Qualitative Risk Assessment and Treatment

By

JAVARIA SANA

(2006-NUST-MS PhD-CSE (E)-23)

Submitted to the Department of Computer Engineering
in partial fulfillment of the requirements for the degree of

Master of Science
in
Computer Software Engineering

Thesis Advisor

Dr. Muhammad Younus Javed

MS-CSE-6
College of Electrical & Mechanical Engineering
National University of Sciences and Technology
2010

Acknowledgements

I thank Almighty Allah for the successful completion of my thesis. I gratefully acknowledge the encouragement and support of my Advisor Dr. Muhammad Younus Javed. He has made available his support in a number of ways and has been a great mentor always providing me with the much needed encouragement and thoughtful direction.

I am indebted to Mr. Farhan Haider and Mr. Ali Nawaz for their support and confidence.

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 financial means and laboratory facilities for my research work.

My parents, my grand parents (late), brother and sisters are mentioned last to emphasize the special nature of their tremendous support and patience all through my candidature. And also wishes to express love and gratitude for their understanding & endless love, through the duration of my studies and completion of the project.

Dedication

I dedicated this thesis in the honour of my parents, my brother and my sisters who always supported me and prayed for my success

Abstract

In most recent times, intensification in the information technology, by establishing large scale strategic environments, is at the maximum; whereas computing tainted to a purely networked milieu. These technical enhancements tackled all logical tiers, however, did not induce augmentation in means and aspects of information protection, especially for larger scale networks. Though, there has been considerable research on different sparse issues like secure routing, secure message exchange, authentication, and trusted computing technologies, to guard against various threats and attacks, but there is no appreciable research targeted at the risk analysis of these larger networks, concentrating more on different parameters involved in strategic environments.

Risk analysis, analytical identification and assessment methodology for different risk factors, can plays a vital role for the protection of strategic environments. This research will envisage comparative scrutiny of Risk Analysis procedure in strategic and commercial organization and creation of a comprehensive and elaborated Risk Model for strategic environments, as well. These design models will be explicated by security rules and policies, providing aid in implementation of the risk analysis model for large sub-systems.

Table of Contents

Acknowledgements i

Dedication ii

Abstract iii

List of Figures vii

List of Tables viii

1 CHAPTER 1: INTRODUCTION 1

1.1 Historical Background of Risk Analysis 2
1.1.1 Problem Statement 3
1.1.2 Breakdown of Report 3

2 CHAPTER 2: EXISTING METHODOLOGIES 4

2.1 CRAMM 4
2.1.1 Introduction 4
2.1.2 Description 5
2.2 Canadian TRA Methodology 7
2.2.1 Using TRA in Risk Management 8
2.2.2 Risk Management Tools 9
2.3 US Model 10
2.3.1 Introduction 10
2.3.2 Objective 11
2.3.3 Basic Risk Methodology 11
2.3.3.1 Risk Assessment 11
2.4 Czech Methodology 16
2.5 Spanish Method MAGERIT 18
2.5.1 Assets 18
2.5.2 Threats 19
2.5.3 Determination of the Impact 20
2.5.3.1 Accumulated Impact 20
2.5.3.2 Deflected Impact 21
2.5.3.3 Aggregation of Impact Values 21
2.5.4 Safeguards 21
2.5.4.1 Reducing the Frequency of Threats 22
2.5.4.2 Damage Limitation 22
2.5.5 Residual Impact 23
2.5.6 Residual Risk 23
2.6 BEATO 23

3 CHAPTER 3: RISK MANAGEMENT 25

3.1 Strategic Organization 25
3.2 Commercial Organization 25
3.3 Asset 25
3.4 Information Asset 26
3.5 Threat 26
3.6 Vulnerability 26
3.7 Risk 26
3.8 Risk Analysis 26
3.9 Risk Assessment 27
3.10 Risk Treatment 27
3.11 Risk Management 27
3.12 Business Continuity Plan 27
3.13 Disaster Recovery Plan 28
3.14 Risk Management 28
3.14.1 Objective of Risk Management 28
3.14.2 Principles of Risk Management 29
3.14.3 Risk Management Phenomenon 29
3.15 Risk Management And System Development Life Cycle(SDLC) 31
3.16 Risk Assessment 34
3.17 Risk Assessment Methodology 35
3.17.1 Qualitative Assessment 36
3.17.1.1 Preliminary Risk Analysis 36
3.17.1.2 Hazard and Operability studies (HAZOP) 37
3.17.1.3 Failure Mode and Effects Analysis (FMEA/FMECA) 37
3.17.2 Quantifiable Assessment 38
3.17.3 Monetary Assessment 39
3.17.4 Probabilistic Assessment 39
3.18 Benefits of Risk Assessment 38
3.18.1 Cost Justification 38
3.18.2 Productivity Audit/Review Savings 39
3.18.3 Breaking Barriers, Business relationships 39
3.18.4 Self Analysis 39
3.18.5 Security Awareness 39
3.18.6 Targeting of Security 42
3.18.7 Baseline Security and Policy 42
3.18.8 Consistency 42
3.18.9 Communication 42
3.19 Risk Management Failure 43

4 CHAPTER 4: COMPARITIVE ANALYSIS AND PROPOSED MODEL 45

4.1 Comparative Analysis of Risk Assessment in Strategic and Commercial Organizations 42
4.2 Proposed Risk Assessment and Treatment model 47
4.2.1 Identification of Assets 47
4.2.2 Asset Evaluated Value 48
4.2.3 Identification of Threat 47
4.2.4 Identification of Vulnerabilities 48
4.2.5 Identification of Risk 49
4.2.6 Performing Risk Assessment 53
4.2.7 Risk Treatment 56
4.2.8 Control Measure Adopted for Treatment 585

5 CHAPTER 5: APPLICATION AND RESULTS 57

5.1 Application of Tool QRATM…….....57
5.2 Results……58

6 CHAPTER 6: CONCLUSION AND FUTURE WORK 64

6.1 Conclusion……64
6.2 Future Work…….65

References 66

List of Figures

Figure 2.1 CRAMM 5

Figure 2.2 Risk Management Model 10

Figure 2.3 Risk Assessment Methodology Flow Chart 13

Figure 2.3 MAGERIT Main Steps.. 19

Figure 2.4 MAGERIT Main Steps including Safegaurds.. 22

Figure 3.1 Risk Analysis in Development Cycle.. 32

Figure 4.1 Proposed Risk Assessment and Treatment Model 49

Figure 5.1 QRATM Analysis Phase 57

Figure 5.2 QRATM Risk Identification and Assessment Phase...................................... 57

Figure 5.3 QRATM Risk Treatment Phase 58

Figure 5.4 QRATM Result Sheet……………………………………………………...58

Figure 5.5 QRATM Analysis Chart…………………………………………………...59

Figure 5.6 Integration with CRAMM…………………..……………………………...60

Figure 5.7 Average Value Graph……………………….……………………………..62

Figure 5.8 Defense Organization Risk Rating…………………………….…………..63

Figure 5.9 Commercial Organization Risk Rating……………………………….……...63

List of Tables

Table 2.1: Likelihood Definitions.. 14

Table 2.2: Magnitude of Impact Definitions... 15

Table 2.3: Frequency Table 20

Table 3.1: Management Practices and Probable risk... 29

Table 3.2: Risk Management and SDLC... 34

Table 4.1 : Similarities of Strategic and Commercial Organization................................. 45

Table 4.2 : Differences of Strategic and Commercial Organization................................. 46

Table 4.3: Value of Information Asset 47

Table 4.4: Threat Types.. 48

Table 4.5: Chances of Risk Occurrence.. 54

Table 4.6: Chances of Risk Detection... 54

Table 4.7: Severity Impact... 52

Table 5.1 QRATM vs CRAMM……………………..………………………………..59

Table 5.2 Risk Rating factors values…….……………..………………………………..61

Table 5.3 Risk Value Matrix………….……………..………………………………..61

CHAPTER 1: INTRODUCTION

Today's highly connected IT infrastructures exist in an environment that is increasingly hostile. Attacks [14] are being mounted with increasing frequency and are demanding ever shorter reaction times. Often, organizations are unable to react to new security threats before their business is impacted. Managing the security of their infrastructures and the business value that those infrastructures deliver has become a primary concern for IT departments.

An effective risk management process [6] is an important component of a successful IT security program. The principal goal of an organization’s risk management process should be to protect the organization and its ability to perform their mission, not just its IT assets. Therefore, the risk management process should not be treated primarily as a technical function carried out by the IT experts who operate and manage the IT system, but as an essential management function of the organization.

An adequate assessment identifies the value and sensitivity of information and system components and then balances that knowledge with the exposure from threats and vulnerabilities. A risk assessment is a pre-requisite to the formation of strategies that guide the institution as it develops, implements, tests, and maintains its information systems security posture. An initial risk assessment may involve a significant one-time effort, but the risk assessment process should be an ongoing part of the information security program. Risk assessments for most industries focus only on the risk to the business entity. Financial institutions must also consider the risk to their customers’ information.

Risk assessments should identify, quantify, and prioritize risks against criteria for risk acceptance and objectives relevant to the organization. The results should guide and determine the appropriate management action and priorities for managing information security risks and for implementing controls selected to protect against these risks. The process of assessing risks and selecting controls may need to be performed a number of times to cover different parts of the organization or individual information systems [11]. Risk assessments should also be performed periodically to address changes in the security requirements and in the risk situation, e.g. in the assets, threats, vulnerabilities, impacts, the risk evaluation, and when significant changes occur. These risk assessments should be undertaken in a methodical manner capable of producing comparable and reproducible results.

The scope [11] of a risk assessment can be either the whole organization, parts of the organization, an individual information system, specific system components, or services where this is practicable, realistic, and helpful

For each of the risks identified following the risk assessment a risk treatment decision needs to be made. Possible options for risk treatment include:

- Applying appropriate controls to reduce the risks
- Knowingly and objectively accepting risks, providing they clearly satisfy the organization's policy and criteria for risk acceptance;
- Avoiding risks by not allowing actions that would cause the risks to occur;
- Transferring the associated risks to other parties, e.g. insurers or supplier [6]

1.1 Historical Background of Risk Analysis

Historical perspective [15] on risk analysis applications in society was given by Covello and Mumpower (1985). Around 3200 B.C. in the Tigris-Euphrates valley, a group called Asipu served as risk analysis consultants for people making risky, uncertain, or difficult decisions Greeks and Romans observed causal relationships between exposure and disease: Hippocrates (4th century B.C.) correlated occurrence of diseases with environmental exposures; Vitruvious (1st century B.C.) noticed lead toxicity; and Agricola (16th century A.D.) noticed the correlation between occupational exposure to mining and health.

Modern risk analysis has roots in probability theory and the development of scientific methods for identifying causal links between adverse health effects and different types of hazardous activities: Blaise Pascal introduced the probability theory in 1657; Edmond Halley proposed life-expectancy tables in 1693; and in 1792, Pierre Simon de LaPlace developed a true prototype of modern quantitative risk analysis with his calculations of the probability of death with and without smallpox vaccination. With the rise of capitalism, money use, and interest rates, there was an increased use of mathematical methods dealing with probabilities and risks. For example, the risk of dying was calculated for insurance purposes (life-expectancy tables). Physicians in the Middle Ages also observed a correlation between exposures to chemicals or agents and health: John Evelyn (1620–1706) noticed that smoke in London caused respiratory problems. He also noticed correlation of scrotal cancer with occupational exposures to soot in chimney sweeps.

1.1.1 Problem Statement

“To determine the Comparative Analysis of Strategic and Commercial Organization and propose Qualitative Risk Assessment and Treatment Model for Strategic organization”

1.1.2 Breakdown of Report

Chapter 1 is a brief introduction of risk assessment, it importance in any organization and the problem statement. Chapter 2 contains the basic concepts, definitions and explanation related to risk management. Risk management also involves assessment and treatment and evaluation of risks. Chapter 3 includes the comparative analysis of risk assessment between strategic and commercial organization through their similarities and differences. A new proposed model is developed for performing risk assessment and treatment for strategic organization. Chapter 5 is conclusion and recommendation.

CHAPTER 2: EXISTING METHODOLOGIES

2.1 CRAMM

2.1.1 Introduction

CRAMM (CCTA Risk Analysis and Management Method) was created in 1987 by the Central Computing and Telecommunications Agency (CCTA) of the United Kingdom government. CRAMM is developed to provide the following:

1) A sound approach to identifying threats and vulnerabilities, and thus being able to establish a sound basis for identifying and stating risks
2) A more justifiable approach for management to understand risks
3) A basis for potential savings, in terms of the cost of security; and
4) A sound approach to improve levels of information and supporting system assets protection.

CRAMM [19] is more of a qualitative methodology than a quantitative methodology and, in broad terms, treats security risk assessment as an evaluation of the risks, and security risk management as the identification of the countermeasures to combat the risks. All aspects of security are addressed within the methodology; namely, personnel security, physical security and security of information. It can handle deliberate and accidental threats, and encompasses existing UK government security policy and guidance. For NATO, a NATO profile has been developed, based on NATO security policy and supporting directives and guidance in order to make the tool easier to use and more specifically tailored to NATO CIS. The methodology allows to use the tool to establish a baseline of information for an organisation or project at any time during its life-cycle, and provides a comprehensive “what-if” capability. This allows to model different scenarios, to assess the impact of changes in a system environment, or changes in policy and directives. It also provides a capability for follow-up reviews, using the previously established baseline of information.

2.1.2 Description

There are three fundamental stages to a CRAMM review, which correspond to the stages identified in the current NATO security risk assessment guidance and are, in broad terms, the following:

1) Stage one – Assessing the value of the information, and identifying the assets which support the business process
2) Stage two – Identifying what threats may affect the system and how vulnerable is the system to those threats; arriving at a conclusion about the risks
3) Stage three – Identifying how the risks can be countered, including what improvements are required to existing control measures

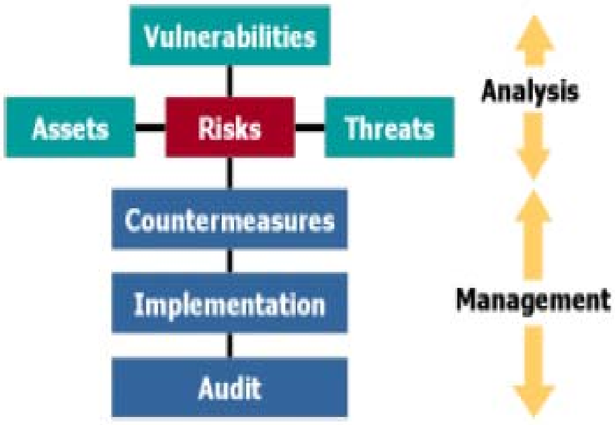


Figure 2.1. CRAMM [19]

Between each stage, there is the capability to produce comprehensive management reports, and conduct management reviews to ensure that the baseline of information is valid.

In stage one, at the start, it is important to identify the purpose of the CRAMM review, where the boundaries of the review are, and the schedule for the review. Equally important is the establishment of a baseline questionnaire (which the tool provides) from which you establish all the information about the physical and data assets. From this, you build up asset models, which show the relationship between data assets and those assets which support those data assets (for example, a computer room and its hardware).

The next step is to apply a valuation to the assets; data assets are valued in terms of impact of disclosure, modification, unavailability and destruction (this is qualitative information based on interviews with the users of information); physical assets are valued in terms of their replacement cost (quantitative information). At the end of this stage, it is recommended to carry out a management review to ensure that you have a sound baseline of information, before moving forward to the next stage. The stage 1 management review helps ensure at an early stage in the risk management process that there is agreement between the operational and security accreditation authorities as to the assets to be protected, and their value to the organization.

In stage two, you move into the threat and vulnerability assessment. The types of threat that are addressed include the following:

1) Logical threats – For example, hacking, unauthorized use of an application, and malicious software;
2) Communications threats – For example, communications infiltration, and mis-routing;
3) The threat of technical failures to communications and information systems hardware and software;
4) Errors by people – For example, system management errors, or errors by users; and
5) Physical threats – For example, theft, willful damage, terrorism, fire, water damage, and natural disasters.

The tool contains a built-in, very extensive library of potential threats and vulnerabilities. The threats can either be based on specific knowledge about previous security incidents, or on generic information.

The vulnerabilities are based on an understanding of the functions and capabilities that are available within the system environment. The threat and vulnerability assessment arrives at qualitative statements for the threats (in terms of very low, low, medium, high, and very high) and vulnerabilities (in terms of low, medium and high).

The next step is to derive measures of risk, and these are derived from a combination of the threat, the vulnerability, and the asset value. The measures of risk are scaled, so that the security requirements to be established are matched to the degree of risk. Again, at the completion of this stage, a further management review is recommended to ensure the validity of the information, before moving forward to select countermeasures.

In stage 3, the final stage, the countermeasures, dependent upon the scale of the risk, are selected. The tool contains countermeasures groups for each individual threat, addressing, for example, identification and authentication, access control, and physical security. Within each countermeasure group, you have the following structure:

1) A policy statement can be derived, verbatim, from the appropriate security policy document or supporting directives or guidance documents;
2) The security objective of applying this particular countermeasure;
3) Detailed descriptions of the functions associated with the countermeasure; and
4) Specific ways, or options, in which the functionality can be provided.

The capability also exists to apply the costs of the countermeasures (both in financial and man-effort terms). Having selected countermeasures, a management review meeting is required to examine the countermeasures, consider those which may not be applicable, identify those for implementation, and identify those aspects where the risk is to be accepted. A powerful aspect of the tool, which is very relevant here, is the back-track capability. This means that you can, if you are not certain why a particular countermeasure has been recommended, review the asset / threat / vulnerability information that led to the countermeasure decision.

All through the stages, varying degrees of management reports can be produced, depending upon the target audience. One of the benefits, in the final stage, is the ability to produce the security-related documentation used in the accreditation process.

2.2 Canadian TRA Methodology

The Communications Security Establishment, a Canadian security lead agency, has developed a series of risk management1 documents to help government departments in meeting the Government of Canada Security Policy (GSP) requirements. The following documents expanded on the standards set out in the GSP:

1) MG2 – Risk Management Framework for Information Technology (IT), 1996. The MG2 provides specific guidance for risk management within an IT system environment and its life cycle;
2) MG3 – A Guide to Risk Assessment and Safeguard Selection for Information Technology Systems, January 1996. The MG3 provides specific guidance for risk assessment and safeguard selection process throughout the IT system life cycle;
3) MG4 – A Guide to Certification and Accreditation for Information Technology Systems, January 1996. The MG4 provides more specific guidance for the certification and accreditation of an IT system throughout its life cycle; and
4) ITSG-04 – Threat and Risk Assessment Working Guide, October 1999. The ITSG-04 provides guidance to an individual (or a departmental team) in carrying out a Threat and Risk Assessment (TRA) for an existing or proposed IT system.

The MG series provides a solid guidance for risk management to managers but lack methodology to assign risk values. A working group was created to develop a TRA working guide to be included as a part of risk management processes.

In addition to CSE efforts in developing a TRA guideline, the Royal Canadian Mounted Police (RCMP) had undertaking initiatives in the same area. As the lead department for federal law enforcement, with a crime prevention mission, the RCMP is also responsible to provide advice to departments on the process of threat and risk assessments and the conduct of IT system security reviews, inspections and audits.

2.2.1 Using TRA in Risk Management

Risk management is the process by which resources are planned, organized, directed, and controlled to ensure the risk of operating a system remains within acceptable bounds at near-optimal cost.

Risk management is an iterative and cumulative process. The following figure outlines the Canadian overall risk management process which involves: planning; the TRA; selection of safeguards; system certification and accreditation; maintenance; and monitoring and adjustments to safeguard selections. Traditional prescriptive approach of mandating (i.e. “shall” implement) specific security controls for systems are not cost effective or are too complex. The current Canadian approach to risk management is a mixed approach that is prescriptive and threat-based. Minimum standards set the prescribed safeguards, which are supplemented through a threat-based process. However, this approach is silent on how minimum standards are established: Minimum standards should also be determined through a risk management process involving a TRA. It would be interesting to get a single global risk management process because both measure similar risks.

The TRA in this model is functional and provides the current level of **R**isk caused by the **T**hreat Agents acting on the Critical **A**ssets of an Information System given its **V**ulnerabilities. More precisely, the risk is a function of the values of the assets, the threat agent attributes, and the vulnerabilities, or $R = f$ (AVal, T, V). Note that R is a probabilistic measure of harmful impacts of a given type on a system (IT-system) and they are many possible impact types.

2.2.2 Risk Management Tools

The current Government of Canada (GoC) information technology risk management scheme is supported by these two basic methodologies, the ITSG-04 and the RCMP TRA guidelines. It must be noted that many government departments have developed their own methodologies to suit their environment but the root to those remains the formal two basic methods with the occasional insight derived from sources such as the National Institute of Standards and Technology Risk framework

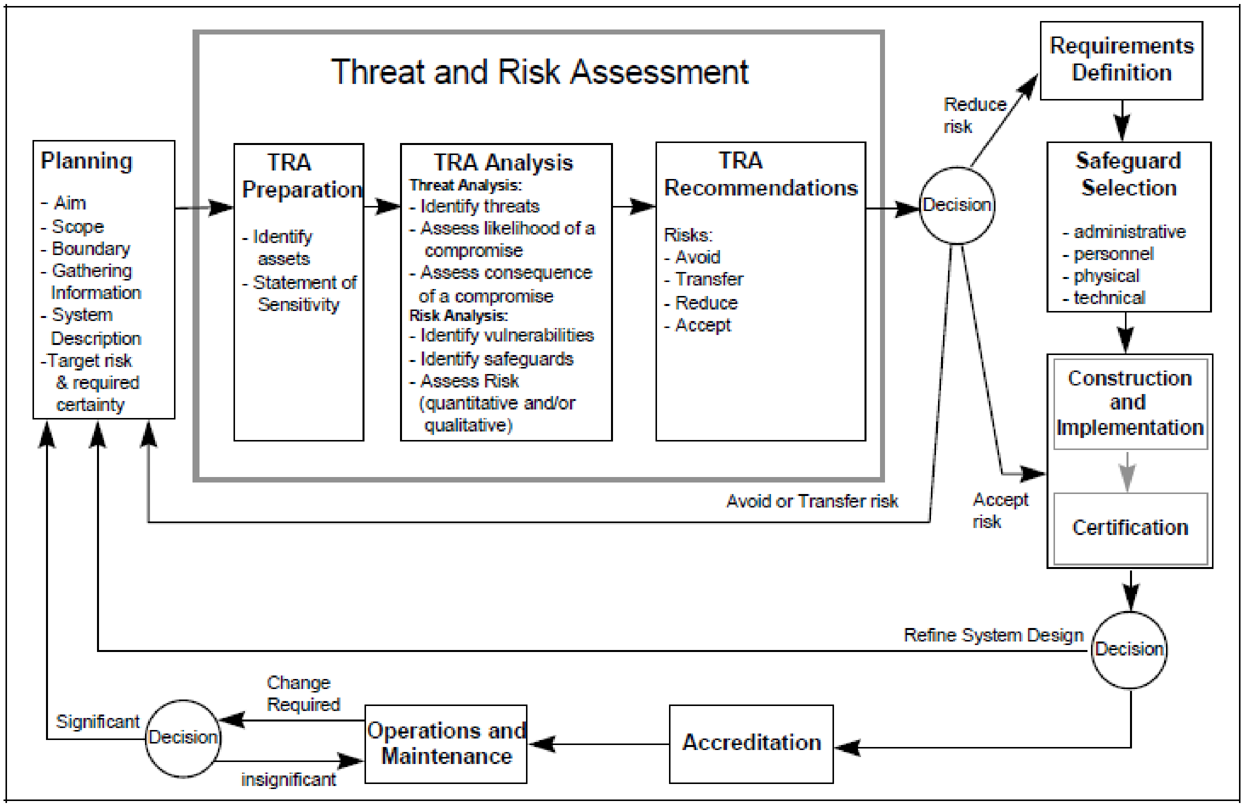


Figure 2.2. Risk Management Model

2.3 US Model

2.3.1 Introduction

The United States has not standardized on any particular risk assessment tool or methodology. Although several tools have been evaluated, each seems to rely on subjective information depending on the system under review, the environment in which it resides and the person performing the evaluation. National Risk Analysis Methodologies are available, but no single methodology has been adopted or is applicable to all systems and all cases. Methodologies vary depending upon the level of assets requiring protection.

For instance a more rigorous process is required for systems which process highly sensitive information.

2.3.2 Objective

The objective of this section is to provide information about risk methodologies used by both National and Federal agencies within the United States. Furthermore, it will define common steps to determine system risk; it is highly likely that these steps are consistent with international risk methodologies.

2.3.3 Basic Risk Methodology

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30 and the Federal Information Security Management Act (FISMA) of 2002 provide a foundation for the general risk methodology used within the United States. NIST SP 800-30 is the risk management guide for general information technology systems and FISMA outlines a mandatory set of processes that must be followed for all information systems used or operated by U.S. Government federal agencies or by contractors or other organizations on behalf of U.S. Government agencies. These documents are complementary and provide a model to manage risk associated with information technology systems.

