 1 shows the flow and steps of proposed model.

The proposed risk assessment model consists of following steps.

Step-1: Identification of Assets

Assets [4][3] can be defined as an organizations resource, data, device, service, or other component which supports information related activities and adds value to the information. The initial most important step is to identify the assets of the organization. Important assets involve hardware, software, interfaces and human resource.

An Information Asset [6] is defined as "Anything that has value to the organization and effects information by performing any one or more of the following; Storing, Disposing, Duplicating, Transferring and Processing"

There is need to identify the Information Assets among the assets of organization. An information asset in Table 3 is classified into five levels. The levels are defined on the basis of importance, usage and criticality of that asset.

Value in Terms of Priorities	Description	Numeric Value
Critical	Assets that affect external parties that are critical to high priority operations and their loss can have severe consequences	5
High	Assets that affect information that can only be shared among higher officials only (or related to highly critical operational activities)	4
Moderate	Assets that affect information that can only be shared within a single department and higher officials	3
Internal	Assets that affect information that can only be shared among selected departments	2
Common	Assets that affect public information, accessible to internal and external human resources	1

Table 3. Value of Information Asset

Step-2: Asset Evaluated Value

The assets [5] of the systems are categorized according to their importance in the organization. The assets are evaluated on the basis of Confidentiality, Integrity and Availability. The value is further prioritized according to the criticality of an asset.

Taking into account the security perspective the method for calculation of Asset value is same as defined in ISO 27001[7]. The formula to calculate the Asset Value is as follows

$$\text{Asset Value} = \text{Confidentiality}+\text{Integrity}+\text{Availability} \quad (1)$$

- **Confidentiality:** The ability to operate privately
- **Integrity:** The ability of detecting change/modification in the information
- **Availability:** Making the information accessible so that it could be used on demand by authorized entity

Step-3: Identification of Threat

Confidentiality, integrity, or availability of information or information systems could harm by the threats [5] [7]. These

threats can be characterized as the potential for agents exploiting vulnerability, which may harm the information or information system by unauthorized disclosure, misuse, alteration or destruction. Traditionally the sources of threat have been categorized as internal (malicious or incompetent employees, contractors, service providers, and former insiders) and external (criminals, recreational hackers, competitors, and terrorists). Identified agents may have different capabilities and motivations. These agents require the ways and techniques to mitigate the risks by focusing many elements of information. Agents may include the Natural and man-made disasters.

