Rajendra Ganpatrao Sabale, Dr. A.R Dani / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com
Vol. 2, Issue 4, June-July 2012, pp.712-716

Risk Management Using Spiral Model for Information Technology

Rajendra Ganpatrao Sabale, Dr. A.R Dani
Student of Ph.D., Singhania University, Pacheri Bari, Dist. Jhunjhunu(Rajasthan), India
International Institute of Informational Techonology,Pune(Maharashtra),India

Abstract:
Now a day almost everything has been digitized and networked either through Local Area Network or Internet. In this digital era, as organizations use automated information technology (IT) systems to process information for improved support to achieve their objectives, risk management plays a critical role in protecting an organization's information assets, and therefore its aim, from IT-related risk.
This paper provides information about IT risk management and good practices to follow to minimize risk. It provides a foundation for the development of an effective risk management policy.

Keywords : automated information, digitized, risk management

Introduction:

1. An effective risk management process is an important component of a successful IT security program. .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. The principal goal of an organization's risk management process should be to protect the organization and its ability to perform their objectives. Risk is the net negative impact of the exercise of vulnerability, considering both the
probability and the impact of occurrence.

2. Purpose

Risk management is the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level. This paper provides groundwork for the development of a successful risk management program,

3. Objective

The objective of performing risk management is to enable the organization to accomplish its task
 By better securing the IT systems that store, process, or transmit organizational information;
 By enabling management to exercise well-informed risk management decisions to
justify the expenditures that are By assisting management in authorizing (or accrediting) the IT systems on the basis of the supporting documentation resulting from the performance of risk management.

4. Target Addressees

This paper provides a common foundation for experienced and inexperienced, technical, and non-technical personnel who support or use the risk management process for their IT
systems. These personnel include: part of an IT budget;
 The Designated Approving Authority whether to allow operation of an IT system
 The IT security program manager, who implements the security program
 Information system security officers (ISSO), who are responsible for IT security
 Business or functional managers, who are responsible for the IT procurement process
 Technical support personnel (e.g., network, system, application, and database administrators; computer specialists; data security analysts), who manage and administer security for the IT systems
 IT system and application programmers who develop and maintain code that could
affect system and data integrity
 Information system auditors, who audit IT systems (DAA), who is respond
 IT consultants, who support clients in risk management.

5. IMPORTANCE OF RISK MANAGEMENT

Risk management encompasses three processes: risk assessment, risk evaluation and. risk mitigation Risk management is the process that allows IT managers to balance the operational and economic costs of protective measures. This process is not unique to the IT environment; indeed it pervades decision-making in all areas of daily routine work. Minimizing 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. sible for the final Effective risk management must be totally integrated into the System Development Life Cycle. Risk management can be performed in support of each system development life cycle phase.

Phase 1—Initiation

• Identified risks are used to support the development of the system requirements, including security requirements, and a security concept.

Phase 2—Development or Acquisition • 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 of operations (strategy) decision

Phase 3— 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—Operation or Maintenance

• Risk management activities are performed for periodic system reauthorization (or reaccreditations) or whenever major changes are made to an IT system in its operational, production environment (e.g., new system interfaces)

Phase 5—Disposal

• 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

6. Risk Management Process

Risk management process involves:

 Identify Organizational Risks: By surveys, interviews, and solicitation of input across divisions and departments of Probability - The likelihood of risk getting realized