2.3.3.1 Risk Assessment

The basic steps which apply to risk assessment are depicted in Figure 2.3

Step 1) Characterize the system in terms of scope and boundary. A system may be a single device or a network of computers supporting a common purpose and managed by a single system owner. It may also include assets such as buildings, personnel and network security components. The US Department of Defense (DoD) implements the DoD Information Technology Security Certification and Accreditation Process (DITSCAP) to document systems used within U.S. DoD.

Step 2) Threat Identification. Threats can be categorized as Natural, Human or Environmental. Natural threats are generally related to weather or earthly disturbance such as earthquakes, floods, tornadoes, lightning, etc. Human threats can be intentional or unintentional and are perpetrated by humans. Environmental Threats can be intentional or unintentional and include items such as chemical hazards, pollution and power fluctuations.

Step 3) Vulnerability Identification may be information obtained from multiple sources, such as open literature, previous security testing, intelligence, etc. Vulnerabilities may include weak system security practices such as easily guessed passwords, lack of physical security, untrustworthy personnel, failure to maintain and update software such as virus scanning and lack of life cycle support.

Step 4) Control Analysis is the determination of countermeasures to thwart an attacker from exploiting vulnerabilities. Countermeasures can include procedures such as training and implementing strong security polices. It can also include software, hardware and personnel, for instance hosting systems in physically secure spaces with a guard force in place.

Step 5) Likelihood determination is the process by which an evaluator systematically weighs the extent to which a potential vulnerability will be exploited. Factors used to determine likelihood are motivation and ability of the perpetrator, identified system vulnerabilities and existing countermeasures. For instance a system processing highly sensitive information might be a sought after target for adversaries. However, the risk of detection and attribution could be extremely high. These elements must be balanced to determine the likelihood that a potential attacker would be prone to mount an attack.

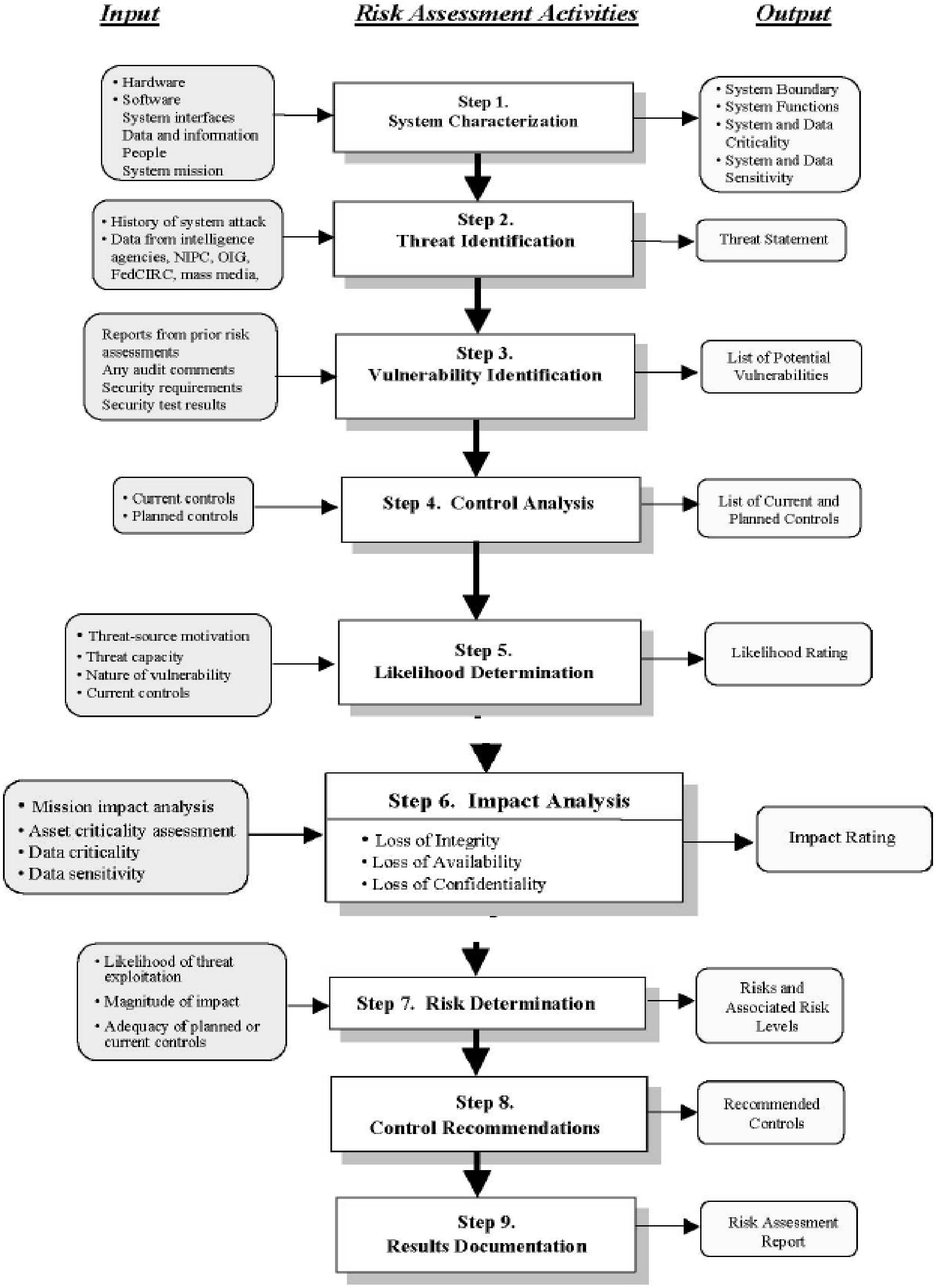


Figure 2.3. Risk Assessment Methodology Flow Chart

The likelihood that a potential vulnerability could be exercised by a given threat-source may be described as high, medium, or low (or more granularly). Table 2 below describes three basic likelihood levels

Likelihood Level	Likelihood Definition
High	The threat-source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective
Medium	The threat-source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability
Low	The threat-source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised

Table 2.1: Likelihood Definitions

Step 6) Impact Analysis is based on a combination of elements and how they affect each other. First, a determination of the impact a successful exploitation may have on the system is required. The evaluator must work with system site personnel and review documentation describing the system. All US Government systems must abide by the DoD Information Technology Security Certification and Accreditation Process (DITSCAP). This is a formal process which documents a system from initial implementation through life cycle management. It includes the operating environment, system security architecture and boundaries, personnel responsible for system maintenance and security, test plans, procedures and results. Once the evaluator has a thorough knowledge about the sensitivity and criticality of the system and its operating environment an impact analysis can be determined. Impacts may be measured in the general terms; High, Medium and Low (or may contain greater granularity).

An impact analysis can be used to determine cost-benefit criteria. Implementing policy controls such as complex passwords to discourage unauthorized access is an example of a low cost mitigation with high benefit potential. For highly sensitive systems a more rigorous security posture may be required and the cost of implementing additional security features may be high. Each system undergoing impact analysis will be unique. Although there may be many similarities, each system must be treated independently and its security mechanisms and environment must be balanced to produce an acceptable level of risk for the system security manager.

Magnitude of impact	**Impact Definition**
High	Exercise of the vulnerability: 1) May result in the highly costly loss of major tangible assets or resources; 2) May significantly violate, harm, or impede an organization’s mission, reputation, or interest; or 3) May result in human death or serious injury.
Medium	Exercise of the vulnerability: 1) May result in the costly loss of tangible assets or resources; 2) May violate, harm, or impede an organization’s mission, reputation, or interest; or 3) May result in human injury.
Low	Exercise of the vulnerability: 1) May result in the loss of some tangible assets or resources; or 2) May noticeably affect an organization’s mission, reputation, or interest.

Table 2.2: Magnitude of Impact Definitions

Step 7) Risk determination is a compilation of information obtained in Steps 1 through 6. The U.S has not standardized on any quantifiable risk methodology formula. The basis for determining risk is common

Risk associated with any system is a function of the comparison of known vulnerabilities, an adversary's inclination and ability to exploit those vulnerabilities and the consistency of security management throughout the life cycle of the system. Unfortunately, the determination of risk level is more dependent on the thoroughness of system documentation and experience of the evaluator than on any methodology.

Step 8) Control recommendation is the process by which mitigations are introduced to reduce or minimize system risk. Control recommendations are based on the risks identified in Step 7. Control mechanisms may be physical, procedural, software or policy based. A determination must be made as to which control mechanisms to implement, this determination may be based on feasibility, operational impact, effectiveness, level of security required, cost and level of risk acceptance.

Step 9) Resulting documentation is the residual risk after security controls have been implemented. This document serves as a resource for managers to understand remaining risks and vulnerabilities associated with their information system. Under FISMA and DITSCAP, U.S. Federal agencies use resulting documentation as basis for accrediting a system, whereby the accreditation authority accepts risk for the system and issues an authority to operate (ATO).

2.4 Czech Methodology

The main steps of this method are:

- Assets identification;
- Threats identification;
- Evaluation of Probability of Threats realization;
- Evaluation of Vulnerability of Assets to the Threats; and
- Calculating of Risk value for every Asset and Threat pair.

After identifying the assets, they are valuated. Assets value vary from 0 (negligible: Asset loss, damage or security violation has only slight or no influence on IS operation and security) to 5 (very high: Asset loss, damage or security violation means outage of the whole IS operation or perhaps total loss of IS security as a whole or important part).

The values should be applied to the costs of obtaining and maintaining a particular Asset and also to the potential impact on organization behavior in case of loss or damage of the Asset.

Criteria used to determine assets values:

- Non compliance with law and/or regulations;
- Damage or break-up of business;
- Loss of good reputation, negative influence on organization image;
- Reduction of security for organization members;
- Unfavorable impact of law;
- Violation of business secret;
- Breaching the purchase order
- Financial loss.

The threat probability is estimated by a value from 0 (the threat cannot occur) to 6 (the threat occurrence is certain or the threat occurs often or regularly or it is a case of continuously threatening status (defect) assessment).

Vulnerability evaluation is then performed. It includes identification of:

- Weak point; and
- Existing security mechanisms.

Weak points can be:

- Physical environment;
- Employees, management and administrative procedures a mechanisms; and
- HW, SW, communication equipment, company premises, etc.

Weak points can be used by the threat to damage assets and business procedures supported by assets. Vulnerabilities are reduced by existing security mechanisms.

An asset vulnerability to the threat is estimated from 0 (the threat cannot occur for the asset) to 4 (the asset is insufficiently resistant to the threat occurrence or is not protected at all).

The risk value is calculated with the following formula:

Final risk = Asset value * Probability of threat occurrence * Vulnerability of assets group

According the value of the final risk are defined as:

- High risk in the range 61 – 90
- Medium risk in the range 31 – 60
- Low risk in the range 1 – 30

2.5 Spanish Method MAGERIT

MAGERIT risk analysis is a methodical approach to determine the risk, following specific steps:

1) Determine the relevant assets for the organization, their inter-relationships and their value i.e. what prejudice (cost) would be caused by their degradation.
2) Determine the threats to which those assets are exposed.
3) Determine what safeguards are available and how effective they are against the risk.
4) Estimate the impact, defined as the damage to the asset arising from the appearance of the threat.
5) Estimate the risk, defined as the weighted impact on the rate of occurrence (or the expectation of appearance) of the threat.

In order to organize the presentation, steps 1, 2, 4 and 5 are handled first, skipping step 3, so that any estimates of impact and risk are "potential" if no safeguards are deployed. Once this theoretical scenario is obtained, the safeguards are incorporated in step three, providing realistic estimates of impact and risk.

2.5.1 Assets

The assets are the resources in the information system or related to it that are necessary for the organization to operate correctly and achieve the objectives proposed by its management.

A type can be assigned to each asset. Dependencies can also be established . A "higher asset" is said to depend on the "lower asset" when the security needs of the higher one are reflected in the security needs of the lower one. In other words, when the appearance of a threat in the lower asset has a prejudicial effect on the high asset. Informally, this could be interpreted as the lower assets being the pillars that support the security of the higher assets. Although it is necessary to adapt to the organization being analyzed in each case, the group of assets can frequently be structured into layers, where the upper layers depend on the lower ones.

Assets are the valuated, either in a qualitative or quantitative way.

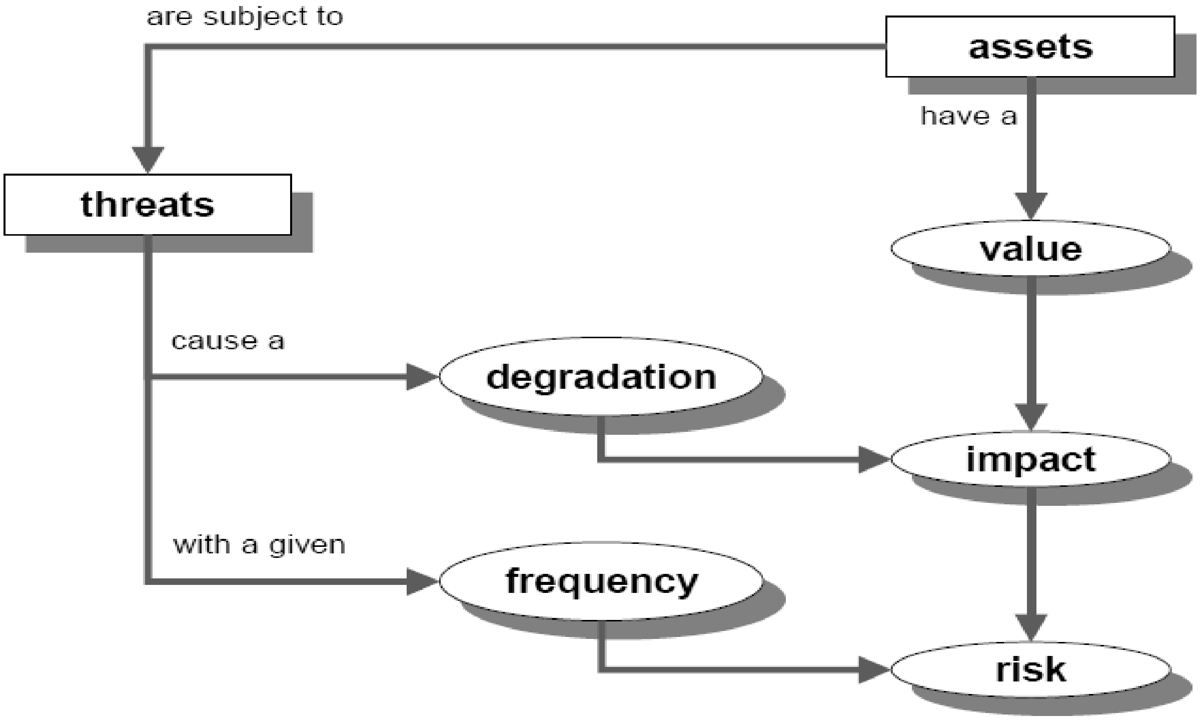


Figure 2.3. MAGERIT Main Steps

2.5.2 Threats

The next step is to determine the threats that may affect each asset.

Once it has been determined that a threat may damage an asset, the asset's vulnerability6 must be estimated considering two aspects:

- **Degradation:** The amount of damage done to the asset.
- **Frequency:** How often the threat appears.

Degradation measures the damage caused by an incident if it occurs. Degradation is often described as a part of the asset's value and therefore expressions appear such as that an active has been “totally degraded,” or “very slightly degraded”. When the threats are not intentional, it is probably enough to know the physically damaged part of an asset in order to calculate the proportional loss of value. But when the threat is intentional, one cannot think of proportions since the attacker may cause a great deal of damage selectively.

Frequency puts degradation into perspective since one threat may have terrible consequences but very unlikely to occur while another threat may have very small consequences but are so frequent as to accumulate into considerable damage.

Frequency is modeled as an annual occurrence rate with the following typical values

100	Very frequent	Daily
10	Frequent	Monthly
1	Normal	Annually
1/10	Infrequent	Every few years

Table 2.3: Frequency Table

2.5.3 Determination of the Impact

Impact is the measurement of the damage to an asset arising from the appearance of a threat. By knowing the value of the assets (in various dimensions) and the degradation caused by the threats, their impact on the system can be derived directly.

2.5.3.1 Accumulated Impact

This is calculated for an asset taking into account:

- Its accumulated value (its own plus the accumulated value of the assets that depend on it).
- The threats to which it is exposed.

The accumulated impact is calculated for each asset, for each threat and in each evaluation dimension, being a function of the accumulated value and of the degradation caused.

Because the accumulated impact is calculated on the assets that carry the weight of the information system, it allows the determination of the safeguards to be adopted in the working media: protection of equipment, back-up copies, etc.

2.5.3.2 Deflected Impact

This is calculated for an asset taking into account:

- Its intrinsic value.
- The threats to which the assets on which it depends are exposed.

The deflected impact is calculated for each asset, for each threat and in each valuation dimension, being a function of the intrinsic value and of the degradation

Because the deflected impact is calculated on assets that have their own value, it allows the determination of the consequences of the technical incidents on the mission of the information system. It is therefore a management presentation that helps in making one of the critical decisions of a risk analysis: accepting a certain level of risk.

2.5.3.3 Aggregation of Impact Values

The above paragraphs determine the impact of a threat on an asset in a certain dimension. These single impacts may be aggregated under certain conditions:

- The deflected impact on different assets may be aggregated.
- The accumulated impact on assets that are not inter-dependent and that do not depend on any higher asset may be aggregated.
- The accumulated impact on assets that are not independent must not be aggregated because this would imply overrating the impact by including the accumulated value of the higher assets several times.
- The impact of different threats on the same asset may be aggregated although it is useful to consider to what measure the different threats are independent and may be concurrent.
- The impact of a threat in different dimensions may be aggregated.

2.5.4 Safeguards

The above steps have not included the safeguards deployed. Thus, the impacts and risks to which the assets would be exposed if they were not protected in any way are measured.

In practice, it is unusual to find unprotected systems: the measures described indicate what would happen if the safeguards were removed.
Safeguards enter into the calculation of the risk in two ways:

2.5.4.1 Reducing the frequency of threats

These are called preventive safeguards. Ideally, they completely prevent a threat from occurring.

2.5.4.2 Damage limitation

There are safeguards that directly limit any degradation while others allow the immediate detection of the attack to stop the progress of the degradation. There are even some safeguards that are limited to allowing the quick recovery of the system when the threat destroys it. In all of these versions, the threat occurs but the consequences are limited.

As well as being classified by their existence, safeguards are also classified by their effectiveness against the risk that they prevent.

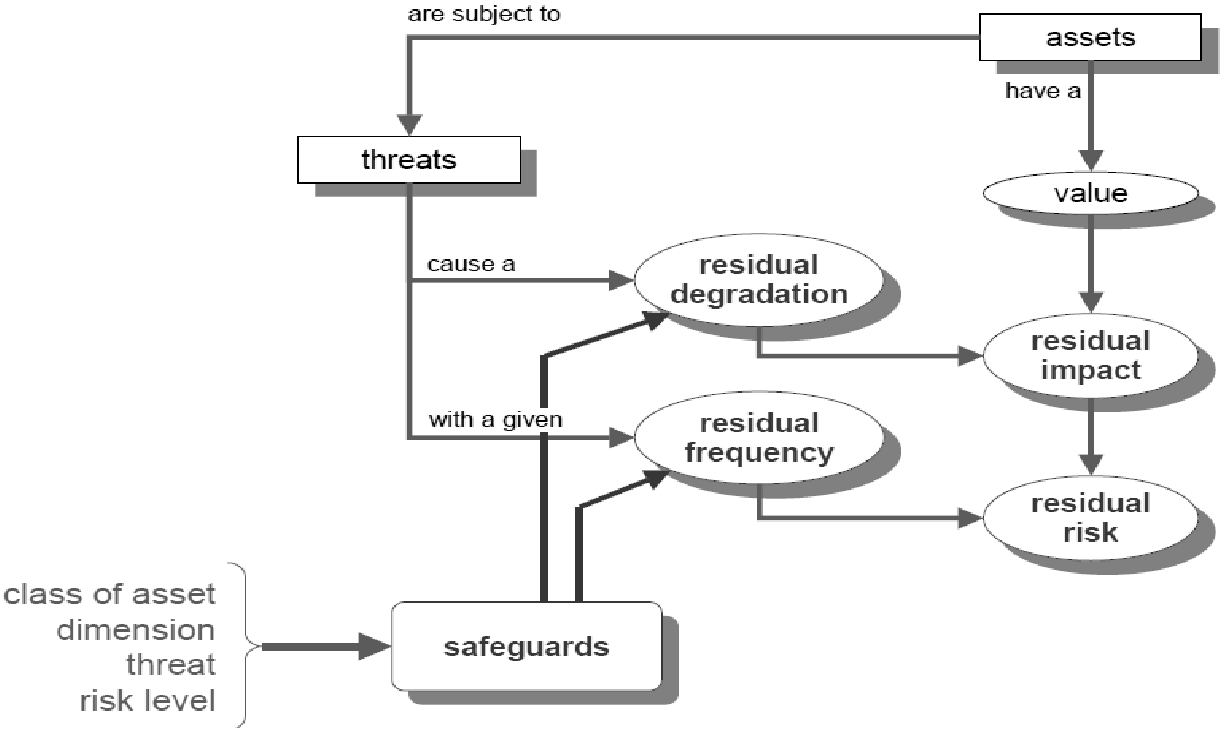


Figure 2.4. MAGERIT Main Steps including Safegaurds

2.5.5 Revision of Step 4: Residual Impact

The calculation of the residual impact is simple. Since neither the assets nor their dependencies have changed, only the size of the degradation, the impact calculations are repeated with this new degradation level.

The size of the degradation, taking into account the effectiveness of the safeguards, is the proportion that remains between perfect effectiveness and real effectiveness.

The residual impact may be accumulated on the lower assets or deflected on the higher assets.

2.5.6 Revision of Step 5: Residual Risk

The calculation of the residual risk is simple. Since neither the assets nor their dependencies have changed, only the size of the degradation and the frequency of threats, the risk calculations are repeated using the residual impact and the new rate of occurrence.

The size of the degradation is taken into consideration in calculating the residual impact.

The size of the frequency, taking into account the effectiveness of the safeguards, is the proportion that remains between perfect effectiveness and real effectiveness.

The residual risk may be accumulated on the lower assets or deflected on the higher assets.

2.6 BEATO

BEATO [18] (sometimes spelled BeATo) stands for "BEnchmark Assessment TOol". Some people refer to it as "Be At zero", meaning the ideal of lowering non-compliance and risk. BEATO is both a tool and a methodology, originally dedicated to Security assessments. It determines the quality of controls as well as the degree of compliance using a Capability Maturity Model.

It allows management to evaluate their current level of security (via consolidations of individual assessments and drill-down), as well as the effects of decisions and projects undertaken for the purpose of improving security.

Both methodology and tool have been developed by Unisys for internal use, originating from 1999 (Y2K compliance). Since 2002 BEATO (and BEATO assessment services) have been marketed to Unisys clients.

BEATO can also be used for compliance assessment relative to all ISO Standards (specifically ISO 9000, ISO/IEC 20000, ISO 27000) with the integral PLATO Risk Management module (PLAnning TOol). PLATO answers the question if poor controls have consequences big enough to warrant investments

CHAPTER 3: RISK MANAGEMENT

There are same basic concepts required for understanding the process of risk management. The important definitions related to this research work are as follows:

3.1 Strategic Organization

A not-for-profit organization monitoring and performing the military/defense oriented activities of a country. Their objectives are associated with defense of the country they are appointed in and they don’t have any commercialization or commercial competition.

3.2 Commercial Organization

Mostly a Profit earning organization (unless it’s an NGO), their objective is to operate, earn profit and market their Products or Services to general public or even strategic organizations. They are usually not the only organization with such objectives in a single region.

3.3 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”. Assets can be tangible including computers, facilities and supplies etc or intangible which includes reputation, data and intellectual. It is usually difficult to compute the values of intangible assets because it may change with the passage of time.

Assets are organization’s resources used to perform operations, e.g. Human Resource, Computers, Networks, Software, Tables, Cupboards, Files, etc. (Anything that has value to the organization)

3.4 Information Asset

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.

3.5 Threat

A potential cause of an unwanted incident, which may result in harm to a system or organization. The threat is “invariably the danger a malicious agent poses and that agent’s motivations (financial gain and prestige etc).” Threats mark themselves as direct attacks on security of system [10]. Also it is a potential cause of an unwanted incident, which may result in harm to a system or organization

3.6 Vulnerability

A weakness of an asset or group of assets that can be exploited by one or more threats. 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”. The reason to resist against the actions can be due to the weaknesses in software or hardware. To model the vulnerability threat capability and system threat resistance are needed.

3.7 Risk

It is combination of probability of an event and its consequences. It indicates [8] both the impact of the cooperation of an asset and the possibility for it being conciliation. less likely and less damaging are dealt with after the more important risks. The risks [9] need to be concentrated on the design, architecture and functionality of the product to provide the implementation procedures and the required maintenance

3.8 Risk Analysis

The process of identifying the most probable threats to an organization and analyzing the related vulnerabilities of the organization to these threats

3.9 Risk Assessment

The process of analyzing the risk's chances of occurrence and its impact on organization's operations and assets. It involves systematic approach to calculate the size and then its significance. It [9] is a process in which different types of risks, their effect on the system are determined. After analysis the risks are prioritized according to the size and timing property.