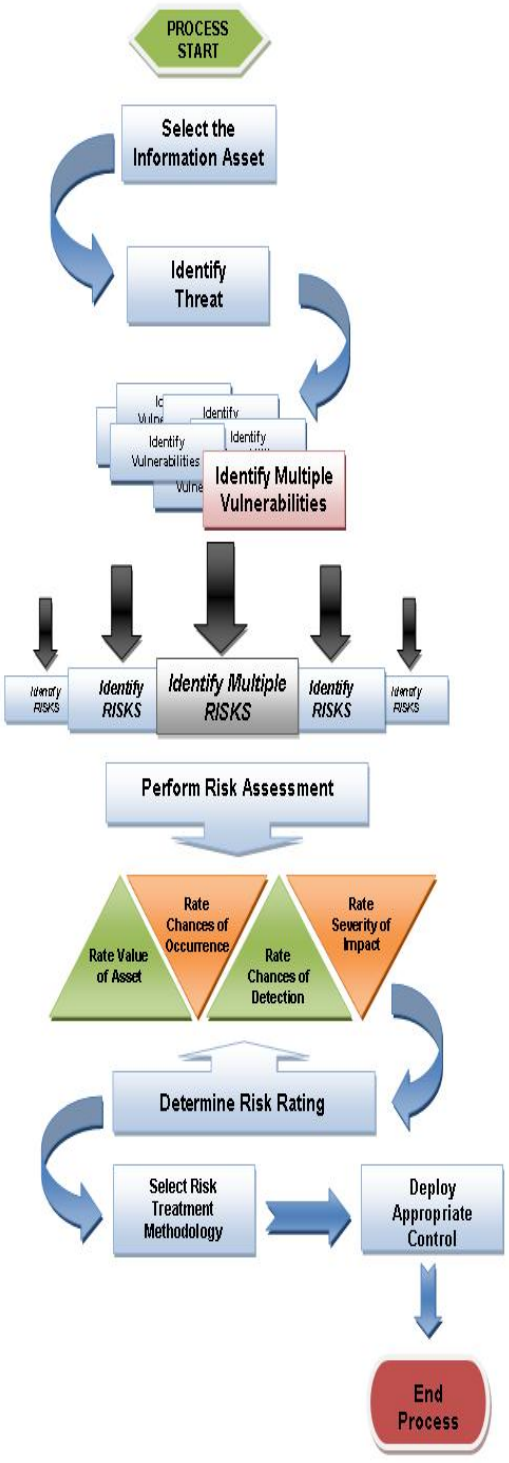

Figure 1. Proposed Risk Assessment and Treatment Model

Step-4: Identification of Vulnerabilities

Weaknesses in systems, control gaps are characterized as vulnerabilities [3] [5] [6], if these are exploited then could result in the unauthorized disclosure, misuse, alteration, or destruction of information or information systems. These are generally grouped as known and expected. Vulnerabilities discovered by testing or by reviewing the environment, knowledge of system weakness, knowledge of inadequate implementation and knowledge of personnel issue are the known vulnerabilities. Whereas the expected vulnerabilities are those that can reasonably be anticipated to arise in the future. This type of vulnerably may include un-patched software, new and unique attack methodologies that bypass current controls, employee and contractor failures to perform security duties satisfactorily, personnel turnover resulting in less experienced and knowledgeable staff, new technology introduced with security flaws, and failure to comply with policies and procedures. There are some vulnerabilities that may exist only for a short time until they are controlled, the risk assessment should consider the risk posed for the time period the vulnerability might exist.

Step-5: Identification of Risk

Risk identification [5] [6] ascertains what risks or hazards exist their characteristics, magnitude, duration, probability of occurrence and recurrence and possible outcomes and consequences. Precise and absolute risk identification is elementary for effective risk management. For managing risk efficiently, they must be identified foremost. During risk identification process, all possible risks need to be identified, rated and documented.

Most common risk identification techniques comprise brainstorming within stakeholders and working groups, surveys, evaluating experiential data and historical information.

Step-6: Performing Risk Assessment

Risk assessment is a process to analyze identified risks causing delays in design, production or delivery of the system. it might results adversely by affecting the system performance or amplifying program cost. Adopted approach is to assign values to identified risks according to its severity level.

The possibility of risk being occurred depends on the specific asset and its vulnerabilities making it exposed to the attacks [1]. The chances of occurrence are divided into categories according to probability of occurrence of risk being arise. The maximum likelihood of risk can occur once in a week and the minimum probability can be once in a year. The value varies between 1 and 5 as described in the table 4 according to the environment and how frequently a risk can be occurred. These values are heuristics and can be changed according to the working of organizations, its value vary among different organizations.

All the values for occurrence, detection and the impact of that risk are taken according to the working environment and methodology of strategic organizations.

Table 4 shows the chances of occurrence of the risk to any information asset.

Value in Terms of Priorities	Description	Numeric Value
Highest	Once in a week	5
High	Once in a month	4
Medium	Once in four months	3
Low	Twice in a year	2
Lowest	Once in a year	1

Table 4. Chances of Risk Occurrence

The chances to detect a risk are prioritized in the manner that a risk detected when it is about to happen has the highest priority with value 5 and the risk having lowest chances to be detected has a value 1. The probability of detection varies from 5 to 1, from the highest to the lowest.

The most important factor is that how strict the impact of a risk can be than the probability to occur and detecting its value. In formula 2, the impact is multiplied with sum of values of Information Assets, chances of occurrence and detection. The multiplication of severity with detection, occurrence and information asset value causes the greater change in differentiating the risks and its criticality; it shows the outcome of the threat. The severity is categorized in the manner that the most critical risk that can affect system the most has the highest value of 10 which effect the most critical assets loss in an organization and the risk having the lowest impact has value of 2 which effect only the common priority assets of the system. The other values are multiples of 2 and vary between the highest "10" and the lowest "2" value.

Table 5 shows the chances to detect the occurrence of risks.

Value in Terms of Priorities	Description	Numeric Value
Highest	Detected every time it's about to happen	5
High	Detected every time it happens	4
Medium	Detected only when effected system is under review	3
Low	Possible to detect on the basis of information received from a third party	2
Lowest	Not possible to detect unless it is occurring	1

Table 5. Chances of Risk Detection

Following formula is used to calculate the Risk rating of the specific Risk:

$$\text{Risk Rating} = [V + O + D] \times S \quad (2)$$

V: **V**alue of Information Asset
O: Chances of Risk **O**ccurrence
D: Chances of Risk **D**etection
S: **S**everity of Impact

Applying the formula when all the values of V, O, D and S are the highest i.e., 5, 5,5and 10 and the lowest value 1, 1, 1 and 2 respectively. The evaluated risk has the following values

Maximum Risk Rating = 150
Minimum Risk Rating = 6

The value of risk ranges between the maximum "150" and minimum "6" value. The calculated value shows the rating value of Risk and according to the value control measures are implemented to lessen probability of risk occurrence and its impact on system.