o Inherent Risk - The nature of the risk event

o Mitigation Control Effectiveness - The effectiveness of mitigation plans

6.1 How to identify Risks?

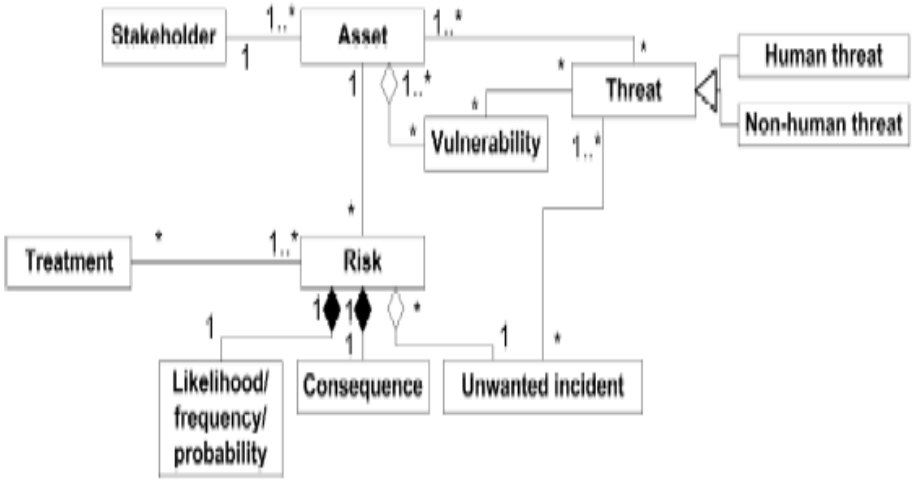
Risk Management application provides tools to quickly put together surveys and polls for gathering inputs from professionals and employees. This data is then collated into a list of identified risks for the organization. The list can be reviewed periodically and updated based on existing business scenarios.

A frequently used technique in security analysis, and in particular in risk identification, is so-called structured brainstorming (HazOp-analysis [18] is a kind of structured brainstorming). It may be understood as a structured ―walk-through‖ of the target of analysis.

The main idea of structured brainstorming is that a group of people with different competencies and backgrounds will view the target from different perspectives and therefore identify more, and possibly other, risks than individuals or a more heterogeneous group. The input to a brainstorming session is various kinds of target models (e.g. UML models). The models are assessed in a stepwise and structured manner under the guidance of the security analysis leader. The identified risks are documented by an analysis secretary.

Construction of a conceptual model based on standardized security risk analysis terminology is first step of developing language model. the most intuitive and common interpretations are used. The conceptual model can be seen as a kind of abstract syntax for the language, and is shown in diagram.

The conceptual model using UML class diagram notation



IT system throughout its SDLC. The conceptual model may be explained as follows: stakeholders are those people and organizations who may affect, be affected by, or perceive themselves to be affected by, a decision or activity regarding the target of analysis An asset is something to which a stakeholder directly assigns value, and hence for which the stakeholder requires protection Assets are subject to vulnerabilities, which are weaknesses which can be exploited by one or more threats A threat is a potential cause of an unwanted incident

6.2 Risk Assessment

Risk assessment is the first process in the risk management methodology. Organizations use risk assessment to determine the extent of the potential threat and the risk associated with an Risk is a function of the likelihood of a given threat-source's exercising a particular vulnerability, and the resulting impact of that adverse event on the organization. Consequence is the level of impact that the potential risk event can have on the achievement of business objectives. Consequence will be measured on a 5 level rating Probability is the likelihood of occurrence of the potential risk event which may lead to the assessed consequences. Probability will be measured on a 5 level rating scale in the risk survey (25-Almost Certain, 20-likely, 15-Possible, 10-Unlikely, 5-Rare)

6.2.1 Calculating Inherent Risk

Inherent risk signifies the exposure arising from a specific risk event before any action has been taken to manage it. Inherent Risk = Consequence X Probability Inherent risk rating will be exhibited on a 4 level rating scale (Extreme Risk, High Risk, Moderate Risk, Low Risk)

	Consequence				
Probability	Insignificant	Minor	Moderate	Very High	Extreme
Almost Certain	M	H	C	C	C
Likely	M	H	C	C	C
Possible	L	M	H	C	C
Unlikely	L	M	M	H	H
Rare	L	L	L	M	M