3.10 Risk Treatment

The Process of selecting the appropriate measures to modify the status of risk (a risk's impact can be reduced but it cannot be eliminated). There are four stages of Risk Treatment;

a. Risk Avoidance: Avoid the activity that can create the risk under observation
b. Risk Mitigation: Deploy a control to reduce the effect of risk
c. Risk Transfer: Outsourcing the responsibility to manage risk and its mitigation to another party
d. Risk Acceptance: Not taking any actions as the impact of risk is very minimal

3.11 Risk Management

The process of Risk Assessment and Treatment, so that to prevent the occurrence of risk. It is the method [11] of coordinated activities to direct and control an organization with regard to risk. Risk management typically includes risk assessment, risk treatment, risk acceptance and risk communication

3.12 Business Continuity Plan

A Backup Plan required to be deployed in case Risk Treatment Plan fails and the risk occurs, the primary objectives of this plan are to ensure continuity of critical operational activities during risk occurrence and recovery to original state

3.13 Disaster Recovery Plan

When business continuity plan involves use of a separate site (usually in case of total site loss), it's called a disaster recovery plan

3.14 Risk Management

Risk management [7] is a structured approach to managing uncertainty through, risk assessment, developing strategies to manage it, and mitigation of risk using managerial resources. It is the culture, processes, and structures that are directed towards the effective management of potential opportunities and adverse effects [21]. The strategies include transferring the risk to another party, avoiding the risk, reducing the negative effect of the risk, and accepting some or all of the consequences of a particular risk. Some traditional risk managements are focused on risks stemming from physical or legal causes (e.g. natural disasters or fires, accidents, death and lawsuits). Financial risk management, on the other hand, focuses on risks that can be managed using traded financial instruments.

Effective risk management [12] does not provide a guarantee against failure. Even in companies with the best risk management people and systems, large losses can and will occur as long as taking the risk of large losses increases expected profits sufficiently for top management to be willing to take that risk. With good risk management, such losses will be attributable to an unlucky "draw," to a one-in-a-hundred event. Ultimately, the likelihood of such large losses will depend on choices made by those entrusted with determining the risk appetite of organization. Risk management ensures that top management knows and understands the probabilities associated with possible outcome of the strategy of organization before the decisions are made to commit its capital

3.14.1 Objective of Risk Management

Objective of risk management is to reduce different risks related to a preselected domain to the level accepted by society. It may refer to numerous types of threats caused by environment, technology, humans, organizations and politics. On the other hand it involves all means available for humans, or in particular, for a risk management entity (person, staff, organization).

3.14.2 Principles of Risk Management

The [13] International Organization for Standardization identifies the following principles of risk management.

Risk management should

- Create value.
- Be an integral part of organizational processes.
- Be part of decision making.
- Explicitly address uncertainty.
- Be systematic and structured.
- Be based on the best available information.
- Be tailored.
- Take into account human factors.
- Be transparent and inclusive.
- Be dynamic, iterative and responsive to change.
- Be capable of continual improvement and enhancement

3.14.3 Risk Management Phenomenon

Risk Management is a process of identifying activities, assets or external/internal sources that can negatively affect an organization’s operations. It is applicable on all types of management structures like for Information Security Management System (ISMS), Environmental Management System (EMS), Occupational Health and Safety Management System (OH&S), operational management through Quality Management Process (QMS), etc. Every management system has its own agendas; therefore all of them come up with their own objectives and end deliverables. Difference in prime objectives, also effects the point of view required to assess the risks associated with each activity. For example, Fire is a threat and risks associated with ISMS, EMS and OH&S will vary because of the differences between the practices;

Management Practices	Threat	Probable Vulnerability	Probable Risk
ISMS	Fire	Assets are vulnerable to fire and electricity can create a fire hazard	Damage to asset and interruption in critical operational activity
EMS	Fire	Flammable items used in process	Air Pollution is produced in case of flammable items catching fire
OH&S	Fire	Flammable items and human resource with low understanding of fire management	Death of workers

Table 3.14: Management practices and Probable risk

In Table 3.14, three different practices are considered for the same threat i.e. “Fire”, but the outcomes and the assessment of vulnerabilities in all three cases is different. But, remember, treatment measures to control “Threat” or to overcome “Vulnerabilities” may be same in all cases, e.g. installation Fire extinguishers in all hazardous areas (where Fire can occur).

The ISMS [11] is “considered to ensure the selection of adequate and proportionate security controls that protect information assets and give confidence to interested parties”. The EMS involves all the resources and all aspects of the organization that influence the environment. The organization’s environmental performance can be improved in terms of cost by searching benefits. OH&S is used to establish occupational health and safety management system of the organization. It defines a set of OH & S management system requirements.

3.15 Risk Management And System Development Life Cycle(SDLC)

Minimizing [6] negative impact on an organization and need for sound basis in decision making are the fundamental reasons organizations implement a risk management process for their IT systems. Effective risk management must be totally integrated into the SDLC. Any IT organization involving SDLC has five phases: initiation, development or acquisition, implementation, operation or maintenance, and disposal. In some cases, an organization may occupy several of these phases at the same time. However, the risk management methodology is the same regardless of the SDLC phase for which the assessment is being conducted. Risk management is an iterative process that can be performed during each major phase of the SDLC.

If each phase is considered individually it also contains further steps to complete. In initiation there is need of complete requirement gathering and according to the gathered information use cases are derived. As shown in Figure 1, there is risk analysis done before and after design phase. According to that the risk based security test cases are generated. After implementation again analysis is done.

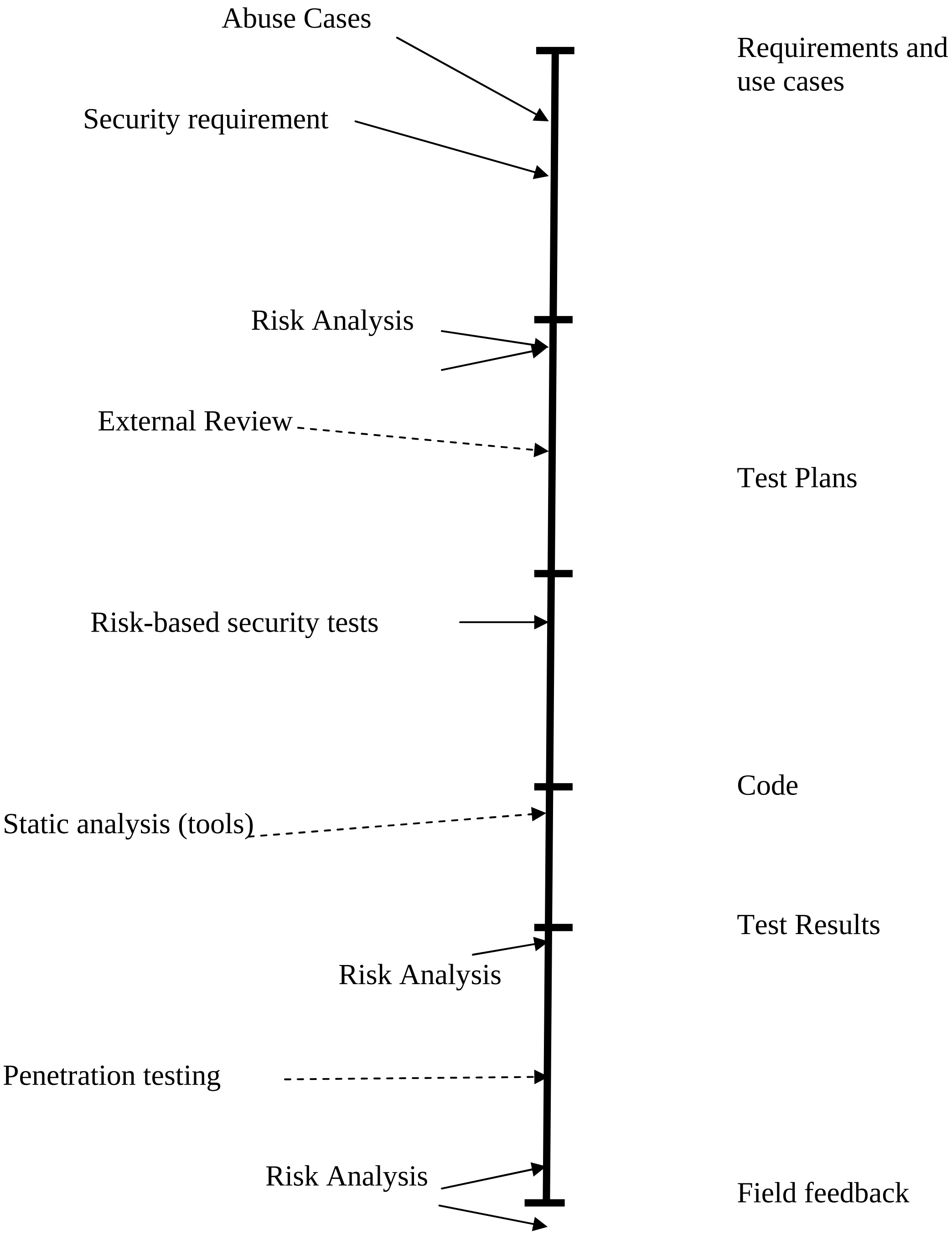


Figure 3.1. Risk Analysis in development Cycle[10]

SDLC phases	Phase Characteristics	Support from risk management Activities
Phase 1, Initiation	The need for an organization is expressed and the purpose and scope of the organization is documented	Identified risks are used to support the development of the system requirements, including security requirements, and a security concept of operations (strategy)
Phase 2- Development	The IT system is designed, purchased, programmed, developed, or otherwise constructed	The risks identified during this phase can be used to support the security analyses of the IT system that may lead to architecture and design tradeoffs during system development
Phase 3- Implementation	The system security features should be configured, enabled, tested, and verified	The risk management process supports the assessment of the system implementation against its requirements and within its modeled operational environment. Decisions regarding risks identified must be made prior to system operation
Phase 4- Operations and maintenance	The system performs its functions. Typically the system is being modified on an ongoing	Risk management activities are performed for periodic system reauthorization (or reaccreditation) or

	basis through the addition of hardware and software and by changes to organizational processes, policies, and procedures	whenever major changes are made to an IT system in its operational, production environment (e.g., new system interfaces)
Phase 5- Disposal	This phase may involve the disposition of information, hardware, and software. Activities may include moving, archiving, discarding, or destroying information and sanitizing the hardware and software	Risk management activities are performed for system components that will be disposed of or replaced to ensure that the hardware and software are properly disposed of, that residual data is appropriately handled, and that system migration is conducted in a secure and systematic manner

Table 3.1: Risk Management and SDLC[10]

3.16 Risk Assessment

Risk assessment [22] is one method in a much broader field of risk management. Risk assessment is a process that does not result in a fixed final answer. It is impossible to determine the true magnitude and extent of any actual contamination at a site.

Once [20] risks have been identified, they must then be assessed as to their potential severity of loss and to the probability of occurrence. These quantities can be either simple to measure, in the case of the value of a lost building, or impossible to know for sure in the case of the probability of an unlikely event occurring. Therefore, in the assessment process it is critical to make the best educated guesses possible in order to properly prioritize the implementation.

The fundamental [13] difficulty in risk assessment is determining the rate of occurrence since statistical information is not available on all kinds of past incidents. Furthermore, evaluating the severity of the consequences (impact) is often quite difficult for immaterial assets. Asset valuation is another question that needs to be addressed. Thus, best educated opinions and available statistics are the primary sources of information. Nevertheless, risk assessment should produce such information for the management of the organization that the primary risks are easy to understand and that the risk management decisions may be prioritized.

Risk assessment [7] may be the most important step in the risk management process, and may also be the most difficult and prone to error. Once risks have been identified and assessed, the steps to properly deal with them are much more programmatical.

Part of the difficulty of risk management is that measurement of both of the quantities in which risk assessment is concerned can be very difficult itself. Uncertainty in the measurement is often large in both cases. Also, risk management would be simpler if a single metric could embody all of the information in the measurement. However, since two quantities are being measured, this is not possible. A risk with a large potential loss and a low probability of occurring must be treated differently than one with a low potential loss but a high likelihood of occurring. In theory both are of nearly equal priority in dealing with first, but in practice it can be very difficult to manage when faced with the scarcity of resources, especially time, in which to conduct the risk management process.

3.17 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 us an idea or scale of risk under observation. These techniques are mostly divided into three types of assessments;

3.17.1 Qualitative Assessment

Qualitative analysis [16] helps in the identification of the assets and resources at risk, vulnerabilities that might allow the threats to be realized, safeguards already in place and those which may be implemented to achieve an acceptable level of risk and increase overall awareness. This analysis uses simple calculations and uses procedure in which it is not necessary to determine the dollar value of all assets and the threat frequencies or the implementation costs of the controls.

In this method, ratings are defined in terms of characteristics and when multiplied /added / combined, 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“, in 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. But this may also result in some confusion like in a combination of “Highest” and “Lowest”, which one will be preferred, will depend highly on experience of the person performing the assessment.

Some of the qualitative methods used in risk analysis namely are preliminary risk analysis (PHA), hazard and operability study (HAZOP), and failure mode and effects analysis (FMEA/FMECA).

3.17.1.1 Preliminary Risk Analysis

Preliminary Risk Analysis Preliminary risk analysis or hazard analysis is a qualitative technique which involves a disciplined analysis of the event sequences which could transform a potential hazard into an accident. In this technique, the possible undesirable events are identified first and then analysed separately. For each undesirable events or hazards, possible improvements, or preventive measures are then formulated.

The result from this methodology provides a basis for determining which categories of hazard should be looked into more closely and which analysis methods are most suitable. Such an analysis also proved valuable in the working environment to which activities lacking safety measures can be readily identified. With the aid of a frequency/ consequence diagram, the identified hazards can then be ranked according to risk, allowing measures to be prioritized to prevent accidents.

3.17.1.2 Hazard and Operability studies (HAZOP)

The HAZOP technique was developed in the early 1970s by Imperial Chemical Industries Ltd. HAZOP can be defined as the application of a formal systematic critical examination of the process and engineering intentions of new or existing facilities to assess the hazard potential that arise from deviation in design specifications and the consequential effects on the facilities as a whole.

This technique is usually performed using a set of guidewords: NO/NOT, MORE OR/LESS OF, AS WELL AS, PART OF REVERSE, AND OTHER THAN. From these guidewords, a scenario that may result in a hazard or an operational problem is identified. Consider the possible flow problems in a process line, the guide word MORE OF will correspond to high flow rate, while that for LESS THAN, low flow rate. The consequences of the hazard and measures to reduce the frequency with which the hazard will occur are then discussed. This technique had gained wide acceptance in the process industries as an effective tool for plant safety and operability improvements. Detailed procedures on how to perform the technique are available in literature.

3.17.1.3 Failure Mode and Effects Analysis (FMEA/FMECA)

This method was developed in the 1950s by reliability engineers to determine problems that could arise from malfunctions of military system. Failure mode and effects analysis is a procedure by which each potential failure mode in a system is analysed to determine its effect on the system and to classify it according to its severity.

When the FMEA is extended by a criticality analysis, the technique is then called failure mode and effects criticality analysis(FMECA). Failure mode and effects analysis has gained wide acceptance by the aerospace and the military industries. In fact, the technique has adapted itself in other form such as misuse mode and effects analysis.

These three techniques outlined above require only the employment of hardware familiar personnel. However, FMEA tends to be more labour intensive, as failure of each individual component in the system has to be considered. A point to note is that these qualitative techniques can be used in the design as well as operational stage of a system.

All the techniques mentioned above have seen wide usage in the nuclear power plant and chemical processing plant. In fact, FMEA, one of the most documented, has been used by Intel and National Semiconductor to improve the reliability of their product. For the case of preliminary risk analysis, it has seen application in safety analysis as well as offshore platform. HAZOP, on the other hand, has been widely used in the chemical industries for detailed failure and effect study on the piping and instrumentation layout.

3.17.2 Quantifiable Assessment

Quantitative analysis [16] identifies the specific envelope in which the losses and safeguards exist. It is based substantially on independently objective processes and metrics and requires an accordingly increased degree of effort be placed in deterring the cost values and an increasing amount of effort be placed into the calculations. It presents its results in a management-friendly form of monetary values, percentages, and probabilities.

In this method, 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 one 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 give 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”.

3.17.3 Monetary Assessment

This method requires us 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, 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.

3.17.4 Probabilistic Assessment

Probabilistic risk assessment (PRA) (or probabilistic safety assessment/analysis) is a systematic and comprehensive methodology to evaluate risks associated with a complex engineered technological entity (such as an airliner or a nuclear power plant). Risk in a PRA is defined as a feasible detrimental outcome of an activity or action. In a PRA, risk is characterized by two quantities (1) the magnitude (severity) of the possible adverse consequence(s), and (2) the likelihood (probability) of occurrence of each consequence.

Consequences are expressed numerically (e.g., the number of people potentially hurt or killed) and their likelihoods of occurrence are expressed as probabilities or frequencies (i.e., the number of occurrences or the probability of occurrence per unit time). The total risk is the expected loss which is the sum of the products of the consequences multiplied by their probabilities.

The spectrums of risks across classes of events are also of concern, and are usually controlled in licensing processes. It would be of concern if rare but high consequence events were found to dominate the overall risk, particularly as these risk assessment is very sensitive to assumptions.

Probabilistic Risk Assessment usually answers three basic questions:

a. What can go wrong with the studied technological entity, or what are the initiators or initiating events (undesirable starting events) that lead to adverse consequence(s)?
b. What and how severe are the potential detriments, or the adverse consequences that the technological entity may be eventually subjected to as a result of the occurrence of the initiator?
c. How likely to occur are these undesirable consequences, or what are their probabilities or frequencies?

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.

3.18 Benefits of Risk Assessment

Risk assessment is necessary for reliability and productivity of an organization.
Following [8] are the main advantages can be achieved by applying this approach

3.18.1 Cost Justification

Additional security almost always involves additional expense. As this does not directly generate income, it should always be justified in financial terms. The Risk

Analysis process should directly and automatically generate such justification for security recommendations in business terms.

3.18.2 Productivity Audit/Review Savings

A Risk Analysis programme should enhance the productivity of the security or audit team. By creating a review structure, formalising a review, pooling security knowledge in the system's "knowledge base" and utilising "self-analysis" features, much more productive use of time is possible. The ability to 'build-in' expertise should also alleviate the need for expensive external security consultants.

3.18.3 Breaking Barriers, Business relationships

Security should be addressed at both business management and IT staff. Business management are responsible for decisions relating to the security risk/level that the enterprise is willing to accept at a given time (which involves consideration of potential business impact). IT management are responsible for decisions relating to specific controls and application. Risk Analysis should not only direct appropriate information at each group, but play a major and pro-active role in enhancing the understanding of the needs and role of the other. It should bring the two groups closer together. Risk Analysis should relate security directly to business issues.

3.18.4 Self Analysis

The Risk Assessment system should be simple enough to enable its use without necessitating particular security knowledge, or indeed, IT expertise. This approach enables security to be driven into more areas and to become more devolved. It enables security to become part of the enterprises culture, allowing business unit management to take more of the responsibility for ensuring an adequate and appropriate level of security.

3.18.5 Security Awareness

The wide scale application of a risk assessment programme, by actively involving a range of, and greater number of, staff, will place security on the agenda for discussion and increase security awareness within the enterprise.

3.18.6 Targeting of Security

Security should be properly targeted, and directly related to potential impacts, threats, and vulnerabilities. Failure to achieve this could result in excessive or unnecessary expenditure. Risk Analysis promotes far better targeting and facilitates related decisions. This not only applies to which areas of a particular system resources should be directed to, but which business systems. Through the application of Risk Analysis across multiple business unit, it is possible to quickly establish the areas of greatest risk to the enterprise as a whole.

3.18.7 Baseline Security and Policy

Many enterprises require adherence to certain 'baseline' standards. This could be for a variety of reasons, such as legislation (e.g., Data Protection Act), enterprise policy, regulatory controls, etc. The Risk Analysis methodology should support such requirements and enable rapid identification of any failings.

3.18.8 Consistency

A major benefit of the application of Risk assessment is that it brings a consistent and objective approach to all security reviews. This not only applies across different applications, but different types of business system. It should also embrace those systems not under the direct control of IT management including paper based systems, PC Systems, or systems utilizing other office equipment.

3.18.9 Communication

By obtaining information from different parts of a business unit, a Risk Assessment aids communication and facilitates decision making.

3.19 Risk Management Failure

If risks [13] are improperly assessed and prioritized, time can be wasted in dealing with risk of losses that are not likely to occur. Spending too much time assessing and managing unlikely risks can divert resources that could be used more profitably. Unlikely events do occur but if the risk is unlikely enough to occur it may be better to simply retain the risk and deal with the result if the loss does in fact occur. Qualitative risk assessment is subjective and lacks consistency. The primary justification for a formal risk assessment process is legal and bureaucratic. Prioritizing the risk management processes too highly could keep an organization from ever completing a project or even getting started. This is especially true if other work is suspended until the risk management process is considered complete.

It is observed that risk management [12] is valuable, it is also important to understand the many ways in which risk management failures may arise. In risk management first step is to identify and measure risks. After the control measure is taken, there are following basic kinds of mistakes that can be made in measuring risk.

- Failure to use appropriate risk metrics involves if the risk is known and seems to be benign to the organization and the measure taken to overcome it is not appropriate causes the failure to any important asset of the organization.
- Mismeasurement of known risks is the case where risk managers have chosen the right metrics, but the risks have been measured incorrectly. A mistake is made in assessing the probability of large loss or the wrong distribution is used altogether.
- Mismeasurement stemming from overlooked risks involves if the concerned individuals ignore a known risk, because of a mistaken assumption that it is immaterial or because of the difficulty of incorporating it in the risk models or it is a case of risks that are truly unknown, or at least completely unanticipated.
- Failure in communicating risks to concerned management is not the job of risk management to determine the overall target level of risk or the kind of risks of the organization. Its role is to provide timely information to the board and top management that allows them to assess the consequences of retaining or laying

off risks. So if the risk is occurred it is necessary to communicate the management in time and to the appropriate management.

- Failure in monitoring and managing risks in case where risk should be monitored constantly or otherwise manage known risks to meet the objectives of concerned management. It may be particularly challenging for financial firms, where risks change abruptly even if the organization does not take new positions

CHAPTER 4: COMPARITIVE ANALYSIS AND PROPOSED MODEL

Risk analysis, analytical identification and assessment methodology for different risk factors, can plays a vital role for the protection of strategic data center environments.

Risk management provides structured methodology for assessing the risks; develop the strategies for managing and impart controls by using the resources to mitigate the risks. The strategies comprise of taking measures to reduce the probability of occurrence of the risk and remedial steps to overcome the effect caused due to that occurrence of risk. It is a process of identifying activities, assets or external/internal sources that can negatively affect an organization’s operations.

4.1 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.

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 4.1 : Similarities of Strategic and Commercial 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.

S.No	Strategic Organization	Commercial Organization
1	Not-for-profit	Works for Profit (can't survive without it)
2	No Competition and not part of market as the services are unique and cannot be commercialized	Have to complete with competitors, therefore biggest threats are competitors and their activities that can effect their profits
3	Risks and their impacts can effect national causes (country's defense structure) and eventually can effect commercial setup as well (it may also effect their assets / resources or services in a negative manner)	Risks and their impacts will affect organization's assets/resources and/or services only, and shall not effect strategic organizations. In some cases, it may have severe effect on its suppliers or customers (but strategic organizations usually have extensive backups as their existence is a Government's prime responsibilities)
4	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
5	In addition to Legal requirements, Defense based regulations are also applicable. Not following them can have severe negative effects strategic decisions	In addition to Legal requirements, customer (especially foreign customers) requirements are also followed (especially in case of software houses and call centers). Not following them can have negative effects commercial position and business relations
6	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
7	Third party involvement is very less in most of the operations and projects	Links to the third party are important for better competition and profit earning

Table 4.2 : Differences of Strategic and Commercial Organization

The coming portions of this chapter will breakdown Risk Assessment and Risk Treatment process in light of both Strategic and Commercial Organizations, considering their similarities and differences.

4.2 Proposed Risk Assessment and Treatment model

It is observed that the basic steps for risk management are same but can be used in different scenarios according the environment and structure of the organization. The goal of proposed model is to provide organization such a qualitative approach to implement risk management process.

