CORE
Metadata, citation and similar papers at core.ac.uk
Provided by International Institute for Science, Technology and Education (IISTE): E-Journals

Mathematical Theory and Modeling
ISSN 2224-5804 (Paper) ISSN 2225-0522 (Online)
Vol.3, No.6, 2013-Selected from International Conference on Recent Trends in Applied Sciences with Engineering Applications
www.iiste.org

Optimization of Different Objective Function in Risk Assessment System

SHWETA SINGH
Department of Mathematics, Radharaman Institute of Tech., & Science, Bhopal (M.P.)
Singh84_s@rediffmail.com
G.C. DUBEY
Department of Mathematics, Govt. MGM College,Itarsi (M.P.)
Gcd.1951@gmail.com
RAJESH SHRIVASTAVA
Department of Mathematics, Govt. Benazir College,Bhopal, (M.P.)
Rajeshraju0101@rediffmail.com

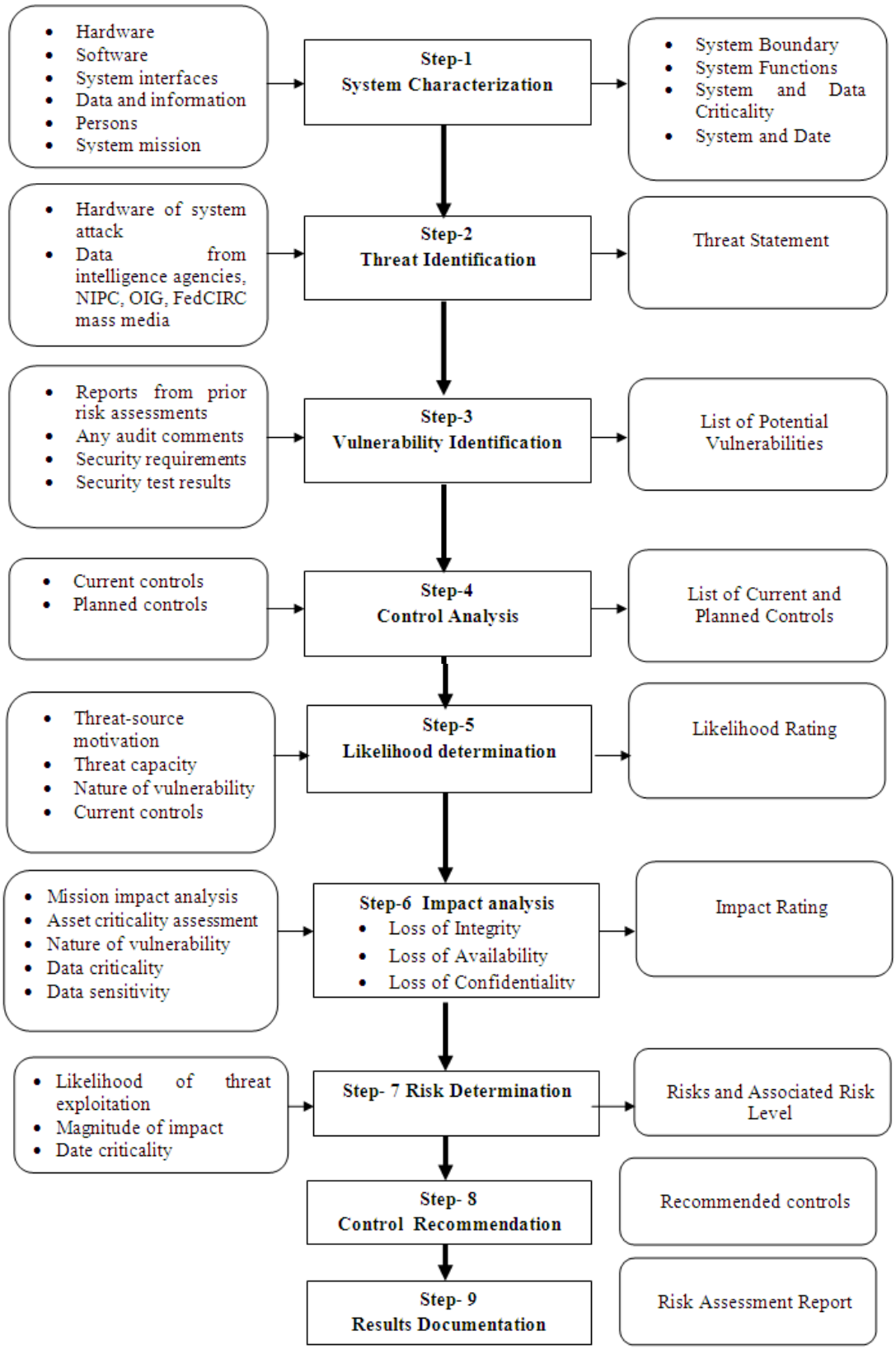
Abstract
This paper proposes a new definition and conceptual framework for Risk assessment system. Risk assessment is the first process in the risk management methodology Organizations use risk system to determine the extent of the potential threat and the risk associated with an IT system throughout its SDLC. The output of this process helps to identify appropriate controls for eliminating risk and to determine the likelihood of a future adverse event. In this paper we will also discuss the Quantitative versus Qualitative Assessment, their advantage and disadvantages, while conducting the impact analysis. Once all the objective function have be optimized and completed, the results should be documented in an official report. This expanded view of Risk assessment emphasis the double role of risk management instruments, protecting basic livelihood as well as promoting risk taking and protecting basic livelihood.
Keywords - Risk assessment, Risk Management, SDLC (System Development life cycle optimization)