Table 6 represents the severity impact of the specific risk. The risk value is prioritized into 5 levels

Value in Terms of Priorities	Description	Numeric Value
Highest	Effects on Critical Priority Assets with site damage and possible human loss/injury	10
High	Effects on Critical Priority Assets	8
Moderate	Effects on High Priority Assets	6
Low	Effects on Internal or Moderate Priority Assets	4
Lowest	Effects on Common Priority Assets	2

Table 6. Severity Impact

Step-7: Risk Treatment

Risk treatment [2][5] is a process which identifies, assesses, chooses and implements options in order to avoid risk at sustainable levels. Some risks may be accepted with no further measures (low risks), but other risks may be accepted simply because there is no credible alternative but contingency actions needs to be developed in case they occur. Risk treatments incur mitigation of probability of the risk event or curtail the scope of the consequence to an acceptable level.

Step-8: Control Measure Adopted for Treatment

The control measures taken for the treatment of risk to the least level is important feature concerning the continuity of the working of assets in the organization. There are different recommended treatments defined on the basis of the working environment of the organization to minimize the affect or the chances of each risk. Different types of controls include [5] [6] preventive, detective, or corrective, and technical controls. Preventive controls act to minimize the probability of a risk to occur. Detective and corrective controls categorize damaging actions as they occur, to ease their termination, and to reduce damage.

6 Comparison with CRAMM

CRAMM is commonly used tool for Risk Management. The basic steps of risk management methodology are compared between the proposed technique and CRAMM. It is observed that an additional layer is defined in the proposed model for risk identification where as in CRAMM only threat analysis is done. The features to be integrated with CRAMM increase the information security by treating and avoidance of the risks toward critical information assets.

Table 7 shows the important factors related to Risk management. The comparison is made between CRAMM and QRATM with these factors. There is integration of some features in the CRAMM to improve the timely management and mitigation of risks.

Sr. #	Risk Assessment and Treatment Method	CRAMM	QRATM
1	Requirement Analysis of Organization	Yes	Yes
2	Asset Valuation	Yes	Yes
3	Identification of Threats	Yes	Yes
4	Classification of threats	Yes	No
4	Identification of Vulnerabilities	Yes	Yes
5	Identification of Risks	Yes	Yes
6	Probability of Occurrence and Detection of Risk	No	Yes
7	Treatment Method	No	Yes
8	Countermeasure against that Risk	Yes	Yes

Table 7. Comparison with CRAMM

QRATM provides more factors for risk assessment and treatment as compared to CRAMM.

The integration of QRTAM with CRAMM in the form of flow diagram is shown in Figure 2.