The proposed risk assessment model consists of following steps

1. Identification of Assets
2. Asset Value
3. Identification of threats
4. Identification of vulnerabilities
5. Identifying Risk
6. Risk Assessment
    a. Value of Information Asset
    b. Chances of Risk Occurrence
    c. Chances of Risk Detection
    d. Severity of Impact
7. Risk Treatment
8. Control deployed

4.2.1 Identification of Assets

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

4.2.2 Asset evaluated Value

The assets [5] of the systems are categorized according to their importance in the organization into Critical, High, moderate, Internal and common. The assets are evaluated on the basis of Confidentiality(C), Integrity(I) and availability(A). These three factors are very important taking into account the evaluation of the assets on the basis of security and reliability of the system. The asset value is calculated by adding the three security factors as follows

Asset value = C+I+A

Confidentiality: The security [6] goal that generates the requirement for protection from intentional or accidental attempts to perform unauthorized data reads. Confidentiality covers data in storage, during processing, and in transit. It is the ability to operate privately

Integrity: The security goal [6] that generates the requirement for protection against either intentional or accidental attempts to violate data integrity (the property that data has when it has not been altered in an unauthorized manner) or system integrity (the quality that a system has when it performs its intended function in an unimpaired manner, free from unauthorized manipulation).The ability of detecting change/modification in the information.

Availability: The security goal [6] that generates the requirement for protection against Intentional or accidental attempts to (1) perform unauthorized deletion of data or (2) otherwise cause a denial of service or data and Unauthorized use of system resources, making the information accessible so that it could be used on demand by authorized entity.

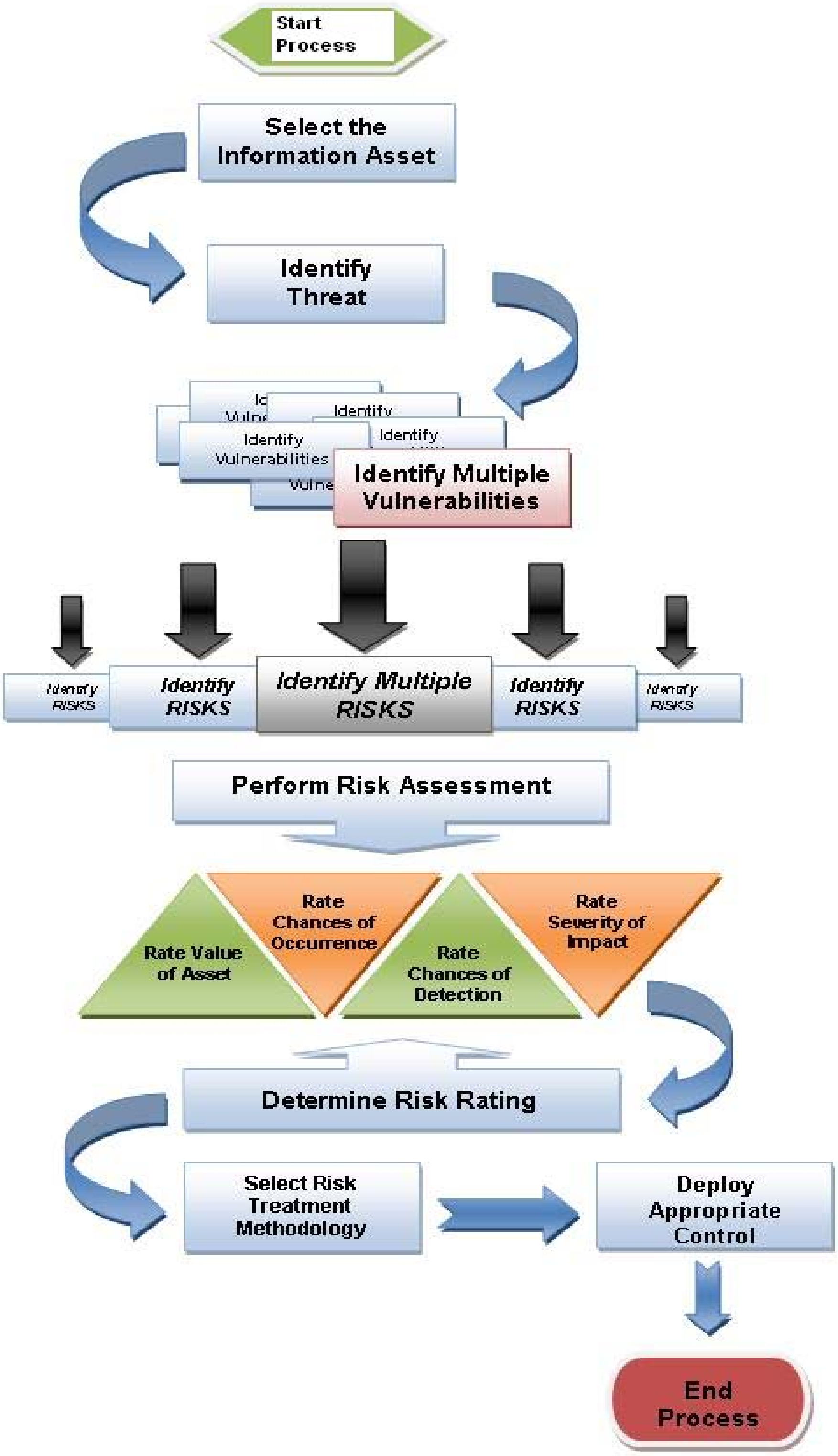


Figure 4.1: Proposed Risk Assessment and Treatment Model

Value in Terms of Priorities	**Description**	**Value in Numeric**
Critical	Assets that affect 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 4.3: Value of Information Asset

4.2.3 Identification of Threat

Threats [5][6] are events that could cause harm to the confidentiality, integrity, or availability of information or information systems. They can be characterized as the potential for agents exploiting vulnerability to cause harm through the unauthorized disclosure, misuse, alteration, or destruction of information or information systems. Threats can arise from a wide variety of sources. Traditionally, the agents have been categorized as internal (malicious or incompetent employees, contractors, service providers, and former insiders) and external (criminals, recreational hackers, competitors, and terrorists). Each of the agents identified may have different capabilities and motivations, which may require the use of different risk mitigation and control techniques and the focus on different information elements or systems.

Generally the threats can be divided into following categories

No	Threat Types	Examples
1	Human	Individual illness, death, robbery, bomb threats, war etc
2	Operational	Loss of access to essential assets, failures in distribution etc
3	Reputational	Loss of business partner or employee confidence, or damage to reputation in the market
4	Procedural	Failures of accountability, internal systems and controls, organization, fraud etc
5	Project	Risks of cost over-runs, jobs taking too long, of insufficient product or service quality, etc
6	Financial	Business failure, stock market, interest rates, unemployment etc
7	Technical	Power failure, heating, ventilation, failure of CPU, failure of system and application software, communication failure etc
8	Natural	Threats from weather, natural disaster, accident, disease etc
9	Political	Changes in tax regimes, public opinion, government policy, foreign influence etc

Table 4.4: Threat Types

4.2.4 Identification of Vulnerabilities

Vulnerabilities [3][5] can be characterized as weaknesses in a system, or control gaps that, if exploited, could result in the unauthorized disclosure, misuse, alteration, or destruction of information or information systems. Vulnerabilities are generally grouped into two types: known and expected. Known vulnerabilities are discovered by testing or other reviews of the environment, knowledge of policy weaknesses, knowledge of inadequate implementations, and knowledge of personnel issues. Adequate and timely testing is essential to identify many of these vulnerabilities. Inadequate or untimely testing may critically weaken the risk assessment.

Expected vulnerabilities [5] to consider are those that can reasonably be anticipated to arise in the future. Examples may include unpatched 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. Although some vulnerabilities may exist only for a short time until they are corrected, the risk assessment should consider the risk posed for the time period the vulnerability might exist. Vulnerability is a defect or weakness in system security procedure, design, implementation, or internal control that an attacker can compromise. It can exist in one or more of the components making up a system, even if those components aren't necessarily involved with security functionality. A given system's vulnerability data are usually compiled from a combination of Operating system and application-level vulnerability test results, code reviews, and higher-level architectural reviews. Software vulnerabilities come in two basic flavors: flaws (design-level problems) or bugs (implementation-level problems). Automated scanners tend to focus on bugs, since human expertise is required for uncovering flaws.

4.2.5 Identification of Risk

Risk identification [5] ascertains what risks or hazards exist or anticipated their characteristics, magnitude, duration, probability of occurrence and recurrence and possible outcomes and consequences. Precise and absolute risk identification is fundamental for effective risk management. In order to manage risks efficiently, they must first be identified. During the 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. Identification involves[7] different types of risks including Software Risks; knowledge of the most common risks associated with Software development, and the platform you are working on and Business Risks which involve the most common risks associated with the business using the Software. Other than these the Testing Risks which have knowledge of the most common risks associated with Software Testing for the platform you are working on, tools being used, and test methods being applied and premature release risk which have ability to determine the risk associated with releasing unsatisfactory or untested Software Products. The Risk Methods includes Strategies and approaches for identifying risks or problems associated with implementing and operating information technology, products and process; assessing their likelihood, and initiating strategies to test those risks

4.2.6 Performing Risk Assessment

Risk assessment is process of analyzing identified risks causing delays in the design, production, or delivery of the system, adversely affect the system's performance, or increase 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 the probability of risk being arise. The maximum probability of the risk can be occurred 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 according to the environment and how frequently a risk can be occurred.

Value in Terms of Priorities	Description	Value in Numeric
Very High	Once in a week	5
High	Once in a month	4
Medium	Once in Six Months	3
Low	Twice in a Year	2
Very Low	Once in a year or less	1

Table 4.5: 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 1and the risk having lowest chances to be detected has a value 5. The probability of detection varies from 1 to 5, from the highest value to the lowest respectively.

Value in Terms of Priorities	Description	Value in Numeric
Very High	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
Very Low	Not possible to detect unless it is occurring	1

Table 4.6: Chances of Risk Detection

The most important is that how strict the impact of a risk can be than the probability to occur and detecting its value. This shows the outcome of the threat[1]. 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 multiple of 2 and vary between the highest "10" and the lowest "2" value.

Value in Terms of Priorities	**Description**	**Value in Numeric**
Critical	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
Internal	Effects on Internal or Moderate Priority Assets	4
Common	Effects on Common Priority Assets	2

Table 4.7: Severity Impact

The following formula is used to perform Risk Assessment:

Risk Rating = [V + O + D] x S (2)

V: Value of Information Asset

O: Chances of Risk occurrence

D: Chances of Risk Detection

S: Severity of Impact

Applying the formula 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. According to the estimated value the control measure is done to reduce the probability of occurrence of risk and its impact to the systems.

Greater the severity of impact greater would be the loss of important factors including confidentiality, integrity and availability[6]

- **Loss of Integrity:** System and data integrity refers to the requirement that information be protected from improper modification. Integrity is lost if unauthorized changes are made to the data or system by either intentional or accidental acts. If the loss of system or data integrity is not corrected, continued use of the contaminated system or corrupted data could result in inaccuracy, fraud, or erroneous decisions. Also, violation of integrity may be the first step in a successful attack against system availability or confidentiality. For all these reasons, loss of integrity reduces the assurance of an organization.

- **Loss of Availability:** If a mission-critical system is unavailable to its end users, the organization’s mission may be affected. Loss of system functionality and operational effectiveness, for example, may result in loss of productive time, thus impeding the end users’ performance of their functions in supporting the organization’s mission.

- **Loss of Confidentiality:** System and data confidentiality refers to the protection of information from unauthorized disclosure. The impact of unauthorized disclosure of confidential information can range from the jeopardizing of national security to the disclosure of Privacy Act data. Unauthorized, unanticipated, or unintentional disclosure could result in loss of public confidence, embarrassment, or legal action against the organization.

4.2.7 Risk Treatment

Risk treatment [2][5] is the process that identifies, evaluates, selects, and implements options in order to avoid or set risk at acceptable levels given constraints and objectives. 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. After identification of risks different [13] methods can be used to mitigate which are as follows:

Risk Avoidance: includes not performing an activity that could carry risk. Avoidance may seem the answer to all risks, but avoiding risks also means losing out on the potential gain that accepting (retaining) the risk may have allowed. Not entering a business to avoid the risk of loss also avoids the possibility of earning profits.

Risk Reduction: involves methods that reduce the severity of the loss or the risk of the loss from occurring. Modern software development methodologies reduce risk by developing and delivering software incrementally. Early methodologies suffered from the fact that they only delivered software in the final phase of development; any problems encountered in earlier phases meant costly rework and often jeopardized the whole project. By developing in iterations, software projects can limit effort wasted to a single iteration. Outsourcing could be an example of risk reduction if the outsourcer can demonstrate higher capability at managing or reducing risks. In this case companies outsource only some of their departmental needs. For example, a company may outsource only its software development, the manufacturing of hard goods, or customer support needs to another company, while handling the business management itself. This way, the company can concentrate more on business development without having to worry as much about the manufacturing process, managing the development team, or finding a physical location for a call center.

Risk Retention: involves accepting the loss when it occurs. True self insurance falls in this category. Risk retention is a viable strategy for small risks where the cost of insuring against the risk would be greater over time than the total losses sustained. All risks that are not avoided or transferred are retained by default. This includes risks that are so large or catastrophic that they either cannot be insured against or the premiums would be infeasible. War is an example since most property and risks are not insured against war, so the loss attributed by war is retained by the insured. Also any amounts of potential loss (risk) over the amount insured is retained risk. This may also be acceptable if the chance of a very large loss is small or if the cost to insure for greater coverage amounts is so great it would hinder the goals of the organization too much.

Risk Transfer: means causing another party to accept the risk, typically by contract or by hedging. Insurance is one type of risk transfer that uses contracts. Other times it may involve contract language that transfers a risk to another party without the payment of an insurance premium. Liability among construction or other contractors is very often transferred this way. On the other hand, taking offsetting positions in derivatives is typically how firms use hedging to financially manage risk.

Some ways of managing risk fall into multiple categories. Risk retention pools are technically retaining the risk for the group, but spreading it over the whole group involves transfer among individual members of the group. This is different from traditional insurance, in that no premium is exchanged between members of the group up front, but instead losses are assessed to all members of the group.

4.2.8 Control Measure Adopted for treatment

Controls [16] are those things which are implemented to prevent the exposure to the threat in the first place, detect if the threat has been realized against the system, and mitigate the impact of the threat against the system or to recover/restore the system. These [20] are safeguards that reduce the probability that a threat will exploit a vulnerability to successfully attack an asset. Identify those safeguards that are currently implemented, and determine their effectiveness in the context of the current analysis.

The institution should identify controls that will mitigate the impact or likelihood of each identified threat agent exploiting a specific vulnerability. Controls [5] are generally categorized by timing (preventive, detective, or corrective) or nature (administrative, technical, or physical). The evaluation should recognize the unique control environment of the institution, and evaluate the effectiveness of that environment in responding to the threats arrayed against it. The evaluation should address the controls that prevent harm as well as those that detect harm and correct damage that occurs. Preventive controls act to limit the likelihood of a threat agent succeeding. Detective and corrective controls are essential to identify harmful actions as they occur, to facilitate their termination, and to reduce damage.

Security controls [6] encompass the use of technical and nontechnical methods. Technical controls are safeguards that are incorporated into computer hardware, software, or firmware (e.g., access control mechanisms, identification and authentication mechanisms, encryption methods, intrusion detection software). Nontechnical controls are management and operational controls, such as security policies; operational procedures; and personnel, physical, and environmental security. The control categories for both technical and nontechnical control methods can be further classified as either preventive or detective.

These two subcategories are explained as follows:

- Preventive controls inhibit attempts to violate security policy and include such controls as access control enforcement, encryption, and authentication.
- Detective controls warn of violations or attempted violations of security policy and include such controls as audit trails, intrusion detection methods, and checksums.

CHAPTER 1: INTRODUCTION

Today's highly connected IT infrastructures exist in an environment that is increasingly hostile. Attacks [14] are being mounted with increasing frequency and are demanding ever shorter reaction times. Often, organizations are unable to react to new security threats before their business is impacted. Managing the security of their infrastructures and the business value that those infrastructures deliver has become a primary concern for IT departments.

An effective risk management process [6] is an important component of a successful IT security program. The principal goal of an organization's risk management process should be to protect the organization and its ability to perform their mission, not just its IT assets. Therefore, the risk management process should not be treated primarily as a technical function carried out by the IT experts who operate and manage the IT system, but as an essential management function of the organization.

An adequate assessment identifies the value and sensitivity of information and system components and then balances that knowledge with the exposure from threats and vulnerabilities. A risk assessment is a pre-requisite to the formation of strategies that guide the institution as it develops, implements, tests, and maintains its information systems security posture. An initial risk assessment may involve a significant one-time effort, but the risk assessment process should be an ongoing part of the information security program. Risk assessments for most industries focus only on the risk to the business entity. Financial institutions must also consider the risk to their customers' information.

Risk assessments should identify, quantify, and prioritize risks against criteria for risk acceptance and objectives relevant to the organization. The results should guide and determine the appropriate management action and priorities for managing information security risks and for implementing controls selected to protect against these risks. The process of assessing risks and selecting controls may need to be performed a number of times to cover different parts of the organization or individual information systems [11]. Risk assessments should also be performed periodically to address changes in the security requirements and in the risk situation, e.g. in the assets, threats, vulnerabilities, impacts, the risk evaluation, and when significant changes occur. These risk assessments should be undertaken in a methodical manner capable of producing comparable and reproducible results.

The scope [11] of a risk assessment can be either the whole organization, parts of the organization, an individual information system, specific system components, or services where this is practicable, realistic, and helpful

For each of the risks identified following the risk assessment a risk treatment decision needs to be made. Possible options for risk treatment include[6]:

- applying appropriate controls to reduce the risks
- knowingly and objectively accepting risks, providing they clearly satisfy the organization’s policy and criteria for risk acceptance
- avoiding risks by not allowing actions that would cause the risks to occur
- transferring the associated risks to other parties, e.g. insurers or supplier

1.1 Historical Background of Risk Analysis

Historical perspective [15] on risk analysis applications in society was given by Covello and Mumpower (1985). Around 3200 B.C. in the Tigris-Euphrates valley, a group called Asipu served as risk analysis consultants for people making risky, uncertain, or difficult decisions Greeks and Romans observed causal relationships between exposure and disease: Hippocrates (4th century B.C.) correlated occurrence of diseases with environmental exposures; Vitruvious (1st century B.C.) noticed lead toxicity; and Agricola (16th century A.D.) noticed the correlation between occupational exposure to mining and health.

Modern risk analysis has roots in probability theory and the development of scientific methods for identifying causal links between adverse health effects and different types of hazardous activities: Blaise Pascal introduced the probability theory in 1657; Edmond Halley proposed life-expectancy tables in 1693; and in 1792, Pierre Simon de LaPlace developed a true prototype of modern quantitative risk analysis with his calculations of the probability of death with and without smallpox vaccination. With the rise of capitalism, money use, and interest rates, there was an increased use of mathematical methods dealing with probabilities and risks. For example, the risk of dying was calculated for insurance purposes (life-expectancy tables). Physicians in the Middle Ages also observed a correlation between exposures to chemicals or agents and health: John Evelyn (1620–1706) noticed that smoke in London caused respiratory problems. He also noticed correlation of scrotal cancer with occupational exposures to soot in chimney sweeps.

1.1.1 Problem Statement

“To determine the comparative analysis of strategic and commercial organization and propose risk assessment and treatment model for Strategic organization”

1.1.2 Breakdown of Report

Chapter 1 is a brief introduction of risk assessment, it importance in any organization and the problem statement. Chapter 2 consists of all the related methodologies of risk assessment and treatment. Chapter 3 contains the basic concepts, definitions and explanation related to risk management and its importance in software development lifecycle. Chapter 4 includes the comparative analysis of risk assessment between strategic and commercial organization through their similarities and differences. A new proposed model is developed for performing risk assessment and treatment for strategic organization. Chapter 5 is related to the application of model and results after applying in Commercial and Strategic Organization. The screen shots of the tool developed for generating compiled result for specific risk. Further the proposed work is compared with already defined models. The last chapter 6 includes conclusion and future work.

CHAPTER 2: EXISTING METHODOLOGIES

2.1 CRAMM

2.1.1 Introduction

CRAMM (CCTA Risk Analysis and Management Method) was created in 1987 by the Central Computing and Telecommunications Agency (CCTA) of the United Kingdom government. CRAMM is developed to provide the following:

- A sound approach to identifying threats and vulnerabilities, and thus being able to establish a sound basis for identifying and stating risks
- A more justifiable approach for management to understand risks
- A basis for potential savings, in terms of the cost of security; and
- A sound approach to improve levels of information and supporting system assets protection.

CRAMM [19] is more of a qualitative methodology than a quantitative methodology and, in broad terms, treats security risk assessment as an evaluation of the risks, and security risk management as the identification of the countermeasures to combat the risks. All aspects of security are addressed within the methodology; namely, personnel security, physical security and security of information. It can handle deliberate and accidental threats, and encompasses existing UK government security policy and guidance. For NATO, a NATO profile has been developed, based on NATO security policy and supporting directives and guidance in order to make the tool easier to use and more specifically tailored to NATO CIS. The methodology allows to use the tool to establish a baseline of information for an organisation or project at any time during its life-cycle, and provides a comprehensive “what-if” capability. This allows to model different scenarios, to assess the impact of changes in a system environment, or changes in policy and directives. It also provides a capability for follow-up reviews, using the previously established baseline of information.

2.1.2 Description

There are three fundamental stages to a CRAMM review, which correspond to the stages identified in the current NATO security risk assessment guidance and are, in broad terms, the following:

- Stage one – Assessing the value of the information, and identifying the assets which support the business process
- Stage two – Identifying what threats may affect the system and how vulnerable is the system to those threats; arriving at a conclusion about the risks
- Stage three – Identifying how the risks can be countered, including what improvements are required to existing control measures

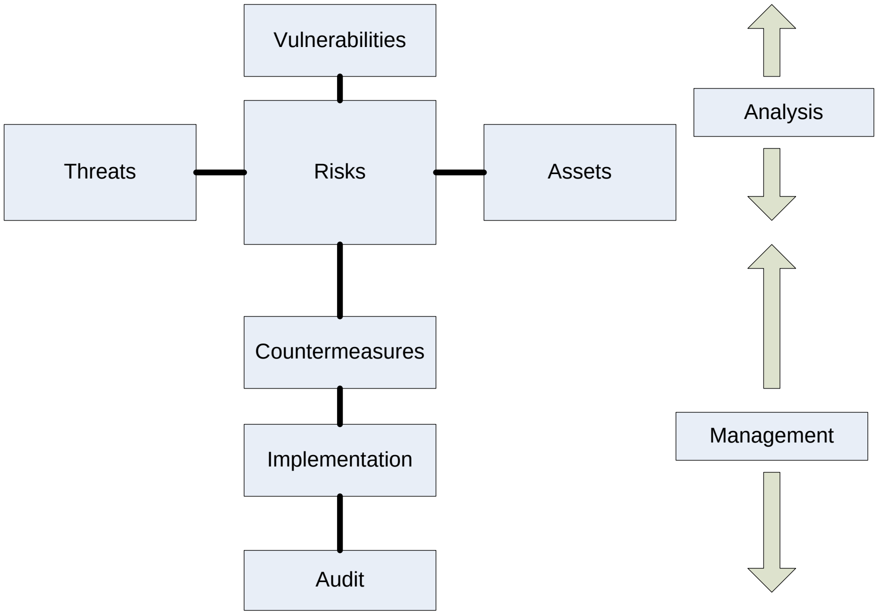


Figure 2.1 CRAMM [19]

Between each stage, there is the capability to produce comprehensive management reports, and conduct management reviews to ensure that the baseline of information is valid.

In stage one, at the start, it is important to identify the purpose of the CRAMM review, where the boundaries of the review are, and the schedule for the review. Equally important is the establishment of a baseline questionnaire (which the tool provides) from which you establish all the information about the physical and data assets. From this, you build up asset models, which show the relationship between data assets and those assets which support those data assets (for example, a computer room and its hardware).

The next step is to apply a valuation to the assets; data assets are valued in terms of impact of disclosure, modification, unavailability and destruction (this is qualitative information based on interviews with the users of information); physical assets are valued in terms of their replacement cost (quantitative information). At the end of this stage, it is recommended to carry out a management review to ensure that you have a sound baseline of information, before moving forward to the next stage. The stage 1 management review helps ensure at an early stage in the risk management process that there is agreement between the operational and security accreditation authorities as to the assets to be protected, and their value to the organization.

In stage two, you move into the threat and vulnerability assessment. The types of threat that are addressed include the following:

- Logical threats – For example, hacking, unauthorized use of an application, and malicious software
- Communications threats – For example, communications infiltration, and mis-routing
- The threat of technical failures to communications and information systems hardware and software
- Errors by people – For example, system management errors, or errors by users
- Physical threats – For example, theft, willful damage, terrorism, fire, water damage, and natural disasters.

The tool contains a built-in, very extensive library of potential threats and vulnerabilities. The threats can either be based on specific knowledge about previous security incidents, or on generic information.

The vulnerabilities are based on an understanding of the functions and capabilities that are available within the system environment. The threat and vulnerability assessment arrives at qualitative statements for the threats (in terms of very low, low, medium, high, and very high) and vulnerabilities (in terms of low, medium and high).

The next step is to derive measures of risk, and these are derived from a combination of the threat, the vulnerability, and the asset value. The measures of risk are scaled, so that the security requirements to be established are matched to the degree of risk. Again, at the completion of this stage, a further management review is recommended to ensure the validity of the information, before moving forward to select countermeasures.