Introduction

Due to technical advancement and needs of the person, the life cycle of product have been shortened. With the customer needs the functional for corporate should be quickly improved in quality for corporate survival. There for the risk factors which occurs during the product development need to be managed in project planning and risk management system. Risk is a function of the likelihood of a given threat-source's a exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization[1][2] The risk assessment methodology encompasses nine primary steps, which is described below:

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

Figure 1 Risk Assessment Methodology Flow chart



STEP 1- SYSTEM CHARACTERIZATION

In assessing risks for an IT system, the first step is to define the scope of the effort. In this step, the boundaries of the IT system are identified, along with the resources and the information that constitute the system.

1.1 System-Related Information

Indentifying risk for an IT system requires a keen understanding of the system's processing environment. The person or persons who conduct the risk assessment must therefore first colled system-related information which is usually classified as follows:

- Hardware
- Software
- System interfaces (e.g. internal and external connectivity)
- Data and information
- Persons who support and use the IT system
- System mission (e.g., the processes performed by the IT system)
- System and data criticality (e.g., the system's value or importance to an organization).
- System and data sensitivity.

1.2 Information-Gathering Techniques

Any, or a combination, of the following techniques can be used in gathering information relevant to the IT system within the its operational boundary[5].

- Questionnaire
- On-site Interviews.
- Document Review
- Use of Automated Scanning Tool.

STEP 2- THREAT IDENTIFICATION

A threat is the potential for a particular threat-source to successfully exercise a particular vulnerability. A vulnerability is a weakness that can be accidentally triggered or intentionally exploited. A threat-source does not present a risk when there is no vulnerabilitiy that can be exercised.

2.1 Threat-Source Identification

The goal of this step is to identify the potential threat-sources and compile a threat statement listing potential threat-sources that are applicable to the IT system being evaluated.

2.2 Motivation and Threat Actions

Motivation and the resources for carrying outan attack make humans potentially dangerous threat-sources.

This information will be useful to organizations studying their human threat environments and customizing their human threat statements.

STEP 3- VULNERABILITY IDENTIFICATION

The analysis of the threat to an IT system must include an analysis of the vulnerabilities associated with the system environment. The goal of this step is to develop a list of system vulnerabilities (flaws or weaknesses) that could be exploited by the potential threat-sources.

3.1 Vulnerability Sources

The technical and nontechnical vulnerabilities associated with an IT system's processing environment can be identified via the information-gathering techniques described in.

3.2 System Security Testing

Proactive methods, employing system testing, can be used to identify system vulnerabilities effieciently, depending on the criticality of the IT system and available resources.

- Automated vulnerability scanning tool.
- Security test and evaluation (ST & E)
- Penetration testing.

3.3 Development of Security Requirements Checklist

During this step, the risk assessment personnel determine whether the security requirements stipulated for the IT system and collected during system characterization are being met by existing or planned security controls.

- Management
- Operational
- Technical

STEP 4- CONTROL ANALYSIS

The goal of this step is to analyze the controls that have been implemented, or are planned for implementation, by the organization to minimize or eliminate the likelihood (or probability) of a threat's exercising a system vulnerability.

STEP 5- LIKELIHOOD DETERMINATION

To derive an overall likelihood rating that indicates the probability that a potential vulnerability may be exercised within the construct of the associated threat environment, the following governing factors must be considered:

- Threat-source motivation and capability
- Nature of the vulnerability
- Existence and effectiveness of current controls.

STEP 6- IMPACT ANALYSIS

The Next major step in measureing level of risk is to determine the adverse impact resulting from a successful threat exercise of a vulnerability. Before beginning the impact analysis, it is necessary to obtain the following necessary informationg as discussed:

- System mission (e.g., the processes performed by the IT system)
- System and data criticality (e.g., the system's value or importance to an organization).
- System and data sensitivity.