Level of Inherent Risk	Description	Inherent Risk I *P
Critical	Critical Risk, Immediate action required	Over 260
High	High Risk, Corporate senior management attention needed to develop and possibly initiate action steps in the near future	151 to 260
Moderate	Moderate Risk, Functional head attention needed	76 to 150
Low	Low Risk, Manage by routine procedures	Less than 75

6.3 Risk Assessment Report

There are different kinds of risk assessment reports. As risk assessment follows risk identification, a lot of these documents will be based on the risk identification reports. Documentation is done in a systematic way and can be from different inputs. Some of stakeholder Analysis - Risk Report: This identifies probable risks posed by take holders and the impact the risk might have on other stakeholders or the project at large. WBS - Risk Report: The work breakdown structure, broken down to work packages can be assessed for risks. It may detail risks at different stages based on cost, schedule, resource and manpower factors. Scope - Risk Report: The scope statement or mission statement may be assessed for risks at the beginning of a project. For example, it could be the impact of a particular project on the community. Cost Evaluation Risk Report: Cost or funds are at constant risk in a project. It has to be maintained and controlled with as little deviation as possible from the forecasted values. Risks related to cost are in the cost evaluation risk reports. Schedule Evaluation Risk Report: Time is luxury that a project cannot afford. It is imperative that time schedules are met with as little delay as possible. Time delays can impact the progress of a project and put it at risk. Such risks are documented in the schedule evaluation risk report. Technical Evaluation Risk Report: Risks related to resources, manpower and departments fall under this category. Risks arising due to quality constraints and those which are due to design errors and poor planning also fall under this group.

6.3. Risk Mitigation

A systematic reduction in the extent of exposure to a risk and/or the likelihood of its occurrence is called risk mitigation. It is also called risk reduction. A solution to mitigate the risk is developed and modeled to determine the level of reduced risk versus the cost to implement. If the solution provides an acceptable level of reduction in risk

for the associated cost, then it is considered successful and the process is complete.

The RMP can be thought of as a **spiral model** that allows a user to complete the process and then review the results. If the risk mitigation process was successful, then the process stops at the end of the post-mitigation task. If the risk or cost is not acceptable, then the entire process is repeated to determine if it can be improved. Best practices require that the known and perceived risk be analyzed according to the degree and likelihood of the adverse results that are anticipated to take place. Thereafter, all such risks analyzed shall be documented according to their levels of priority in a form known as the risk mitigation plan. After which, the development and integration of the corresponding risk mitigation strategies follows, and shall be referenced against the previously prepared risk management plan. A risk mitigation plan shall serve as the checklist of the anticipated risks, accordance with degree of their probability, as High, Medium or Low. Some project managers, however, deem it more appropriate to categorize the risks as most Likely, Likely or Unlikely. There are different kinds of risk assessment reports. As risk assessment follows risk identification, a lot of these documents will be based on the risk identification reports. Documentation is done in a systematic way and can be from different inputs. Some of them are discussed below.

7. Good Security Practice

The risk assessment process is usually repeated at least every 3 years. However, risk management should be conducted and integrated in the SDLC for IT systems, not because it is required by law or regulation, but because it is a good practice and supports the organization‘s business objectives. There should be a specific schedule for assessing and mitigating mission risks, but the Periodically performed process should also be flexible enough to allow changes where warranted, such as major changes to the IT system and processing environment due to changes resulting from policies and new technologies.

8. Keys for Success

A successful risk management program will rely on

(1) Senior management‘s commitment. (2) The full support and participation of the IT team

(3) The competence of the risk assessment team, which must have the expertise to apply the risk assessment methodology to a specific site and system, identify mission risks, and provide cost-effective safeguards that meet the needs of the organization.

(4) The awareness and cooperation of members of the user community, who must follow procedures and comply with the implemented controls to safeguard the mission of their organization.

(5) An ongoing evaluation and assessment of the IT-related mission risks.

Reference :

(1) Risk Management guide by National Institute of Standard Technology.
(2) IT security and risk management by Verizon Business.
(3) A graphical approach to risk identification, motivated by Empirical.