In stage 3, the final stage, the countermeasures, dependent upon the scale of the risk, are selected. The tool contains countermeasures groups for each individual threat, addressing, for example, identification and authentication, access control, and physical security. Within each countermeasure group, you have the following structure:

- A policy statement can be derived, verbatim, from the appropriate security policy document or supporting directives or guidance documents;
- The security objective of applying this particular countermeasure;
- Detailed descriptions of the functions associated with the countermeasure; and
- Specific ways, or options, in which the functionality can be provided.

The capability also exists to apply the costs of the countermeasures (both in financial and man-effort terms). Having selected countermeasures, a management review meeting is required to examine the countermeasures, consider those which may not be applicable, identify those for implementation, and identify those aspects where the risk is to be accepted. A powerful aspect of the tool, which is very relevant here, is the back-track capability. This means that you can, if you are not certain why a particular countermeasure has been recommended, review the asset / threat / vulnerability information that led to the countermeasure decision.

All through the stages, varying degrees of management reports can be produced, depending upon the target audience. One of the benefits, in the final stage, is the ability to produce the security-related documentation used in the accreditation process.

2.2 Canadian TRA Methodology

The [23] Communications Security Establishment, a Canadian security lead agency, has developed a series of risk management1 documents to help government departments in meeting the Government of Canada Security Policy (GSP) requirements. The following documents expanded on the standards set out in the GSP:

- MG2 – Risk Management Framework for Information Technology (IT), 1996. The MG2 provides specific guidance for risk management within an IT system environment and its life cycle;
- MG3 – A Guide to Risk Assessment and Safeguard Selection for Information Technology Systems, January 1996. The MG3 provides specific guidance for risk assessment and safeguard selection process throughout the IT system life cycle;
- MG4 – A Guide to Certification and Accreditation for Information Technology Systems, January 1996. The MG4 provides more specific guidance for the certification and accreditation of an IT system throughout its life cycle
- ITSG-04 – The ITSG-04 provides guidance to an individual (or a departmental team) in carrying out a Threat and Risk Assessment (TRA) for an existing or proposed IT system.

The MG series provides a solid guidance for risk management to managers but lack methodology to assign risk values. A working group was created to develop a TRA working guide to be included as a part of risk management processes.

In addition to CSE efforts in developing a TRA guideline, the Royal Canadian Mounted Police (RCMP) had undertaking initiatives in the same area. As the lead department for federal law enforcement, with a crime prevention mission, the RCMP is also responsible to provide advice to departments on the process of threat and risk assessments and the conduct of IT system security reviews, inspections and audits.

2.2.1 Using TRA in Risk Management

Risk management is the process by which resources are planned, organized, directed, and controlled to ensure the risk of operating a system remains within acceptable bounds at near-optimal cost.

Risk management is an iterative and cumulative process. The following figure outlines the Canadian overall risk management process which involves: planning; the TRA; selection of safeguards; system certification and accreditation; maintenance; and monitoring and adjustments to safeguard selections. Traditional prescriptive approach of mandating (i.e. "shall" implement) specific security controls for systems are not cost effective or are too complex. The current Canadian approach to risk management is a mixed approach that is prescriptive and threat-based. Minimum standards set the prescribed safeguards, which are supplemented through a threat-based process. However, this approach is silent on how minimum standards are established: Minimum standards should also be determined through a risk management process involving a TRA. It would be interesting to get a single global risk management process because both measure similar risks.

The TRA in this model is functional and provides the current level of **R**isk caused by the **T**hreat Agents acting on the Critical **A**ssets of an Information System given its **V**ulnerabilities. More precisely, the risk is a function of the values of the assets, the threat agent attributes, and the vulnerabilities, or $R = f$ (AVal, T, V). Note that R is a probabilistic measure of harmful impacts of a given type on a system (IT-system) and they are many possible impact types.

2.2.2 Risk Management Tools

The current Government of Canada (GoC) information technology risk management scheme is supported by these two basic methodologies, the ITSG-04 and the RCMP TRA guidelines. It must be noted that many government departments have developed their own methodologies to suit their environment but the root to those remains the formal two basic methods with the occasional insight derived from sources such as the National Institute of Standards and Technology Risk framework

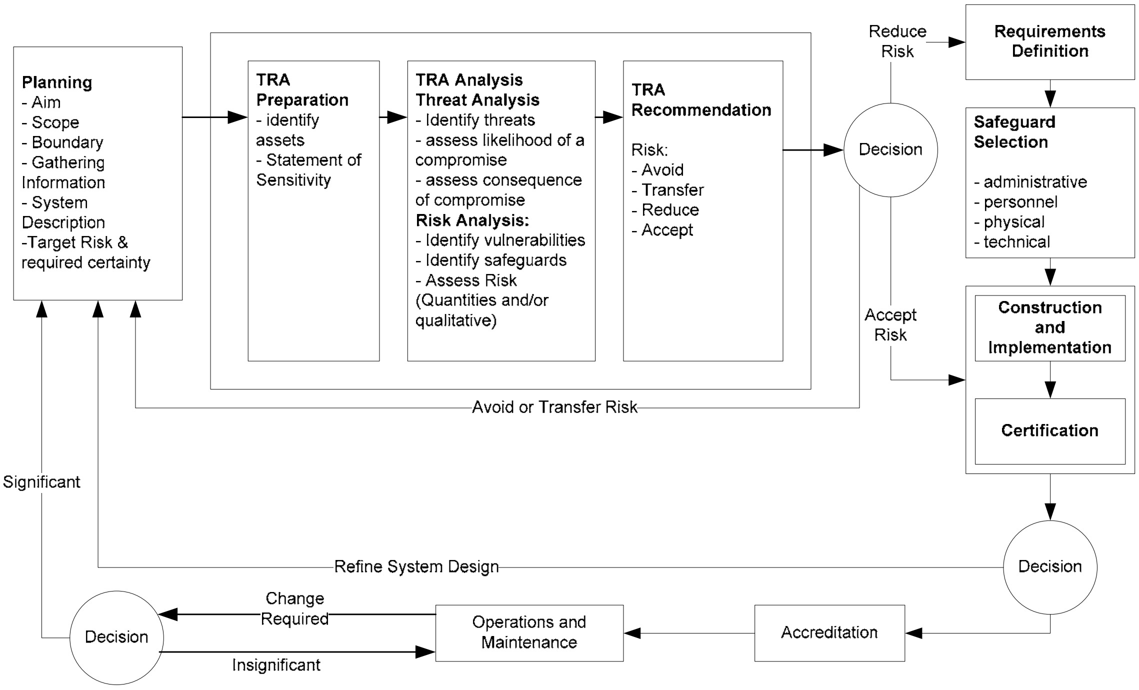


Figure 2.2. Risk Management Model[23]

2.3 US Model

2.3.1 Introduction

The United States has not standardized on any particular risk assessment tool or methodology. Although several tools have been evaluated, each seems to rely on subjective information depending on the system under review, the environment in which it resides and the person performing the evaluation. National Risk Analysis

Methodologies are available, but no single methodology has been adopted or is applicable to all systems and all cases. Methodologies vary depending upon the level of assets requiring protection.

For instance a more rigorous process is required for systems which process highly sensitive information.

2.3.2 Objective

The objective of this section is to provide information about risk methodologies used by both National and Federal agencies within the United States. Furthermore, it will define common steps to determine system risk; it is highly likely that these steps are consistent with international risk methodologies.

2.3.3 Basic Risk Methodology

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30 and the Federal Information Security Management Act (FISMA) of 2002 provide a foundation for the general risk methodology used within the United States. NIST SP 800-30 is the risk management guide for general information technology systems and FISMA outlines a mandatory set of processes that must be followed for all information systems used or operated by U.S. Government federal agencies or by contractors or other organizations on behalf of U.S. Government agencies. These documents are complementary and provide a model to manage risk associated with information technology systems.

2.3.3.1 Risk Assessment

The basic steps which apply to risk assessment are depicted in Figure 2.3

Step 1: Characterize the system in terms of scope and boundary. A system may be a single device or a network of computers supporting a common purpose and managed by a single system owner. It may also include assets such as buildings, personnel and network security components. The US Department of Defense (DoD) implements the DoD

Information Technology Security Certification and Accreditation Process (DITSCAP) to document systems used within U.S. DoD.

Step 2: Threat Identification. Threats can be categorized as Natural, Human or Environmental. Natural threats are generally related to weather or earthly disturbance such as earthquakes, floods, tornadoes, lightning, etc. Human threats can be intentional or unintentional and are perpetrated by humans. Environmental Threats can be intentional or unintentional and include items such as chemical hazards, pollution and power fluctuations.

Step 3: Vulnerability Identification may be information obtained from multiple sources, such as open literature, previous security testing, intelligence, etc. Vulnerabilities may include weak system security practices such as easily guessed passwords, lack of physical security, untrustworthy personnel, failure to maintain and update software such as virus scanning and lack of life cycle support.

Step 4: Control Analysis is the determination of countermeasures to thwart an attacker from exploiting vulnerabilities. Countermeasures can include procedures such as training and implementing strong security polices. It can also include software, hardware and personnel, for instance hosting systems in physically secure spaces with a guard force in place.

Step 5: Likelihood determination is the process by which an evaluator systematically weighs the extent to which a potential vulnerability will be exploited. Factors used to determine likelihood are motivation and ability of the perpetrator, identified system vulnerabilities and existing countermeasures. For instance a system processing highly sensitive information might be a sought after target for adversaries. However, the risk of detection and attribution could be extremely high. These elements must be balanced to determine the likelihood that a potential attacker would be prone to mount an attack.

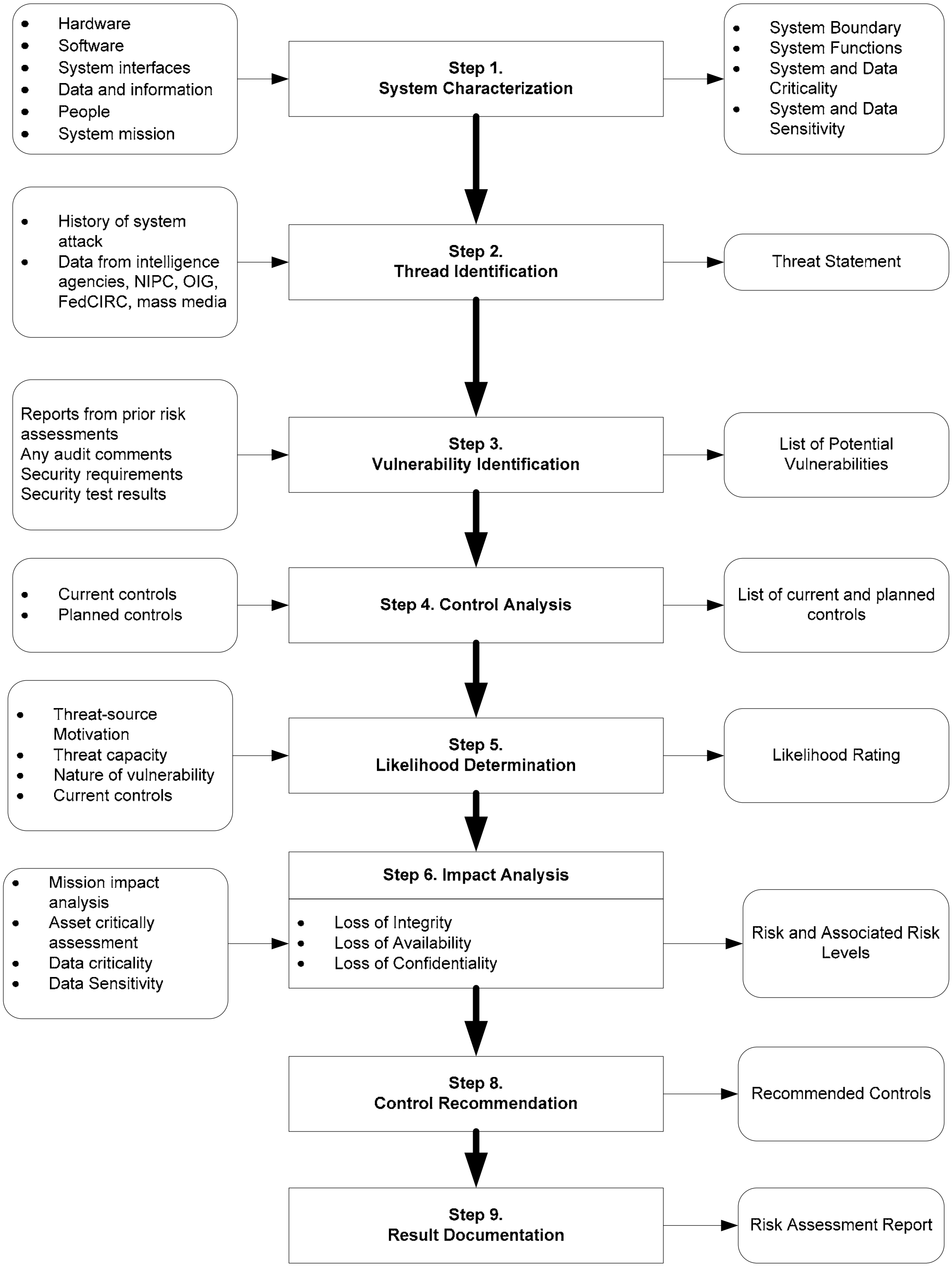


Figure 2.3. Risk Assessment Methodology Flow Chart[23]

The likelihood that a potential vulnerability could be exercised by a given threat-source may be described as high, medium, or low (or more granularly). Table 2.1 below describes three basic likelihood levels

Likelihood Level	Likelihood Definition
High	The threat-source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective
Medium	The threat-source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability
Low	The threat-source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised

Table 2.1: Likelihood Definitions[23]

Step 6: Impact Analysis is based on a combination of elements and how they affect each other. First, a determination of the impact a successful exploitation may have on the system is required. The evaluator must work with system site personnel and review documentation describing the system. All US Government systems must abide by the DoD Information Technology Security Certification and Accreditation Process (DITSCAP). This is a formal process which documents a system from initial implementation through life cycle management. It includes the operating environment, system security architecture and boundaries, personnel responsible for system maintenance and security, test plans, procedures and results. Once the evaluator has a thorough knowledge about the sensitivity and criticality of the system and its operating environment an impact analysis can be determined. Impacts may be measured in the general terms; High, Medium and Low (or may contain greater granularity).

An impact analysis can be used to determine cost-benefit criteria. Implementing policy controls such as complex passwords to discourage unauthorized access is an example of a low cost mitigation with high benefit potential. For highly sensitive systems a more rigorous security posture may be required and the cost of implementing additional security features may be high. Each system undergoing impact analysis will be unique. Although there may be many similarities, each system must be treated independently and its security mechanisms and environment must be balanced to produce an acceptable level of risk for the system security manager.

Magnitude of impact	**Impact Definition**
High	Exercise of the vulnerability: 1) May result in the highly costly loss of major tangible assets or resources; 2) May significantly violate, harm, or impede an organization’s mission, reputation, or interest; or 3) May result in human death or serious injury.
Medium	Exercise of the vulnerability: 1) May result in the costly loss of tangible assets or resources; 2) May violate, harm, or impede an organization’s mission, reputation, or interest; or 3) May result in human injury.
Low	Exercise of the vulnerability: 1) May result in the loss of some tangible assets or resources; or 2) May noticeably affect an organization’s mission, reputation, or interest.

Table 2.2: Magnitude of Impact Definitions[23]

Step 7: Risk determination is a compilation of information obtained in Steps 1 through 6. The U.S has not standardized on any quantifiable risk methodology formula. The basis for determining risk is common

Risk associated with any system is a function of the comparison of known vulnerabilities, an adversary's inclination and ability to exploit those vulnerabilities and the consistency of security management throughout the life cycle of the system. Unfortunately, the determination of risk level is more dependent on the thoroughness of system documentation and experience of the evaluator than on any methodology.

Step 8: Control recommendation is the process by which mitigations are introduced to reduce or minimize system risk. Control recommendations are based on the risks identified in Step 7. Control mechanisms may be physical, procedural, software or policy based. A determination must be made as to which control mechanisms to implement, this determination may be based on feasibility, operational impact, effectiveness, level of security required, cost and level of risk acceptance.

Step 9: Resulting documentation is the residual risk after security controls have been implemented. This document serves as a resource for managers to understand remaining risks and vulnerabilities associated with their information system. Under FISMA and DITSCAP, U.S. Federal agencies use resulting documentation as basis for accrediting a system, whereby the accreditation authority accepts risk for the system and issues an authority to operate (ATO).

2.4 Czech Methodology

Czech methodology is used for risk analysis. It calculates the risk value through asset value, vulnerability and the chance to occur a threat.

The main steps of this method are:

- Assets identification;
- Threats identification;
- Evaluation of Probability of Threats realization;

- Evaluation of Vulnerability of Assets to the Threats; and
- Calculating of Risk value for every Asset and Threat pair.

After identifying the assets, they are valuated. Assets value vary from 0 (negligible: Asset loss, damage or security violation has only slight or no influence on IS operation and security) to 5 (very high: Asset loss, damage or security violation means outage of the whole IS operation or perhaps total loss of IS security as a whole or important part).

The values should be applied to the costs of obtaining and maintaining a particular Asset and also to the potential impact on organization behavior in case of loss or damage of the Asset.

Criteria used to determine assets values:

- Non compliance with law and/or regulations;
- Damage or break-up of business;
- Loss of good reputation, negative influence on organization image;
- Reduction of security for organization members;
- Unfavorable impact of law;
- Violation of business secret;
- Breaching the purchase order
- Financial loss.

The threat probability is estimated by a value from 0 (the threat cannot occur) to 6 (the threat occurrence is certain or the threat occurs often or regularly or it is a case of continuously threatening status (defect) assessment).

Vulnerability evaluation is then performed. It includes identification of:

- Weak point; and
- Existing security mechanisms.

Weak points can be:

- Physical environment;
- Employees, management and administrative procedures a mechanisms; and
- HW, SW, communication equipment, company premises, etc.

Weak points can be used by the threat to damage assets and business procedures supported by assets. Vulnerabilities are reduced by existing security mechanisms.

An asset vulnerability to the threat is estimated from 0 (the threat cannot occur for the asset) to 4 (the asset is insufficiently resistant to the threat occurrence or is not protected at all).

The risk value is calculated with the following formula:

Final risk = Asset value * Probability of threat occurrence * Vulnerability of assets group

According the value of the final risk are defined as:

- High risk in the range 61 – 90
- Medium risk in the range 31 – 60
- Low risk in the range 1 – 30

2.5 Spanish Method MAGERIT

MAGERIT risk analysis is a methodical approach to determine the risk, following specific steps:

- Determine the relevant assets for the organization, their inter-relationships and their value i.e. what prejudice (cost) would be caused by their degradation.
- Determine the threats to which those assets are exposed.
- Determine what safeguards are available and how effective they are against the risk.
- Estimate the impact, defined as the damage to the asset arising from the appearance of the threat.
- Estimate the risk, defined as the weighted impact on the rate of occurrence (or the expectation of appearance) of the threat.

In order to organize the presentation, steps 1, 2, 4 and 5 are handled first, skipping step 3, so that any estimates of impact and risk are “potential” if no safeguards are deployed. Once this theoretical scenario is obtained, the safeguards are incorporated in step three, providing realistic estimates of impact and risk.

2.5.1 Assets

The assets are the resources in the information system or related to it that are necessary for the organization to operate correctly and achieve the objectives proposed by its management.

A type can be assigned to each asset. Dependencies can also be established . A “higher asset” is said to depend on the “lower asset” when the security needs of the higher one are reflected in the security needs of the lower one. In other words, when the appearance of a threat in the lower asset has a prejudicial effect on the high asset. Informally, this could be interpreted as the lower assets being the pillars that support the security of the higher assets. Although it is necessary to adapt to the organization being analyzed in each case, the group of assets can frequently be structured into layers, where the upper layers depend on the lower ones.
Assets are the valuated, either in a qualitative or quantitative way.

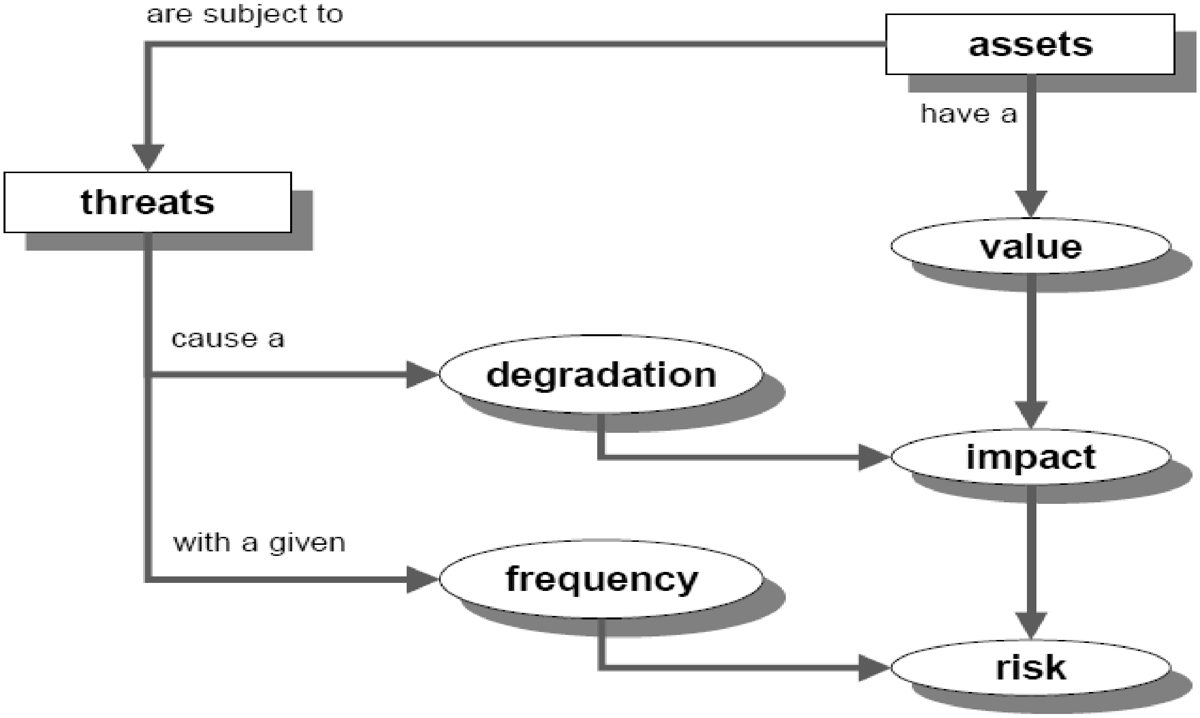


Figure 2.3 MAGERIT Main Steps[23]

2.5.2 Threats

The next step is to determine the threats that may affect each asset.

Once it has been determined that a threat may damage an asset, the asset’s vulnerability6 must be estimated considering two aspects:

- Degradation: The amount of damage done to the asset.
- Frequency**:** How often the threat appears.

Degradation measures the damage caused by an incident if it occurs. Degradation is often described as a part of the asset’s value and therefore expressions appear such as that an active has been “totally degraded,” or “very slightly degraded”. When the threats are not intentional, it is probably enough to know the physically damaged part of an asset in order to calculate the proportional loss of value. But when the threat is intentional, one cannot think of proportions since the attacker may cause a great deal of damage selectively.

Frequency puts degradation into perspective since one threat may have terrible consequences but very unlikely to occur while another threat may have very small consequences but are so frequent as to accumulate into considerable damage.

Frequency is modeled as an annual occurrence rate with the following typical values

100	Very frequent	Daily
10	Frequent	Monthly
1	Normal	Annually
1/10	Infrequent	Every few years

Table 2.3: Frequency Table[23]

2.5.3 Determination of the Impact

Impact is the measurement of the damage to an asset arising from the appearance of a threat. By knowing the value of the assets (in various dimensions) and the degradation caused by the threats, their impact on the system can be derived directly.

2.5.3.1 Accumulated Impact

This is calculated for an asset taking into account:

- Its accumulated value (its own plus the accumulated value of the assets that depend on it).
- The threats to which it is exposed.

The accumulated impact is calculated for each asset, for each threat and in each evaluation dimension, being a function of the accumulated value and of the degradation caused.

Because the accumulated impact is calculated on the assets that carry the weight of the information system, it allows the determination of the safeguards to be adopted in the working media: protection of equipment, back-up copies, etc.

2.5.3.2 Deflected Impact

This is calculated for an asset taking into account:

- Its intrinsic value.
- The threats to which the assets on which it depends are exposed.

The deflected impact is calculated for each asset, for each threat and in each valuation dimension, being a function of the intrinsic value and of the degradation

Because the deflected impact is calculated on assets that have their own value, it allows the determination of the consequences of the technical incidents on the mission of the information system. It is therefore a management presentation that helps in making one of the critical decisions of a risk analysis: accepting a certain level of risk.