STEP 7- RISK DETERMINATION

The purpose of this step is to assess the level of risk to the IT system. The determination of risk for a particualar threat/vulnerability pair can be expressed as a function of-

- The likelihood of a given threat-source's attempting to excrexcise a given vulnerability.
- The magnitude of the impact should a threat-source successfully exercise the vulnerability.
- The adequacy of planned or existing security controls for reducing or eliminating risk.

Table-1
Risk-Level Matrix

Threat Likelihood	Impact		
	Low (10)	Medium (50)	High (100)
High (1.0)	Low 10X1.0=10	Medium 50X1.0=50	High 100X1.0=100
Medium (0.5)	Low 10X0.5=5	Medium 50X0.5=25	High 100X0.5=50
Low (0.1)	Low 10X0.1=1	Medium 50X0.1=5	High 100X0.1=10

Risk Scale : High (>50 to 100); Medium (>10 to 50); Low (1 to 10)[8]

Table 2
Risk Scale and Necessary Actions

Risk Level	Risk Description and Necessary Actions
High	It an observation or finding is evaluated as a high risk, there is a strong need for corrective measures. An existing system may continue ot operate, but a corrective action plan must be put in place as soon as possible.
Medium	If an observation is rated as medium risk, corrective actions are neede and a plan must be developed to incorporate these actions within a reasonable period of time.
Low	If an observation is described as low risk the system's DAA must determine whether corrective actions are still required or decide to accept the risk

STEP 8 - CONTROL RECOMMENDATIONS

During this step of the process, controls that could mitigate or eliminate the identified risks, as appropriate to the organization's operation, are provided. The goal of the recommended controls is to reduce the level of risk to the IT system and its data to an acceptable level. The following factors should be considered in recommending control and alternative solutions to minimize or eliminate identified risks:

- Effectiveness of recommended options (e.g. system compatibility)
- Legislation and regulation
- Organizational policy
- Operational impact
- Safety and reliability

STEP 9 - RESULTS DOCUMENTATION

Once the risk assessment has been completed (threat-sources and vulnerabilities identified, risks assessed, and recommended controls provided), the results should be documented in an official report or briefing.

CONCLUSION

A risk assessment report is a management report that helps senior management, the mission owners, make decisions on policy, procedural, budget and system operational and management changes. Unlike an audit or investigation report, which looks for wrongdoing, a risk assessment report should not be presented in an accusatory manner but as a systematic and analytical approach to assessing risk so that senior mmanagement will understand the risks and allocate resources to reduce and correct potential losses. For this reason, some people prefer to address the threat/vulnerability pairs as observations instead of findings in the risk assessment report.

References -

1. J. Coppendale, "Manage risk in product and process development and avoid unpleasant surprises" Journal of Engineering Management, Vol.5, pp.33-38
2. L.P. Cooper, " A research agenda to reduce risk in new product development through knowledge management: a practitioner perspective," Journal of Engineering and Technology Management, 2003
3. P.K. Dey, " Project Risk Management : A combined Analytic Hierarchy process and decision tree Approach," cost Engineering, 44,2002.
4. H.G. Choi and J.O. Ahn, "Risk analysis models and risk degree determination in new product development: A case study" Journal of Engineering and Technology Management, pp. 110-114. 2010.
5. D.W. Choi, J.S.Kim, and H.G. Choi, "Determination of Integrated Risk degrees in product development project," Proceeding of the world congress on Engineering and computer science 2009, Vol.II, 2009.

This academic article was published by The International Institute for Science, Technology and Education (IISTE). The IISTE is a pioneer in the Open Access Publishing service based in the U.S. and Europe. The aim of the institute is Accelerating Global Knowledge Sharing.

More information about the publisher can be found in the IISTE's homepage: http://www.iiste.org

CALL FOR PAPERS

The IISTE is currently hosting more than 30 peer-reviewed academic journals and collaborating with academic institutions around the world. There's no deadline for submission. **Prospective authors of IISTE journals can find the submission instruction on the following page:** http://www.iiste.org/Journals/

The IISTE editorial team promises to the review and publish all the qualified submissions in a **fast** manner. All the journals articles are available online to the readers all over the world without financial, legal, or technical barriers other than those inseparable from gaining access to the internet itself. Printed version of the journals is also available upon request of readers and authors.

IISTE Knowledge Sharing Partners

EBSCO, Index Copernicus, Ulrich's Periodicals Directory, JournalTOCS, PKP Open Archives Harvester, Bielefeld Academic Search Engine, Elektronische Zeitschriftenbibliothek EZB, Open J-Gate, OCLC WorldCat, Universe Digtial Library , NewJour, Google Scholar