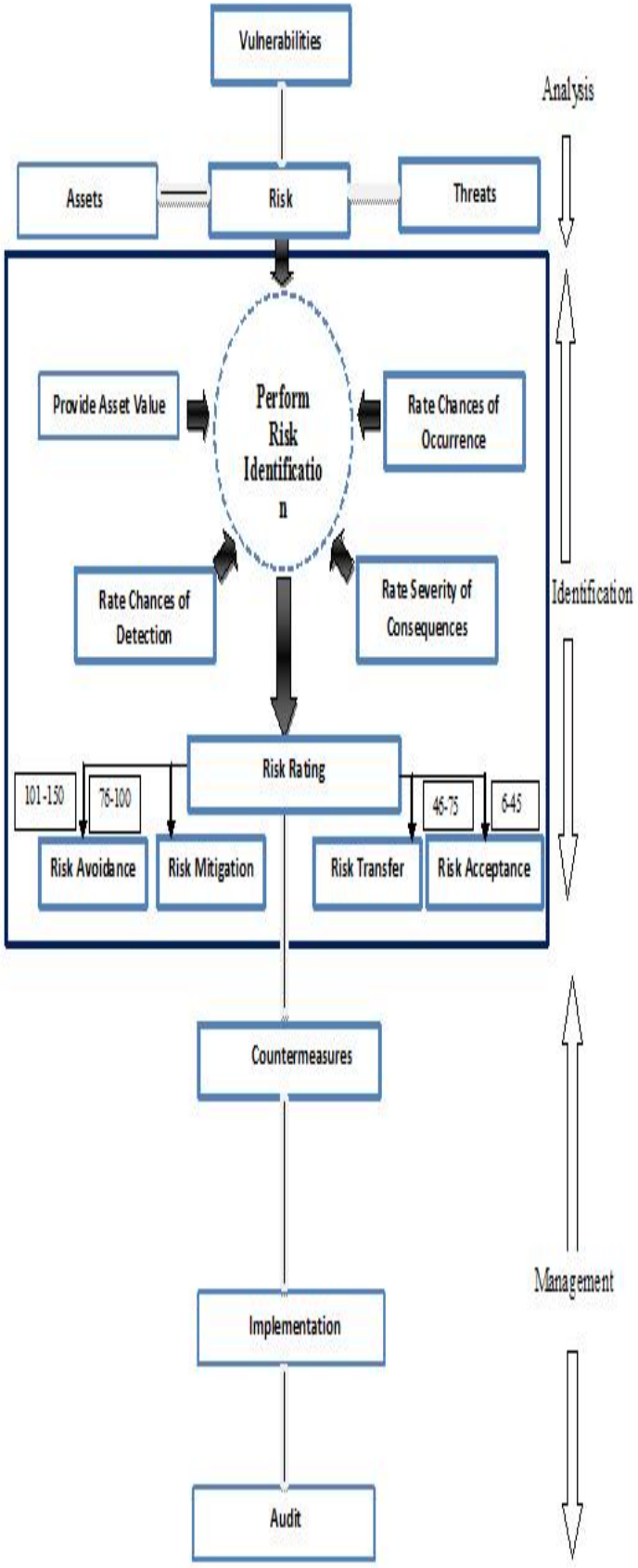

Figure 2. Integration of QRATM with CRAMM

7 Advantages of QRATM

With integrating the new factors into CRAMM following benefits can be achieved by the organization using this technique:

1. The risks are identified to granular level in the initial stage.
2. The treatment and control measure for the risk is already taken in account.
3. The chances of whole failure decreased to minimum level.
4. The impact of the risks segregate occurrence of the most likely and unlikely risks.

8 Results

The proposed model is applied in both Commercial and Strategic organizations. It is observed that on the basis of their objectives the resulted value of Risk rating for same Risk type is different.

Figure 3 shows the risk rating in Strategic organization, where red color show that risk is Critical, green is high priority, blue moderate and white are low or acceptable risks. The Y-axis contains the numeric value of risk while on X-axis there is name of specific risk to the asset.

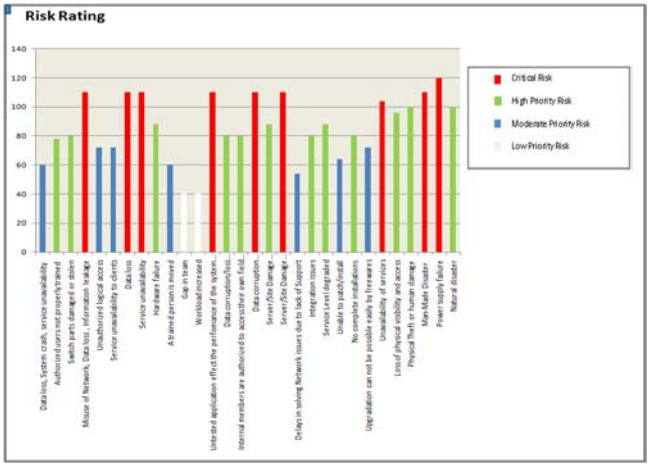

Figure 3. Risk Rating of Strategic Organization(XYZ)

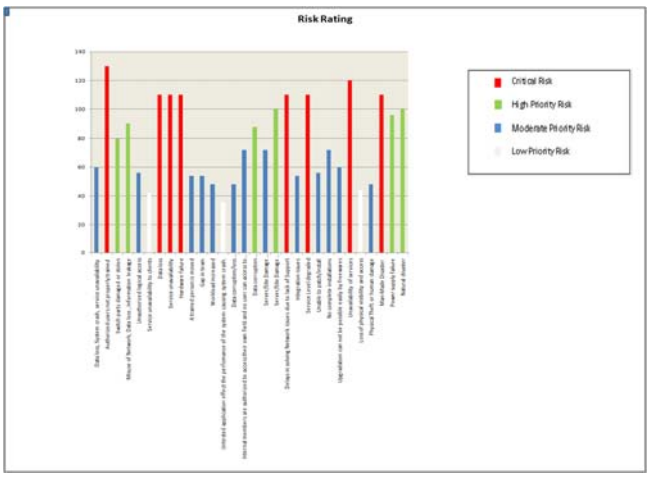

Figure 4. Risk Rating of Commercial Organization (ABC)

Figure 4 shows the risk rating in commercial organization, where red color show that risk is critical, green is high priority, blue moderate and white are low or acceptable risks. The Y-axis contains the numeric value of risk while on X-axis shows the specific risk to the asset.