2.5.3.3 Aggregation of Impact Values

The above paragraphs determine the impact of a threat on an asset in a certain dimension. These single impacts may be aggregated under certain conditions:

- The deflected impact on different assets may be aggregated.
- The accumulated impact on assets that are not inter-dependent and that do not depend on any higher asset may be aggregated.

- The accumulated impact on assets that are not independent must not be aggregated because this would imply overrating the impact by including the accumulated value of the higher assets several times.
- The impact of different threats on the same asset may be aggregated although it is useful to consider to what measure the different threats are independent and may be concurrent.
- The impact of a threat in different dimensions may be aggregated.

2.5.4 Safeguards

The above steps have not included the safeguards deployed. Thus, the impacts and risks to which the assets would be exposed if they were not protected in any way are measured. In practice, it is unusual to find unprotected systems: the measures described indicate what would happen if the safeguards were removed.

Safeguards enter into the calculation of the risk in two ways:

2.5.4.1 Reducing the frequency of threats

These are called preventive safeguards. Ideally, they completely prevent a threat from occurring.

2.5.4.2 Damage limitation

There are safeguards that directly limit any degradation while others allow the immediate detection of the attack to stop the progress of the degradation. There are even some safeguards that are limited to allowing the quick recovery of the system when the threat destroys it. In all of these versions, the threat occurs but the consequences are limited.

As well as being classified by their existence, safeguards are also classified by their effectiveness against the risk that they prevent.

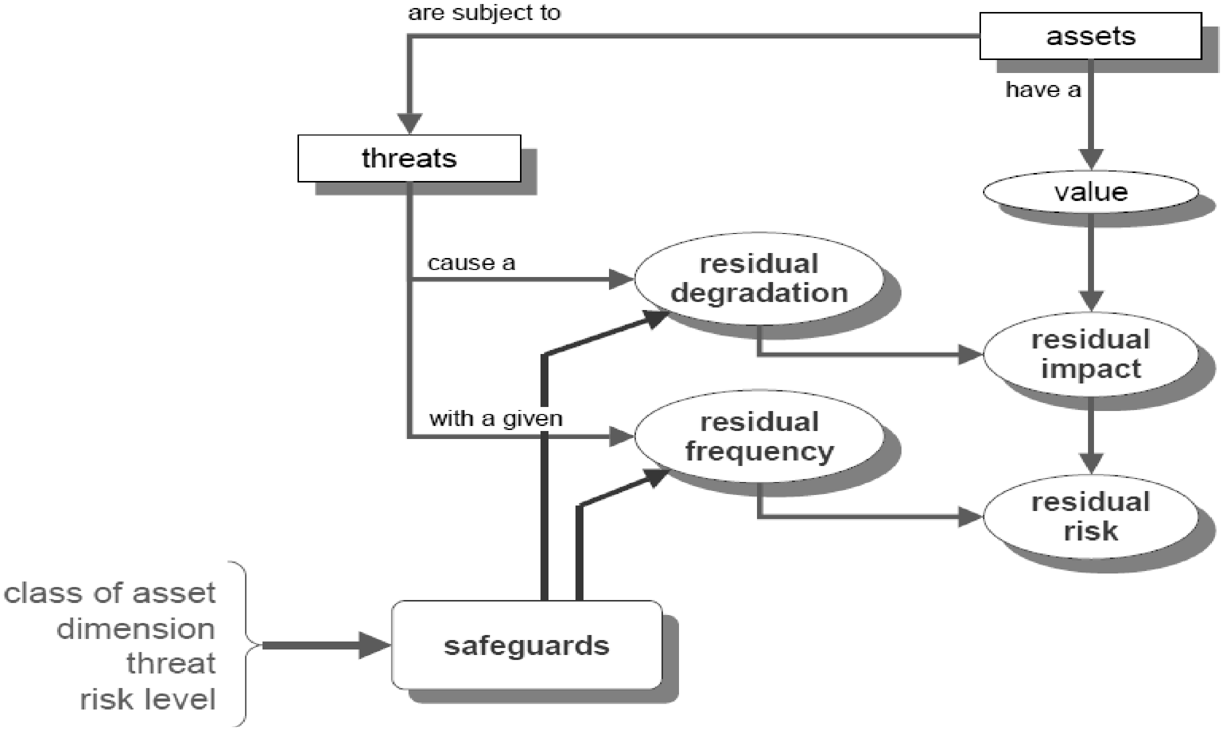


Figure 2.4. MAGERIT Main Steps including Safegaurds[23]

2.5.5 Residual Impact

The calculation of the residual impact is simple. Since neither the assets nor their dependencies have changed, only the size of the degradation, the impact calculations are repeated with this new degradation level.

The size of the degradation, taking into account the effectiveness of the safeguards, is the proportion that remains between perfect effectiveness and real effectiveness.

The residual impact may be accumulated on the lower assets or deflected on the higher assets.

2.5.6 Residual Risk

The calculation of the residual risk is simple. Since neither the assets nor their dependencies have changed, only the size of the degradation and the frequency of threats, the risk calculations are repeated using the residual impact and the new rate of occurrence.

The size of the degradation is taken into consideration in calculating the residual impact. The size of the frequency, taking into account the effectiveness of the safeguards, is the proportion that remains between perfect effectiveness and real effectiveness.

The residual risk may be accumulated on the lower assets or deflected on the higher assets.

2.6 BEATO

BEATO [18] (sometimes spelled BeATo) stands for "BEnchmark Assessment TOol". Some people refer to it as "Be At zero", meaning the ideal of lowering non-compliance and risk. BEATO is both a tool and a methodology, originally dedicated to Security assessments. It determines the quality of controls as well as the degree of compliance using a Capability Maturity Model.

It allows management to evaluate their current level of security (via consolidations of individual assessments and drill-down), as well as the effects of decisions and projects undertaken for the purpose of improving security.

Both methodology and tool have been developed by Unisys for internal use, originating from 1999 (Y2K compliance). Since 2002 BEATO (and BEATO assessment services) have been marketed to Unisys clients.

BEATO can also be used for compliance assessment relative to all ISO Standards (specifically ISO 9000, ISO/IEC 20000, ISO 27000) with the integral PLATO Risk Management module (PLAnning TOol).

CHAPTER 3: RISK MANAGEMENT

There are same basic concepts required for understanding the process of risk management. The important definitions related to this research work are as follows:

3.1 Strategic Organization

A not-for-profit organization monitoring and performing the military/defense oriented activities of a country. Their objectives are associated with defense of the country they are appointed in and they don’t have any commercialization or commercial competition.

3.2 Commercial Organization

Mostly a Profit earning organization (unless it’s an NGO), their objective is to operate, earn profit and market their Products or Services to general public or even strategic organizations. They are usually not the only organization with such objectives in a single region.

3.3 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”. Assets can be tangible including computers, facilities and supplies etc or intangible which includes reputation, data and intellectual. It is usually difficult to compute the values of intangible assets because it may change with the passage of time.

Assets are organization’s resources used to perform operations, e.g. Human Resource, Computers, Networks, Software, Tables, Cupboards, Files, etc. (Anything that has value to the organization)

3.4 Information Asset

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.

3.5 Threat

A potential cause of an unwanted incident, which may result in harm to a system or organization. The threat is “invariably the danger a malicious agent poses and that agent’s motivations (financial gain and prestige etc).” Threats mark themselves as direct attacks on security of system [10]. Also it is a potential cause of an unwanted incident, which may result in harm to a system or organization

3.6 Vulnerability

A weakness of an asset or group of assets that can be exploited by one or more threats. 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”. The reason to resist against the actions can be due to the weaknesses in software or hardware. To model the vulnerability threat capability and system threat resistance are needed.

3.7 Risk

It is combination of probability of an event and its consequences. It indicates [8] both the impact of the cooperation of an asset and the possibility for it being conciliation. less likely and less damaging are dealt with after the more important risks. The risks [9] need to be concentrated on the design, architecture and functionality of the product to provide the implementation procedures and the required maintenance

3.8 Risk Analysis

The process of identifying the most probable threats to an organization and analyzing the related vulnerabilities of the organization to these threats

3.9 Risk Assessment

The process of analyzing the risk’s chances of occurrence and its impact on organization’s operations and assets. It involves systematic approach to calculate the size and then its significance. It [9] is a process in which different types of risks, their effect on the system are determined. After analysis the risks are prioritized according to the size and timing property.

3.10 Risk Treatment

The Process of selecting the appropriate measures to modify the status of risk (a risk's impact can be reduced but it cannot be eliminated). There are four stages of Risk Treatment;

a. Risk Avoidance: Avoid the activity that can create the risk under observation
b. Risk Mitigation: Deploy a control to reduce the effect of risk
c. Risk Transfer: Outsourcing the responsibility to manage risk and its mitigation to another party
d. Risk Acceptance: Not taking any actions as the impact of risk is very minimal

3.11 Risk Management

The process of Risk Assessment and Treatment, so that to prevent the occurrence of risk. It is the method [11] of coordinated activities to direct and control an organization with regard to risk. Risk management typically includes risk assessment, risk treatment, risk acceptance and risk communication

3.12 Business Continuity Plan

A Backup Plan required to be deployed in case Risk Treatment Plan fails and the risk occurs, the primary objectives of this plan are to ensure continuity of critical operational activities during risk occurrence and recovery to original state

3.13 Disaster Recovery Plan

When business continuity plan involves use of a separate site (usually in case of total site loss), it's called a disaster recovery plan

3.14 Risk Management

Risk management [7] is a structured approach to managing uncertainty through, risk assessment, developing strategies to manage it, and mitigation of risk using managerial resources. It is the culture, processes, and structures that are directed towards the effective management of potential opportunities and adverse effects [21]. The strategies include transferring the risk to another party, avoiding the risk, reducing the negative effect of the risk, and accepting some or all of the consequences of a particular risk. Some traditional risk managements are focused on risks stemming from physical or legal causes (e.g. natural disasters or fires, accidents, death and lawsuits). Financial risk management, on the other hand, focuses on risks that can be managed using traded financial instruments.

Effective risk management [12] does not provide a guarantee against failure. Even in companies with the best risk management people and systems, large losses can and will occur as long as taking the risk of large losses increases expected profits sufficiently for top management to be willing to take that risk. With good risk management, such losses will be attributable to an unlucky “draw,” to a one-in-a-hundred event. Ultimately, the likelihood of such large losses will depend on choices made by those entrusted with determining the risk appetite of organization. Risk management ensures that top management knows and understands the probabilities associated with possible outcome of the strategy of organization before the decisions are made to commit its capital

3.14.1 Objective of Risk Management

Objective of risk management is to reduce different risks related to a preselected domain to the level accepted by society. It may refer to numerous types of threats caused by environment, technology, humans, organizations and politics. On the other hand it involves all means available for humans, or in particular, for a risk management entity (person, staff, organization).

3.14.2 Principles of Risk Management

The [13] International Organization for Standardization identifies the following principles of risk management. Risk management should

- Create value.
- Be an integral part of organizational processes.
- Be part of decision making.
- Explicitly address uncertainty.
- Be systematic and structured.
- Be based on the best available information.
- Be tailored.

- Take into account human factors.
- Be transparent and inclusive.
- Be dynamic, iterative and responsive to change.
- Be capable of continual improvement and enhancement

3.14.3 Risk Management Phenomenon

Risk Management is a process of identifying activities, assets or external/internal sources that can negatively affect an organization’s operations. It is applicable on all types of management structures like for Information Security Management System (ISMS), Environmental Management System (EMS), Occupational Health and Safety Management System (OH&S), operational management through Quality Management Process (QMS), etc. Every management system has its own agendas; therefore all of them come up with their own objectives and end deliverables. Difference in prime objectives, also effects the point of view required to assess the risks associated with each activity. For example, Fire is a threat and risks associated with ISMS, EMS and OH&S will vary because of the differences between the practices;

Management Practices	**Threat**	**Probable Vulnerability**	**Probable Risk**
ISMS	Fire	Assets are vulnerable to fire and electricity can create a fire hazard	Damage to asset and interruption in critical operational activity
EMS	Fire	Flammable items used in process	Air Pollution is produced in case of flammable items catching fire
OH&S	Fire	Flammable items and human resource with low understanding of fire management	Death of workers

Table 3.1: Management Practices and Probable risk

In Table 3.1, three different practices are considered for the same threat i.e. “Fire”, but the outcomes and the assessment of vulnerabilities in all three cases is different. But, remember, treatment measures to control “Threat” or to overcome “Vulnerabilities” may be same in all cases, e.g. installation Fire extinguishers in all hazardous areas (where Fire can occur).

The ISMS [11] is “considered to ensure the selection of adequate and proportionate security controls that protect information assets and give confidence to interested parties”. The EMS involves all the resources and all aspects of the organization that influence the environment. The organization’s environmental performance can be improved in terms of cost by searching benefits. OH&S is used to establish occupational health and safety management system of the organization. It defines a set of OH & S management system requirements.

3.15 Risk Management and System Development Life Cycle(SDLC)

Minimizing [6] negative impact on an organization and need for sound basis in decision making are the fundamental reasons organizations implement a risk management process for their IT systems. Effective risk management must be totally integrated into the SDLC. Any IT organization involving SDLC has five phases: initiation, development or acquisition, implementation, operation or maintenance, and disposal. In some cases, an organization may occupy several of these phases at the same time. However, the risk management methodology is the same regardless of the SDLC phase for which the assessment is being conducted. Risk management is an iterative process that can be performed during each major phase of the SDLC.

If each phase is considered individually it also contains further steps to complete. In initiation there is need of complete requirement gathering and according to the gathered information use cases are derived. As shown in Figure 1, there is risk analysis done before and after design phase. According to that the risk based security test cases are generated. After implementation again analysis is done.

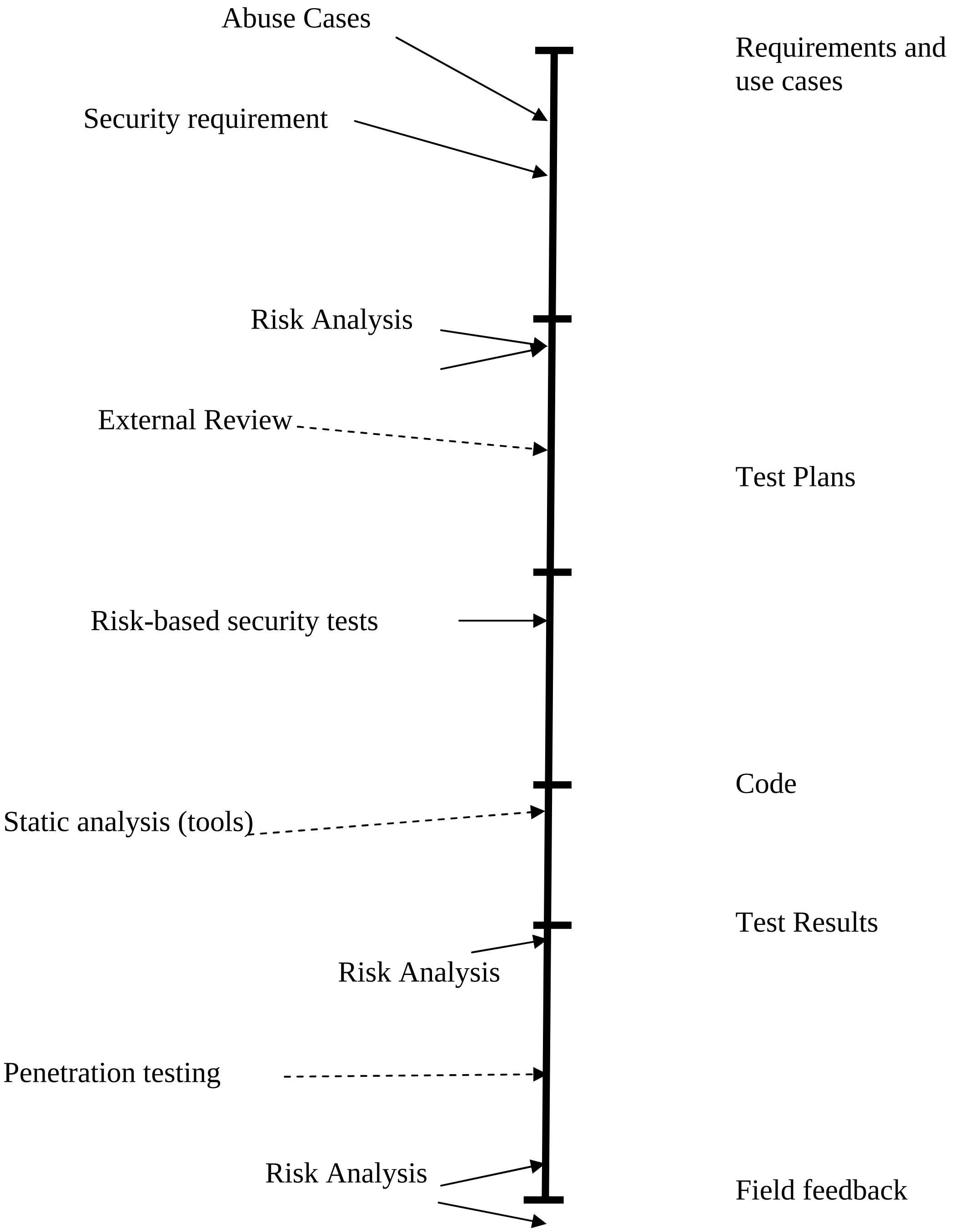


Figure 3.1. Risk Analysis in Development Cycle[10]

SDLC phases	Phase Characteristics	Support from Risk Management Activities
Phase 1- Initiation	The need for an organization is expressed and the purpose and scope of the organization is documented	Identified risks are used to support the development of the system requirements, including security requirements, and a security concept of operations (strategy)
Phase 2- Development	The IT system is designed, purchased, programmed, developed, or otherwise constructed	The risks identified during this phase can be used to support the security analyses of the IT system that may lead to architecture and design tradeoffs during system development
Phase 3- Implementation	The system security features should be configured, enabled, tested, and verified	The risk management process supports the assessment of the system implementation against its requirements and within its modeled operational environment. Decisions regarding risks identified must be made prior to system operation
Phase 4- Operations and Maintenance	The system performs its functions. Typically the system is being modified on an ongoing basis through the addition of hardware and software and by changes to organizational processes, policies, and procedures	Risk management activities are performed for periodic system reauthorization (or reaccreditation) or whenever major changes are made to an IT system in its operational, production environment (e.g., new system interfaces)
Phase 5- Disposal	This phase may involve the disposition of information, hardware, and software. Activities may include moving, archiving, discarding, or destroying information and sanitizing the hardware and software	Risk management activities are performed for system components that will be disposed of or replaced to ensure that the hardware and software are properly disposed of, that residual data is appropriately handled, and that system migration is conducted in a secure and systematic manner

Table 3.1: Risk Management and SDLC[10]

3.16 Risk Assessment

Risk assessment [22] is one method in a much broader field of risk management. Risk assessment is a process that does not result in a fixed final answer. It is impossible to determine the true magnitude and extent of any actual contamination at a site.

Once [20] risks have been identified, they must then be assessed as to their potential severity of loss and to the probability of occurrence. These quantities can be either simple to measure, in the case of the value of a lost building, or impossible to know for sure in the case of the probability of an unlikely event occurring. Therefore, in the assessment process it is critical to make the best educated guesses possible in order to properly prioritize the implementation.

The fundamental [13] difficulty in risk assessment is determining the rate of occurrence since statistical information is not available on all kinds of past incidents. Furthermore, evaluating the severity of the consequences (impact) is often quite difficult for immaterial assets. Asset valuation is another question that needs to be addressed. Thus, best educated opinions and available statistics are the primary sources of information. Nevertheless, risk assessment should produce such information for the management of the organization that the primary risks are easy to understand and that the risk management decisions may be prioritized.

Risk assessment [7] may be the most important step in the risk management process, and may also be the most difficult and prone to error. Once risks have been identified and assessed, the steps to properly deal with them are much more programmatical.

Part of the difficulty of risk management is that measurement of both of the quantities in which risk assessment is concerned can be very difficult itself. Uncertainty in the measurement is often large in both cases. Also, risk management would be simpler if a single metric could embody all of the information in the measurement. However, since two quantities are being measured, this is not possible. A risk with a large potential loss and a low probability of occurring must be treated differently than one with a low potential loss but a high likelihood of occurring. In theory both are of nearly equal priority in dealing with first, but in practice it can be very difficult to manage when faced with the scarcity of resources, especially time, in which to conduct the risk management process.

3.17 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 us an idea or scale of risk under observation. These techniques are mostly divided into three types of assessments;

3.17.1 Qualitative Assessment

Qualitative analysis [16] helps in the identification of the assets and resources at risk, vulnerabilities that might allow the threats to be realized, safeguards already in place and those which may be implemented to achieve an acceptable level of risk and increase overall awareness. This analysis uses simple calculations and uses procedure in which it is not necessary to determine the dollar value of all assets and the threat frequencies or the implementation costs of the controls.

In this method, ratings are defined in terms of characteristics and when multiplied /added / combined, 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“, in 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. But this may also result in some confusion like in a combination of “Highest” and “Lowest”, which one will be preferred, will depend highly on experience of the person performing the assessment.

Some of the qualitative methods used in risk analysis namely are preliminary risk analysis (PHA), hazard and operability study (HAZOP), and failure mode and effects analysis (FMEA/FMECA).

3.17.1.1 Preliminary Risk Analysis

Preliminary Risk Analysis Preliminary risk analysis or hazard analysis is a qualitative technique which involves a disciplined analysis of the event sequences which could transform a potential hazard into an accident. In this technique, the possible undesirable events are identified first and then analysed separately. For each undesirable events or hazards, possible improvements, or preventive measures are then formulated.

The result from this methodology provides a basis for determining which categories of hazard should be looked into more closely and which analysis methods are most suitable. Such an analysis also proved valuable in the working environment to which activities lacking safety measures can be readily identified. With the aid of a frequency/ consequence diagram, the identified hazards can then be ranked according to risk, allowing measures to be prioritized to prevent accidents.

3.17.1.2 Hazard and Operability Studies (HAZOP)

The HAZOP technique was developed in the early 1970s by Imperial Chemical Industries Ltd. HAZOP can be defined as the application of a formal systematic critical examination of the process and engineering intentions of new or existing facilities to assess the hazard potential that arise from deviation in design specifications and the consequential effects on the facilities as a whole.

This technique is usually performed using a set of guidewords: NO/NOT, MORE OR/LESS OF, AS WELL AS, PART OF REVERSE, AND OTHER THAN. From these guidewords, a scenario that may result in a hazard or an operational problem is identified. Consider the possible flow problems in a process line, the guide word MORE OF will correspond to high flow rate, while that for LESS THAN, low flow rate. The consequences of the hazard and measures to reduce the frequency with which the hazard will occur are then discussed. This technique had gained wide acceptance in the process industries as an effective tool for plant safety and operability improvements. Detailed procedures on how to perform the technique are available in literature.

3.17.1.3 Failure Mode and Effects Analysis (FMEA/FMECA)

This method was developed in the 1950s by reliability engineers to determine problems that could arise from malfunctions of military system. Failure mode and effects analysis is a procedure by which each potential failure mode in a system is analysed to determine its effect on the system and to classify it according to its severity.

When the FMEA is extended by a criticality analysis, the technique is then called failure mode and effects criticality analysis(FMECA). Failure mode and effects analysis has gained wide acceptance by the aerospace and the military industries. In fact, the technique has adapted itself in other form such as misuse mode and effects analysis.

These three techniques outlined above require only the employment of hardware familiar personnel. However, FMEA tends to be more labour intensive, as failure of each individual component in the system has to be considered. A point to note is that these qualitative techniques can be used in the design as well as operational stage of a system.

All the techniques mentioned above have seen wide usage in the nuclear power plant and chemical processing plant. In fact, FMEA, one of the most documented, has been used by Intel and National Semiconductor to improve the reliability of their product. For the case of preliminary risk analysis, it has seen application in safety analysis as well as offshore platform. HAZOP, on the other hand, has been widely used in the chemical industries for detailed failure and effect study on the piping and instrumentation layout.

3.17.2 Quantifiable Assessment

Quantitative analysis [16] identifies the specific envelope in which the losses and safeguards exist. It is based substantially on independently objective processes and metrics and requires an accordingly increased degree of effort be placed in deterring the cost values and an increasing amount of effort be placed into the calculations. It presents its results in a management-friendly form of monetary values, percentages, and probabilities.

In this method, 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 one 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 give 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”.

3.17.3 Monetary Assessment

This method requires us 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, 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.

3.17.4 Probabilistic Assessment

Probabilistic risk assessment (PRA) (or probabilistic safety assessment/analysis) is a systematic and comprehensive methodology to evaluate risks associated with a complex engineered technological entity (such as an airliner or a nuclear power plant). Risk in a PRA is defined as a feasible detrimental outcome of an activity or action. In a PRA, risk is characterized by two quantities (1) the magnitude (severity) of the possible adverse consequence(s), and (2) the likelihood (probability) of occurrence of each consequence.

Consequences are expressed numerically (e.g., the number of people potentially hurt or killed) and their likelihoods of occurrence are expressed as probabilities or frequencies (i.e., the number of occurrences or the probability of occurrence per unit time). The total risk is the expected loss which is the sum of the products of the consequences multiplied by their probabilities.

The spectrums of risks across classes of events are also of concern, and are usually controlled in licensing processes. It would be of concern if rare but high consequence events were found to dominate the overall risk, particularly as these risk assessment is very sensitive to assumptions.

Probabilistic Risk Assessment usually answers three basic questions:

- What can go wrong with the studied technological entity, or what are the initiators or initiating events (undesirable starting events) that lead to adverse consequence(s)?
- What and how severe are the potential detriments, or the adverse consequences that the technological entity may be eventually subjected to as a result of the occurrence of the initiator?
- How likely to occur are these undesirable consequences, or what are their probabilities or frequencies?

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.

3.18 Benefits of Risk Assessment

Risk assessment is necessary for reliability and productivity of an organization. Following [8] are the main advantages can be achieved by applying this approach

3.18.1 Cost Justification

Additional security almost always involves additional expense. As this does not directly generate income, it should always be justified in financial terms. The Risk Analysis process should directly and automatically generate such justification for security recommendations in business terms.

3.18.2 Productivity Audit/Review Savings

A Risk Analysis programme should enhance the productivity of the security or audit team. By creating a review structure, formalising a review, pooling security knowledge in the system's "knowledge base" and utilising "self-analysis" features, much more productive use of time is possible. The ability to 'build-in' expertise should also alleviate the need for expensive external security consultants.

3.18.3 Breaking Barriers, Business Relationships

Security should be addressed at both business management and IT staff. Business management are responsible for decisions relating to the security risk/level that the enterprise is willing to accept at a given time (which involves consideration of potential business impact). IT management are responsible for decisions relating to specific controls and application. Risk Analysis should not only direct appropriate information at each group, but play a major and pro-active role in enhancing the understanding of the needs and role of the other. It should bring the two groups closer together. Risk Analysis should relate security directly to business issues.

3.18.4 Self Analysis

The Risk Assessment system should be simple enough to enable its use without necessitating particular security knowledge, or indeed, IT expertise. This approach enables security to be driven into more areas and to become more devolved. It enables security to become part of the enterprises culture, allowing business unit management to take more of the responsibility for ensuring an adequate and appropriate level of security.

3.18.5 Security Awareness

The wide scale application of a risk assessment programme, by actively involving a range of, and greater number of, staff, will place security on the agenda for discussion and increase security awareness within the enterprise.

3.18.6 Targeting of Security

Security should be properly targeted, and directly related to potential impacts, threats, and vulnerabilities. Failure to achieve this could result in excessive or unnecessary expenditure. Risk Analysis promotes far better targeting and facilitates related decisions. This not only applies to which areas of a particular system resources should be directed to, but which business systems. Through the application of Risk Analysis across multiple business unit, it is possible to quickly establish the areas of greatest risk to the enterprise as a whole.

3.18.7 Baseline Security and Policy

Many enterprises require adherence to certain 'baseline' standards. This could be for a variety of reasons, such as legislation (e.g., Data Protection Act), enterprise policy, regulatory controls, etc. The Risk Analysis methodology should support such requirements and enable rapid identification of any failings.

3.18.8 Consistency

A major benefit of the application of Risk assessment is that it brings a consistent and objective approach to all security reviews. This not only applies across different applications, but different types of business system. It should also embrace those systems not under the direct control of IT management including paper based systems, PC Systems, or systems utilizing other office equipment.

3.18.9 Communication

By obtaining information from different parts of a business unit, a Risk Assessment aids communication and facilitates decision making.

3.19 Risk Management Failure

If risks [13] are improperly assessed and prioritized, time can be wasted in dealing with risk of losses that are not likely to occur. Spending too much time assessing and managing unlikely risks can divert resources that could be used more profitably. Unlikely events do occur but if the risk is unlikely enough to occur it may be better to simply retain the risk and deal with the result if the loss does in fact occur. Qualitative risk assessment is subjective and lacks consistency. The primary justification for a formal risk assessment process is legal and bureaucratic. Prioritizing the risk management processes too highly could keep an organization from ever completing a project or even getting started. This is especially true if other work is suspended until the risk management process is considered complete.

It is observed that risk management [12] is valuable, it is also important to understand the many ways in which risk management failures may arise. In risk management first step is to identify and measure risks. After the control measure is taken, there are following basic kinds of mistakes that can be made in measuring risk.

- Failure to use appropriate risk metrics involves if the risk is known and seems to be benign to the organization and the measure taken to overcome it is not appropriate causes the failure to any important asset of the organization.
- Mismeasurement of known risks is the case where risk managers have chosen the right metrics, but the risks have been measured incorrectly. A mistake is made in assessing the probability of large loss or the wrong distribution is used altogether.
- Mismeasurement stemming from overlooked risks involves if the concerned individuals ignore a known risk, because of a mistaken assumption that it is immaterial or because of the difficulty of incorporating it in the risk models or it is a case of risks that are truly unknown, or at least completely unanticipated.
- Failure in communicating risks to concerned management is not the job of risk management to determine the overall target level of risk or the kind of risks of the organization. Its role is to provide timely information to the board and top management that allows them to assess the consequences of retaining or laying off risks. So if the risk is occurred it is necessary to communicate the management in time and to the appropriate management.
- Failure in monitoring and managing risks in case where risk should be monitored constantly or otherwise manage known risks to meet the objectives of concerned management. It may be particularly challenging for financial firms, where risks change abruptly even if the organization does not take new positions

CHAPTER 4: COMPARITIVE ANALYSIS AND PROPOSED MODEL

Risk analysis, analytical identification and assessment methodology for different risk factors, can plays a vital role for the protection of strategic data center environments.

Risk management provides structured methodology for assessing the risks; develop the strategies for managing and impart controls by using the resources to mitigate the risks. The strategies comprise of taking measures to reduce the probability of occurrence of the risk and remedial steps to overcome the effect caused due to that occurrence of risk. It is a process of identifying activities, assets or external/internal sources that can negatively affect an organization's operations.

4.1 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.

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 4.1 : Similarities of Strategic and Commercial 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.

S.No	Strategic Organization	Commercial Organization
1	Not-for-profit	Works for Profit (can't survive without it)
2	No Competition and not part of market as the services are unique and cannot be commercialized	Have to complete with competitors, therefore biggest threats are competitors and their activities that can effect their profits
3	Risks and their impacts can effect national causes (country's defense structure) and eventually can effect commercial setup as well (it may also effect their assets / resources or services in a negative manner)	Risks and their impacts will affect organization's assets/resources and/or services only, and shall not effect strategic organizations. In some cases, it may have severe effect on its suppliers or customers (but strategic organizations usually have extensive backups as their existence is a Government's prime responsibilities)
4	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
5	In addition to Legal requirements, Defense based regulations are also applicable. Not following them can have severe negative effects strategic decisions	In addition to Legal requirements, customer (especially foreign customers) requirements are also followed (especially in case of software houses and call centers). Not following them can have negative effects commercial position and business relations
6	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
7	Third party involvement is very less in most of the operations and projects	Links to the third party are important for better competition and profit earning

Table 4.2 : Differences of Strategic and Commercial Organization

The coming portions of this chapter will breakdown Risk Assessment and Risk Treatment process in light of both Strategic and Commercial Organizations, considering their similarities and differences.

4.2 Proposed Risk Assessment and Treatment model

It is observed that the basic steps for risk management are same but can be used in different scenarios according the environment and structure of the organization. The goal of proposed model is to provide organization such a qualitative approach to implement risk management process.

The proposed risk assessment model consists of following steps

1. Identification of Assets
2. Asset Value
3. Identification of threats
4. Identification of vulnerabilities
5. Identifying Risk
6. Risk Assessment
    a. Chances of Risk Occurrence
    b. Chances of Risk Detection
    c. Severity of Impact
7. Risk Treatment
8. Control deployed

4.2.1 Identification of Assets

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

4.2.2 Asset Evaluated Value

The assets [5] of the systems are categorized according to their importance in the organization into Critical, High, moderate, Internal and common. The assets are evaluated on the basis of Confidentiality(C), Integrity(I) and availability(A). These three factors are very important taking into account the evaluation of the assets on the basis of security and reliability of the system. The asset value is calculated by adding the three security factors as follows

Asset value = C+I+A

- **Confidentiality:** The security [6] goal that generates the requirement for protection from intentional or accidental attempts to perform unauthorized data reads. Confidentiality covers data in storage, during processing, and in transit. It is the ability to operate privately

- **Integrity:** The security goal [6] that generates the requirement for protection against either intentional or accidental attempts to violate data integrity (the property that data has when it has not been altered in an unauthorized manner) or system integrity (the quality that a system has when it performs its intended function in an unimpaired manner, free from unauthorized manipulation).The ability of detecting change/modification in the information.

- **Availability:** The security goal [6] that generates the requirement for protection against Intentional or accidental attempts to (1) perform unauthorized deletion of data or (2) otherwise cause a denial of service or data and Unauthorized use of system resources, making the information accessible so that it could be used on demand by authorized entity.

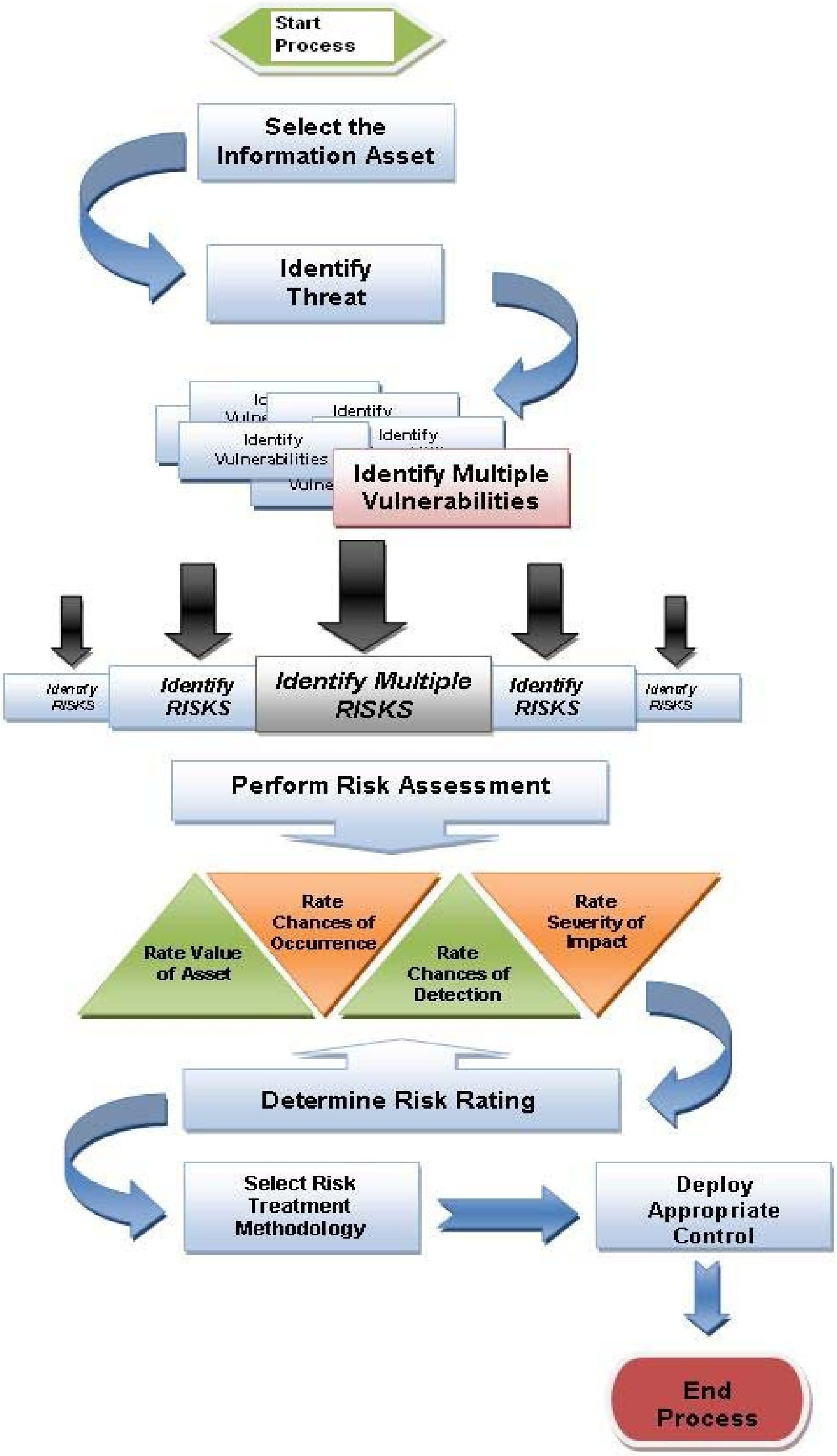


Figure 4.1: Proposed Risk Assessment and Treatment Model

Value in Terms of Priorities	**Description**	**Value in Numeric**
Critical	Assets that affect 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 4.3: Value of Information Asset

4.2.3 Identification of Threat

Threats [5][6] are events that could cause harm to the confidentiality, integrity, or availability of information or information systems. They can be characterized as the potential for agents exploiting vulnerability to cause harm through the unauthorized disclosure, misuse, alteration, or destruction of information or information systems. Threats can arise from a wide variety of sources. Traditionally, the agents have been categorized as internal (malicious or incompetent employees, contractors, service providers, and former insiders) and external (criminals, recreational hackers, competitors, and terrorists). Each of the agents identified may have different capabilities and motivations, which may require the use of different risk mitigation and control techniques and the focus on different information elements or systems.

Generally the threats can be divided into following categories

No	Threat Types	Examples
1	Human	Individual illness, death, robbery, bomb threats, war etc
2	Operational	Loss of access to essential assets, failures in distribution etc
3	Reputational	Loss of business partner or employee confidence, or damage to reputation in the market
4	Procedural	Failures of accountability, internal systems and controls, organization, fraud etc
5	Project	Risks of cost over-runs, jobs taking too long, of insufficient product or service quality, etc
6	Financial	Business failure, stock market, interest rates, unemployment etc
7	Technical	Power failure, heating, ventilation, failure of CPU, failure of system and application software, communication failure etc
8	Natural	Threats from weather, natural disaster, accident, disease etc
9	Political	Changes in tax regimes, public opinion, government policy, foreign influence etc

Table 4.4: Threat Types

4.2.4 Identification of Vulnerabilities

Vulnerabilities [3][5] can be characterized as weaknesses in a system, or control gaps that, if exploited, could result in the unauthorized disclosure, misuse, alteration, or destruction of information or information systems. Vulnerabilities are generally grouped into two types: known and expected. Known vulnerabilities are discovered by testing or other reviews of the environment, knowledge of policy weaknesses, knowledge of inadequate implementations, and knowledge of personnel issues. Adequate and timely testing is essential to identify many of these vulnerabilities. Inadequate or untimely testing may critically weaken the risk assessment.

Expected vulnerabilities [5] to consider are those that can reasonably be anticipated to arise in the future. Examples may include unpatched 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. Although some vulnerabilities may exist only for a short time until they are corrected, the risk assessment should consider the risk posed for the time period the vulnerability might exist. Vulnerability is a defect or weakness in system security procedure, design, implementation, or internal control that an attacker can compromise. It can exist in one or more of the components making up a system, even if those components aren’t necessarily involved with security functionality. A given system’s vulnerability data are usually compiled from a combination of Operating system and application-level vulnerability test results, code reviews, and higher-level architectural reviews. Software vulnerabilities come in two basic flavors: flaws (design-level problems) or bugs (implementation-level problems). Automated scanners tend to focus on bugs, since human expertise is required for uncovering flaws.

4.2.5 Identification of Risk

Risk identification [5] ascertains what risks or hazards exist or anticipated their characteristics, magnitude, duration, probability of occurrence and recurrence and possible outcomes and consequences. Precise and absolute risk identification is fundamental for effective risk management. In order to manage risks efficiently, they must first be identified. During the 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. Identification involves[7] different types of risks including Software Risks; knowledge of the most common risks associated with Software development, and the platform you are working on and Business Risks which involve the most common risks associated with the business using the Software. Other than these the Testing Risks which have knowledge of the most common risks associated with Software Testing for the platform you are working on, tools being used, and test methods being applied and premature release risk which have ability to determine the risk associated with releasing unsatisfactory or untested Software Products. The Risk Methods includes Strategies and approaches for identifying risks or problems associated with implementing and operating information technology, products and process; assessing their likelihood, and initiating strategies to test those risks

4.2.6 Performing Risk Assessment

Risk assessment is process of analyzing identified risks causing delays in the design, production, or delivery of the system, adversely affect the system's performance, or increase 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 the probability of risk being arise. The maximum probability of the risk can be occurred 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 according to the environment and how frequently a risk can be occurred.

Value in Terms of Priorities	**Description**	**Value in Numeric**
Very High	Once in a week	5
High	Once in a month	4
Medium	Once in Six Months	3
Low	Twice in a Year	2
Very Low	Once in a year or less	1

Table 4.5: 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 1and the risk having lowest chances to be detected has a value 5. The probability of detection varies from 1 to 5, from the highest value to the lowest respectively.

Value in Terms of Priorities	**Description**	**Value in Numeric**
Very High	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
Very Low	Not possible to detect unless it is occurring	1

Table 4.6: Chances of Risk Detection

The most important is that how strict the impact of a risk can be than the probability to occur and detecting its value. This shows the outcome of the threat[1]. 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 multiple of 2 and vary between the highest “10” and the lowest “2” value.

Value in Terms of Priorities	**Description**	**Value in Numeric**
Critical	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
Internal	Effects on Internal or Moderate Priority Assets	4
Common	Effects on Common Priority Assets	2

Table 4.7: Severity Impact

The following formula is used to perform Risk Assessment:

Risk Rating = [V + O + D] x S (2)

V: Value of Information Asset

O: Chances of Risk occurrence

D: Chances of Risk Detection

S: Severity of Impact

Applying the formula 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. According to the estimated value the control measure is done to reduce the probability of occurrence of risk and its impact to the systems.

Greater the severity of impact greater would be the loss of important factors including confidentiality, integrity and availability[6]

- **Loss of Integrity:** System and data integrity refers to the requirement that information be protected from improper modification. Integrity is lost if unauthorized changes are made to the data or system by either intentional or accidental acts. If the loss of system or data integrity is not corrected, continued use of the contaminated system or corrupted data could result in inaccuracy, fraud, or erroneous decisions. Also, violation of integrity may be the first step in a successful attack against system availability or confidentiality. For all these reasons, loss of integrity reduces the assurance of an organization.

- **Loss of Availability:** If a mission-critical system is unavailable to its end users, the organization’s mission may be affected. Loss of system functionality and operational effectiveness, for example, may result in loss of productive time, thus impeding the end users’ performance of their functions in supporting the organization’s mission.

- **Loss of Confidentiality:** System and data confidentiality refers to the protection of information from unauthorized disclosure. The impact of unauthorized disclosure of confidential information can range from the jeopardizing of national security to the disclosure of Privacy Act data. Unauthorized, unanticipated, or unintentional disclosure could result in loss of public confidence, embarrassment, or legal action against the organization.

4.2.7 Risk Treatment

Risk treatment [2][5] is the process that identifies, evaluates, selects, and implements options in order to avoid or set risk at acceptable levels given constraints and objectives.

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. After identification of risks different [13] methods can be used to mitigate which are as follows:

- **Risk Avoidance:** includes not performing an activity that could carry risk. Avoidance may seem the answer to all risks, but avoiding risks also means losing out on the potential gain that accepting (retaining) the risk may have allowed. Not entering a business to avoid the risk of loss also avoids the possibility of earning profits.

- **Risk Reduction:** involves methods that reduce the severity of the loss or the risk of the loss from occurring. Modern software development methodologies reduce risk by developing and delivering software incrementally. Early methodologies suffered from the fact that they only delivered software in the final phase of development; any problems encountered in earlier phases meant costly rework and often jeopardized the whole project. By developing in iterations, software projects can limit effort wasted to a single iteration. Outsourcing could be an example of risk reduction if the outsourcer can demonstrate higher capability at managing or reducing risks. In this case companies outsource only some of their departmental needs. For example, a company may outsource only its software development, the manufacturing of hard goods, or customer support needs to another company, while handling the business management itself. This way, the company can concentrate more on business development without having to worry as much about the manufacturing process, managing the development team, or finding a physical location for a call center.

- **Risk Retention:** involves accepting the loss when it occurs. True self insurance falls in this category. Risk retention is a viable strategy for small risks where the cost of insuring against the risk would be greater over time than the total losses sustained. All risks that are not avoided or transferred are retained by default. This includes risks that are so large or catastrophic that they either cannot be insured against or the premiums would be infeasible. War is an example since most property and risks are not insured against war, so the loss attributed by war is retained by the insured. Also any amounts of potential loss (risk) over the amount insured is retained risk. This may also be acceptable if the chance of a very large loss is small or if the cost to insure for greater coverage amounts is so great it would hinder the goals of the organization too much.

- **Risk Transfer:** means causing another party to accept the risk, typically by contract or by hedging. Insurance is one type of risk transfer that uses contracts. Other times it may involve contract language that transfers a risk to another party without the payment of an insurance premium. Liability among construction or other contractors is very often transferred this way. On the other hand, taking offsetting positions in derivatives is typically how firms use hedging to financially manage risk.

Some ways of managing risk fall into multiple categories. Risk retention pools are technically retaining the risk for the group, but spreading it over the whole group involves transfer among individual members of the group. This is different from traditional insurance, in that no premium is exchanged between members of the group up front, but instead losses are assessed to all members of the group.

4.2.8 Control Measure Adopted for Treatment

Controls [16] are those things which are implemented to prevent the exposure to the threat in the first place, detect if the threat has been realized against the system, and mitigate the impact of the threat against the system or to recover/restore the system. These [20] are safeguards that reduce the probability that a threat will exploit a vulnerability to successfully attack an asset. Identify those safeguards that are currently implemented, and determine their effectiveness in the context of the current analysis.

The institution should identify controls that will mitigate the impact or likelihood of each identified threat agent exploiting a specific vulnerability. Controls [5] are generally categorized by timing (preventive, detective, or corrective) or nature (administrative, technical, or physical). The evaluation should recognize the unique control environment of the institution, and evaluate the effectiveness of that environment in responding to the threats arrayed against it. The evaluation should address the controls that prevent harm as well as those that detect harm and correct damage that occurs. Preventive controls act to limit the likelihood of a threat agent succeeding. Detective and corrective controls are essential to identify harmful actions as they occur, to facilitate their termination, and to reduce damage.

Security controls [6] encompass the use of technical and nontechnical methods. Technical controls are safeguards that are incorporated into computer hardware, software, or firmware (e.g., access control mechanisms, identification and authentication mechanisms, encryption methods, intrusion detection software). Nontechnical controls are management and operational controls, such as security policies; operational procedures; and personnel, physical, and environmental security. The control categories for both technical and nontechnical control methods can be further classified as either preventive or detective.

These two subcategories are explained as follows:

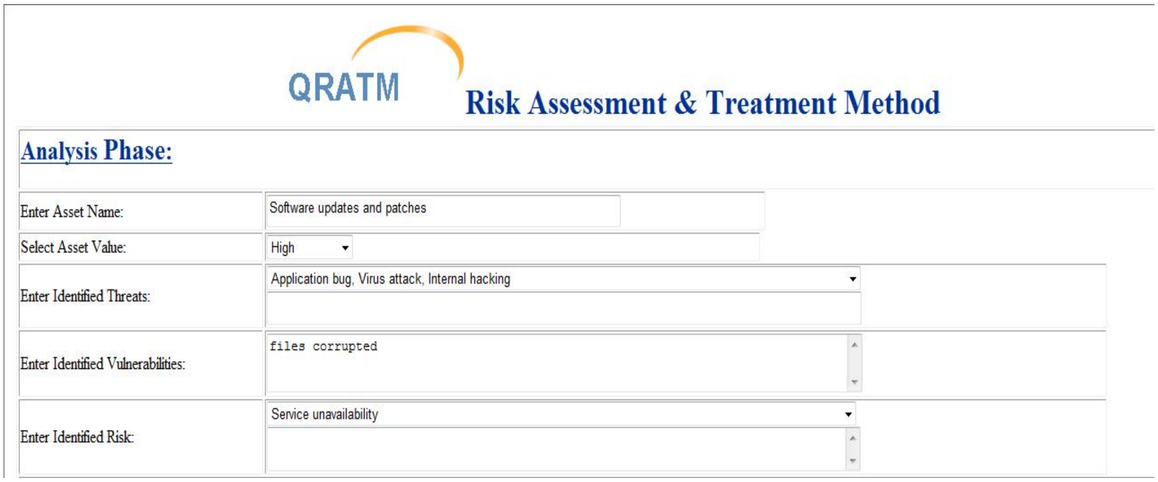
- Preventive controls inhibit attempts to violate security policy and include such controls as access control enforcement, encryption, and authentication.
- Detective controls warn of violations or attempted violations of security policy and include such controls as audit trails, intrusion detection methods, and checksums.