9 Conclusion

A qualitative approach is easy to implement in any organization because there is no complex calculations and monetary values involved. It provides the guidelines to overcome with the risks in order to keep the system working in a continuous manner. All the steps defined in the proposed approach, make this model to be used in any organization either it is strategic or commercial. An important factor is to find out the basic objective of any organization on the basis of which the requirement can be fulfilled. The above mentioned model can be exercised in both Strategic as well as Commercial organization, depending on their qualitative objectives for Risk Assessment and Treatment.

Acknowledgment

I thank Allah Almighty for the success and completion of this research work. I gratefully acknowledge the encouragement and support of my advisors, friends, especially my parents, brother and sisters. They made available their support in a number of ways and have been a great mentor always providing me with the much needed encouragement and thoughtful direction.

I am thankful to Farhan Haider, Ali Nawaz and Rizwan Ahmed for providing me help regarding the comparative study of commercial and strategic organizations.

I would also like to convey thanks to the National University of Science and Technology (NUST), College of E & ME and Faculty of Department of Computer Engineering for providing me the laboratory facilities for my research work.

10 Recommendations

The further stage after Risk assessment and treatment methodology is business continuity planning. In such case the services of the information system are considered with assets as well and then the disaster recovery. Every organization must need to do disaster recovery in order to have secure system and methodology which would be of great help in the long run. The most important is making your system information security management system through complying with ISO 27001 by implementing all the phases including risk assessment and treatment, business continuity and disaster recovery plan.

References

[1] Jan Øyvind Aagedal, Folker den Braber, Theo Dimitrakos, Bjørn Axel Gran, Dimitris Raptis, Ketil Stølen, *"Model-based Risk Assessment to Improve Enterprise Security"*, Enterprise Distributed Object Computing Conference (EDOC'02), Proceedings of the Sixth International IEEE 2002.

[2] Ajith Abraham1, Crina Grosan1 2, Vaclav Snasel, *"Programming Risk Assessment Models for Online Security Evaluation Systems"*, 2009 IEEE

[3] James W. Freeman (CISSP), Thomas C. Dm (CISSP), Richard B. Neely (CISSP), *"Risk Assessment for Large Heterogeneous Systems"*, 1997 IEEE

[4] http://www.ffiec.gov/ffiecinfobase/booklets/information_security/03_info_sec_strategy.htm

[5] Gray Stoneburner, Alice Goguen, and Alexis Feringa, NIST Technology Administration, U.S. Department of commerce. Risk Management guide for Information technology system.
[6] Final Draft, International Standard, ISO/IEC 27001:2005
[7] Javaria Sana, Dr. M Younus Javed, *"Comparative analysis of Commercial and Strategic organization with Risk Assessment and Treatment Model"*, Proceedings of the "International Conference on Compuetr networks and System security", ICCNSS 2010
[8] Liu Ren-hui and Zhai Feng-yong *"Model Identification of Risk Management System"*, Proceedings of IEEE 2008.
[9] A Qualitative Risk Analysis and Management Tool - CRAMM. SANS Institute InfoSec Reading Room

Author Biographies

Javaria Sana was born in Mianwali Pakistan on 25 Dec 1982. She had completed her initial education from Abdul Razzaq Fazaiya College, Mianwali and then did Bechalors of Engineering in Software Engineering from APCOMS Rawalpindi. She had done MS in Software Engineering from College of Electrical and Mechanical Engineering, NUST Pakistan. This research work is contribution towards the completion of her MS Degree. Her areas of interests include Information Security, Network Security and Information Assurance.

M Hasan Islam PhD, ISO 27001 Lead Auditor is a faculty member in Department of Electrical and Computer Engineering, at Centre for Advanced Studies in Engineering (CASE), Islamabad, Pakistan. He has a vast teaching and industry experience. His areas of research are networks, wireless and ad hoc networks, management and performance analysis, design and implementation of security policies. Dr. Hasan has been a key note speaker and author of a number of research papers published both locally and internationally acclaimed conferences/journals.

Bushra Fayyaz born in Saudi Arabia on 20 Sep 1984. She had completed her early education in Saudi Arabia and then completed BESE from Fatima Jinnah women University Rawalpindi. She had done MS in Software engineering from COMSATS Islamabad, Pakistan. Her areas of interests include Information Security, network security and Information Assurance.