CHAPTER 5: APPLICATION AND RESULTS

5.1 Application of Tool QRATM

A tool is developed to calculate the risk rating and showing the results in form of graphs. There are three phases which involves the analysis of assets identification & assessment and risk treatment; made to calculate the risk rating. The screen shots of the tools are taken which are as follows:

Phase 1: Analysis Phase



QRATM Risk Assessment & Treatment Method

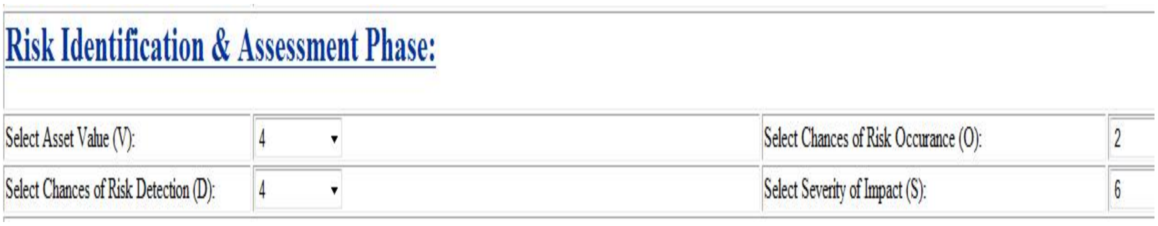
Analysis Phase:

Enter Asset Name:	Software updates and patches
Select Asset Value:	High
Enter Identified Threats:	Application bug, Virus attack, Internal hacking
Enter Identified Vulnerabilities:	files corrupted
Enter Identified Risk:	Service unavailability

Figure 5.1 QRATM Analysis Phase

In this phase the important asset, its value, the related threat, vulnerabilities and risks are identified.

Phase 2: Risk Identification and Assessment Phase



Risk Identification & Assessment Phase:

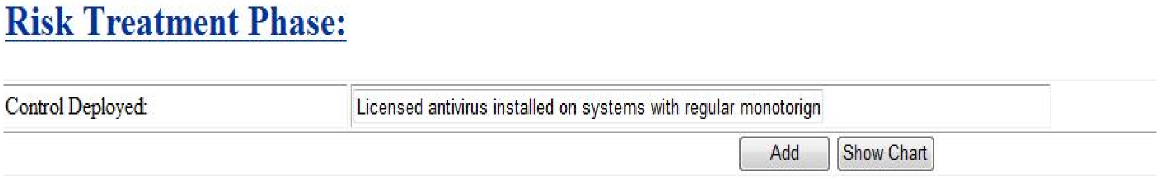
Select Asset Value (V):	4	Select Chances of Risk Occurance (O):	2
Select Chances of Risk Detection (D):	4	Select Severity of Impact (S):	6

Figure 5.2 QRATM Risk Identification and Assessment Phase

In this phase the values assigned on the basis of probability to occur any risk, its chances of detection and the impact of that specified risk.

Phase 3: Risk Treatment

In treatment phase the countermeasure to that risk are made and also identify the method to ovoid that risk.

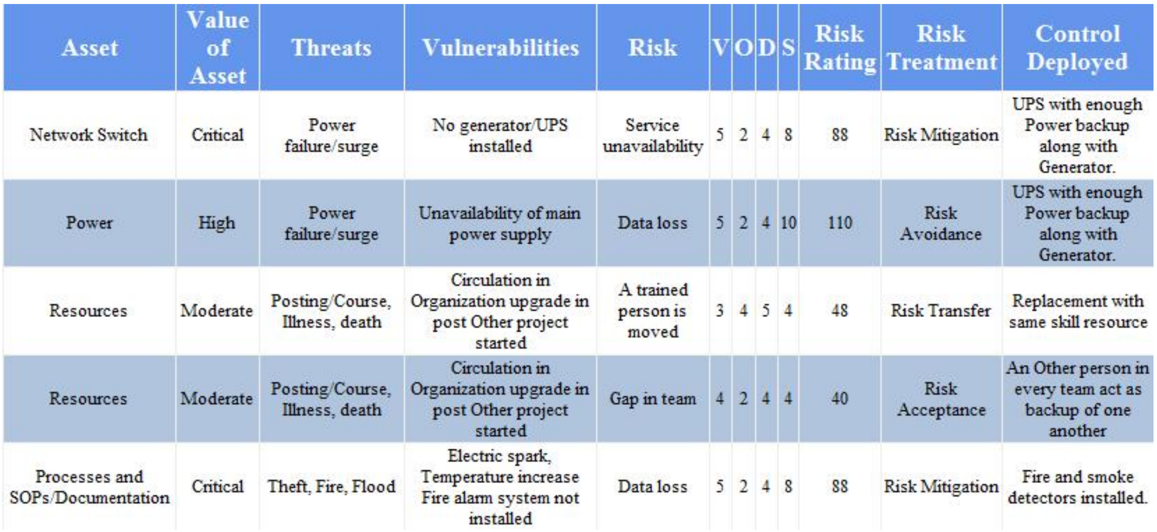


Risk Treatment Phase:

Control Deployed:	Licensed antivirus installed on systems with regular monotorign

Figure 5.3 QRATM Treatment Phase

5.2 Results



Asset	Value of Asset	Threats	Vulnerabilities	Risk	V	O	D	S	Risk Rating	Risk Treatment	Control Deployed
Network Switch	Critical	Power failure/surge	No generator/UPS installed	Service unavailability	5	2	4	8	88	Risk Mitigation	UPS with enough Power backup along with Generator.
Power	High	Power failure/surge	Unavailability of main power supply	Data loss	5	2	4	10	110	Risk Avoidance	UPS with enough Power backup along with Generator.
Resources	Moderate	Posting/Course, Illness, death	Circulation in Organization upgrade in post Other project started	A trained person is moved	3	4	5	4	48	Risk Transfer	Replacement with same skill resource
Resources	Moderate	Posting/Course, Illness, death	Circulation in Organization upgrade in post Other project started	Gap in team	4	2	4	4	40	Risk Acceptance	An Other person in every team act as backup of one another
Processes and SOPs/Documentation	Critical	Theft, Fire, Flood	Electric spark, Temperature increase Fire alarm system not installed	Data loss	5	2	4	8	88	Risk Mitigation	Fire and smoke detectors installed.

Figure 5.4 QRATM Result Sheet

Above table is generated as a result which maintains all the phases of QRATM. So a complete preview of all types of assets and its related risks with countermeasures are identified.

The results are shown in form of Bar graph. Risks are divided into four categories to show its priority. The most critical value is shown by red color whose value is greater than 100, the high priority are risks shown in green color which ranges between 76 to 100. The moderate priority risks are shown with blue color and ranges from 46 to 75 and the acceptable or low priority are shown with white color whose value ranges from 6 to 45 as shown in the graph.

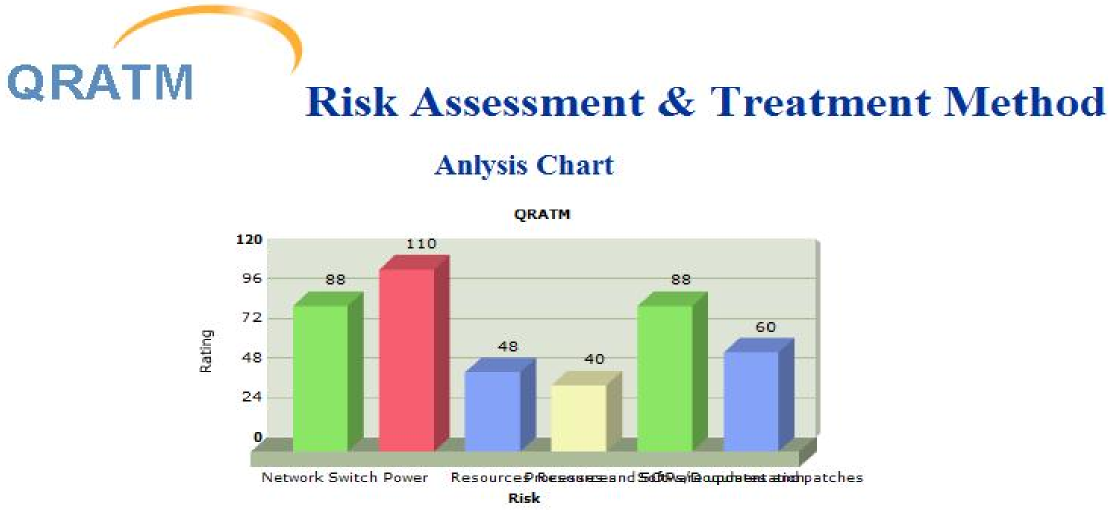


Figure 5.5 QRATM Analysis Chart

5.3 Comparison with CRAMM

The following table contains the basic steps of Risk Assessment and Treatment are compared in both models i.e., CRAMM and QRATM

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	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 5.1 QRATM vs CRAMM

A layer of risk identification and Assessment is added in the CRAMM to categorize risk. This is shown in following figure

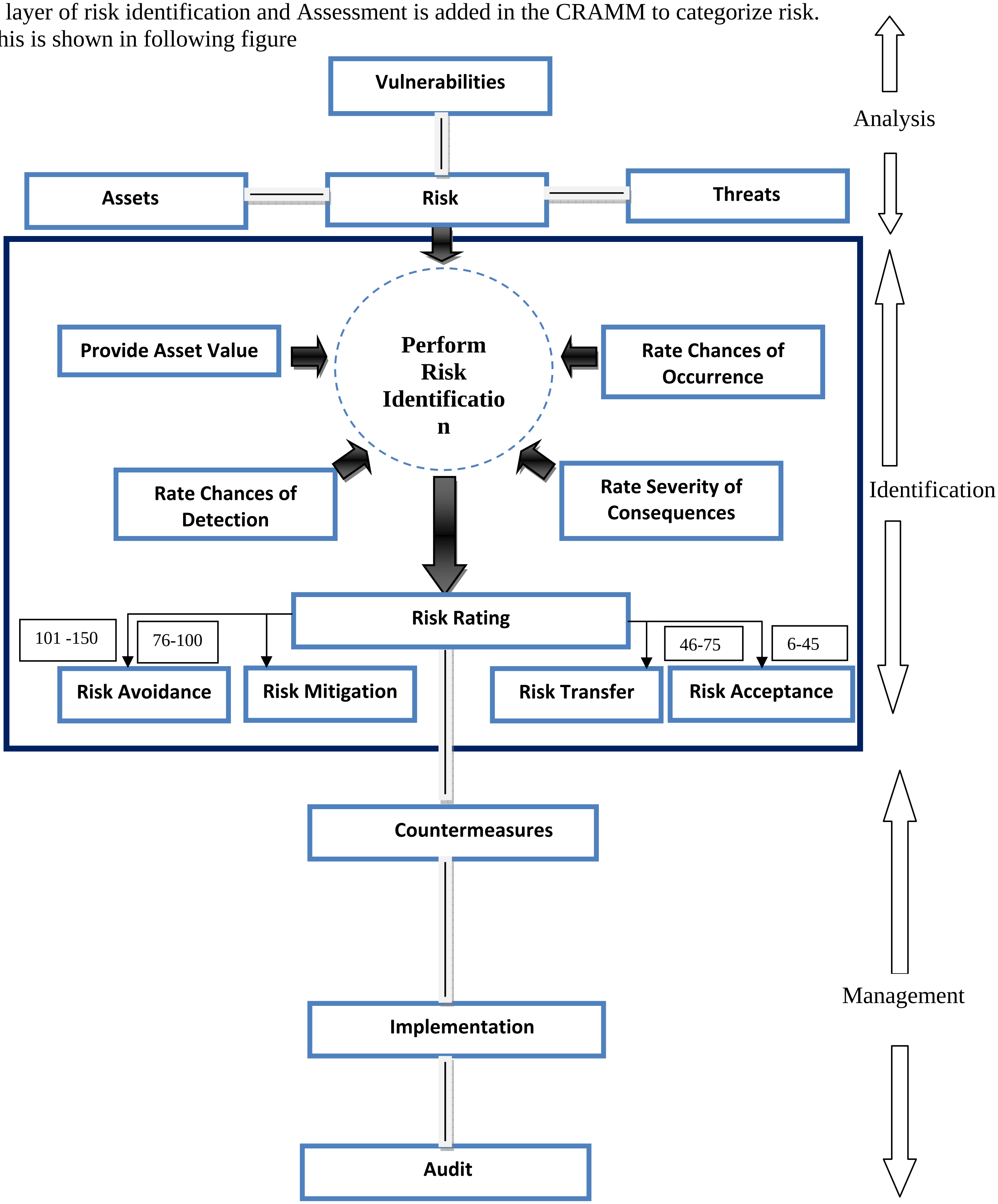


Figure 5.6 Integration with CRAMM

5.4 Comparison with “Qualitative Risk Analysis Method” by Hrvoje Segudovic

He describes the risk assessment matrix for which consists of Asset value, vulnerability and threat value. The risk rating is calculated by following formula

$$R = AV + V + T$$

where

AV = Asset Value
V = Vulnerability
T = Threat
R= Risk

The values of resource value, vulnerability and threat are divided as shown in the table.

Value	**AV**	**V**	**T**
0	Very low	Low	Low
1	Low	Medium	Medium
2	Medium	High	High
3	High		
4	Very high		

Table 5.2 Risk Rating factors values[24]

The matrix of these three factors is defined to calculate the value of risk

	Threat	**0**			**1**			**2**		
	Vulnerability	**0**	**1**	**2**	**0**	**1**	**2**	**0**	**1**	**2**
Resource Value	**0**	**0**	**1**	**2**	**1**	**2**	**3**	**2**	**3**	**4**
	1	**1**	**2**	**3**	**2**	**3**	**4**	**3**	**4**	**5**
	2	**2**	**3**	**4**	**3**	**4**	**5**	**4**	**5**	**6**
	3	**3**	**4**	**5**	**4**	**5**	**6**	**5**	**6**	**7**
	4	**4**	**5**	**6**	**5**	**6**	**7**	**6**	**7**	**8**

Table 5.3 Risk Value Matrix[24]

All the factors are added to calculate the risk rating value. This method gives the average value result of the risk and no prioritization of risk is defined.

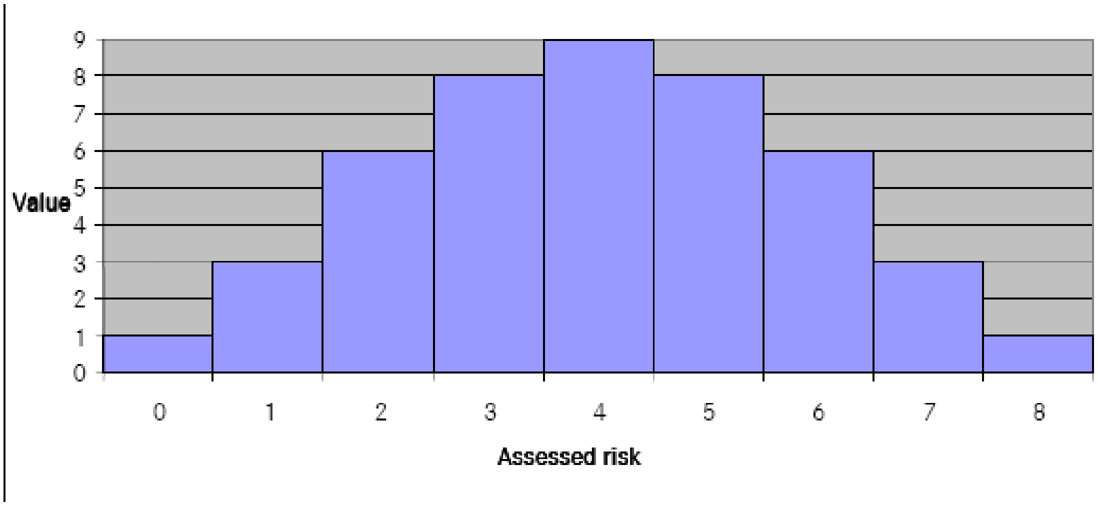


Figure 5.7 Average Value Graph[24]

Whereas using QRATM, the risks are prioritized on the basis of its value. The method is defined to overcome with the risk according to its value. QRATM is applied in both Commercial and Strategic organization and results are found on the basis of their objective. The results consist of risk and its rating in both organizations.

Risk Assessment and Treatment in Strategic Organization (Defense Organization)

The following graph shows the risk rating in Strategic organization, where red color show the 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 the specific risk to the asset.

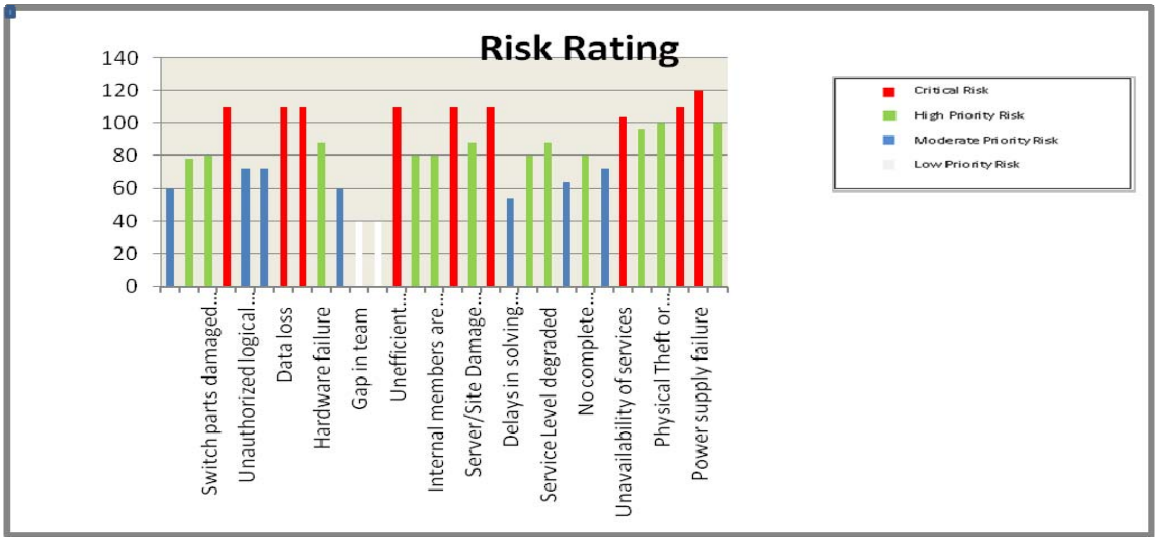


Figure 5.8 Defense Organization Risk Rating

Risk Assessment and Treatment in Commercial Organization (Wateen Organization)

The following graph shows the risk rating in Strategic organization, where red color show the risk is Critical, green is high priority, blue moderate and white are low or acceptable risks.

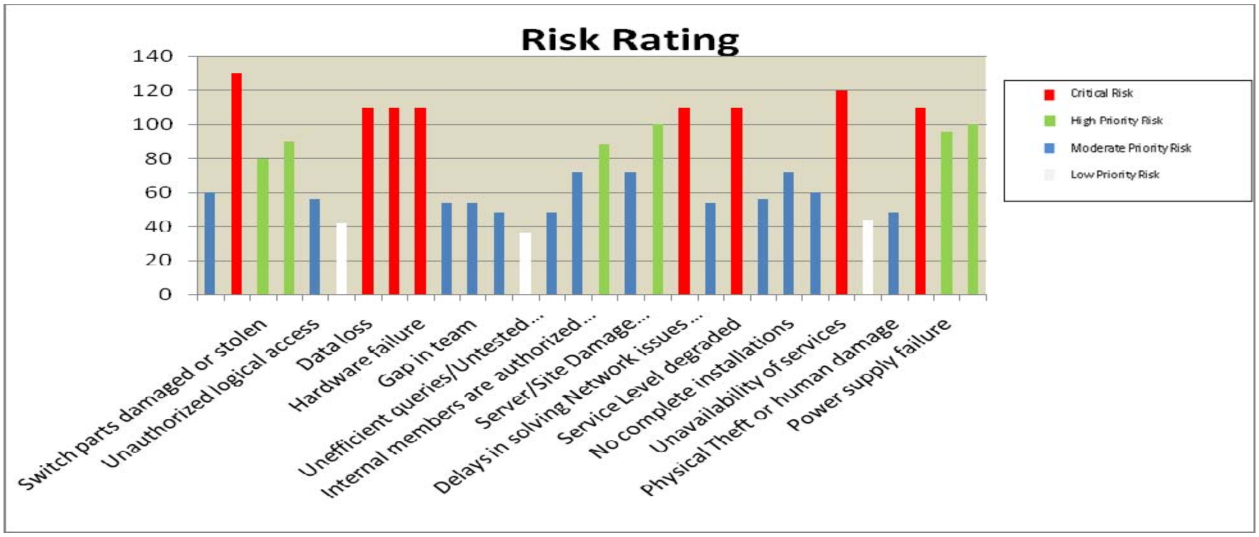


Figure 5.9 Commercial Organization Risk Rating

CHAPTER 6: CONCLUSION AND FUTURE WORK

6.1 Conclusion

Risk assessment is the most important step in the risk management process, and may also be the most difficult and prone to error. Once risks have been identified and assessed, the steps to properly deal with them are much more programmatical. It is more favorable to take countermeasures before getting into a problem.

Risk assessment and treatment is fundamental to the security of any organization and essential in ensuring that controls and expenditure are fully commensurate with the risks to which the organization is exposed.

There are many conventional methods for performing risk analysis are becoming more and more untenable in terms of usability, flexibility, and critically. The most important is to know the objectives of organization. The risk is categorized according to its importance in the specific organization and the countermeasures are applied taking into account the objectives of organization.

A new Qualitative model is proposed and its applicability is checked in both Commercial and Strategic organization. Considering the same risks in both it is observed that the impact is different in both organizations on the basis of their basic objectives.

Following research contributions have been made by this work

- Comparative analysis on the basis of Risk Assessment and Treatment is being done among Commercial and Strategic organizations
- Qualitative Risk Assessment and Treatment model is proposed
- The model is compared with globally used model CRAMM
- The results are compared with related work of Hrvoje Segudovic
- A tool is established for calculating Risk Rating
- Results shows the categorization and prioritization of Risk

6.2 Future Work

After Risk Assessment and Treatment the next step is Business Continuity Plan and Disaster Recovery. Business continuity planning means to counteract interruptions to business activities and to protect critical organization processes from the effects of major failures of information systems or disasters and to ensure their timely resumption. Disaster Recovery is done for the total site loss case includes natural disasters. Fulfilling all these steps leads to the audit of organization for certification like ISO 27001and CMMI. Both the Strategic and Commercial organizations are currently working for certification of ISO 27001.

References

[1] Proceedings of the Sixth International “ENTERPRISE DISTRIBUTED OBJECT COMPUTING” Conference (EDOC’02), IEEE 2002 “Model-based Risk Assessment to Improve Enterprise Security”, Jan Øyvind Aagedal, Folker den Braber, Theo Dimitrakos, Bjørn Axel Gran, Dimitris Raptis, Ketil Stølen

[2] An Introduction to Information System Risk Management, SANS Institute InfoSec Reading Room

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

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

[5] http://www.ffiec.gov/ffiecinfobase/booklets/information_security/03_info_sec_strategy.htm Booklet: Information Security. Section: Information Security Risk assessment

[6] NIST Technology Administration, U.S. Department of commerce. Risk Management guide for Information technology system, Gary Stoneburner, Alice Goguen, and Alexis Feringa

[7] Software Testing : Risk Analysis eBook from www.OneStopTesting.com

[8] http://www.eon-commerce.com/riskanalysis/benefits.htm

[9] 2008 IEEE Model Identification of Risk Management System by Liu Ren-hui and Zhai Feng-yong

[10] 2004 IEEE , IEEE SECURITY & PRIVACY, Risk Analysis in Software Design by DENIS VERDON Fidelity nal Financial & GARY MCGRAW Cigital

[11] Final Draft, International Standard, ISO/IEC FDIS 17799:2005

[12] Risk management failures, what are they and when do they happen? By Rene M. Stulz

[13] http://en.wikipedia.org/wiki/Risk_management

[14] A new quantitative approach for information security risk assessment Abbas Asosheh, Bijan Dehmoubed, Amir Khani ISI 2009, June 8-11, 2009, Richardson, TX, USA

[15] Fundamentals of Risk analysis and risk management, Edited by Vlasta Molak, President GAIA UNLIMITED, Inc. Cincinnati, Ohio 1997

[16] A method for quantitative risk analysis, *By James W. Meritt, CISSP*

[17] http://www.itworks.lu/risk-analysis-ebios.php

[18] http://en.wikipedia.org/wiki/BEATO

[19] http://www.cramm.org/howitworks.php

[20] http://www.bhpbilliton.com/bbContentRepository/docs/impactAssessmentMethodology.pdf

[21] http://contamsites.landcareresearch.co.nz/whatisriskman.htm

[22] http://contamsites.landcareresearch.co.nz/limitations_of_risk_assessment.htm

[23] TR-IST-049-03.pdf Chapter 3: Review of Existing Methodologies

[24] Qualitative Risk Analysis Method Comparison by Hrvoje Segudovic INFIGO-MD-2006-01