Chapter 6

Risk Engineering

6.1 Risk Engineering

Risk analysis and management are a series of works that help a system development team to understand and manage uncertainty. Many problems can arise while developing a system. A risk is a potential problem – it may happen may not. There are several steps to analyze and manage risks. The first step is risk identification. Next each risk is analyzed to determine the likelihood that it will occur and the damage that it will do if it does occur. Once this information is established risks are remarked. Finally, a plan is developed to manage those risks with high probability and impact.

There are different Stages of risks. They area:

1. **Risk identification:** Risk identification is the process of detecting potential risks or hazards through data collection. A range of data collection and manipulation tools and techniques exists. The team is using both automated and manual techniques to collect data and begin to characterize potential risks to Web resources. Web crawling is one effective way to collect information about the state of Web pages and sites.

2. **Risk classification:** Risk classification is the process of developing a structured model to categorize risk and fitting observable risk attributes and events into the model. The team combines quantitative and qualitative methods to characterize.

3. **Risk assessment:** Risk assessment is the process of defining relevant risk scenarios or sequences of events that could result in damage or loss and the probability of these events. Many sources focus on risk assessment. Rosenthal describes the characteristics of a generic standard for risk assessment as "transparent, coherent, consistent, complete, comprehensive, impartial, uniform, balanced, defensible, sustainable, flexible, and accompanied by suitable and sufficient guidance.

4. **Risk analysis:** Risk analysis determines the potential impact of risk patterns or scenarios, the possible extent of loss, and the direct and indirect costs of recovery. This step identifies vulnerabilities, considers the willingness of the organization to accept risk given potential consequences, and develops mitigation responses.

5. **Risk management implementation:** defines policies, procedures, and mechanisms to manage and respond to identifiable risks. The implemented program should

balance the value of assets and the direct and indirect costs of preventing or recovering from damage or loss. (Risk Managment, 2018)

6.2 Risk Identifications

Table XIII. Risk Identifications

Risk Type	Possible Risks
Technology	▪ Security of the system. ▪ Reusable software components may contain defects and cannot be reused as planned.
People	▪ Key staff are ill and unavailable at critical o times. ▪ Required training for staff is not available.
Organization	▪ Organizational financial problems reductions in the project budget.
Requirements	▪ Changes to requirements that require major design rework are proposed. ▪ Customers fail to understand the impact of requirements changes.

(Risk Managment, 2018)

6.3 Risk Analysis

Table XIV. Risk Analysis

Risk	Probability	Effect
Organizational financial problems force reduction in the project budget	Low	Disastrous
Security of the System High Serious	High	Serious
Reusable software components contain defects that means they cannot be reused as planned.	Moderate	Serious
Changes to requirements that require major design rework are proposed.	Moderate	Serious
Required training for staff is not available.	Moderate	Tolerable
Customers fail to understand the impact of requirements changes.	Moderate	Tolerable

(Risk Managment, 2018)

6.4 Risk Planning

Table XV. Risk Planning

Risk	Strategy
Security	Investigate the possible security leaks and measurements.
Organizational financial problem	Prepare a briefing document for senior management showing how the project is making a very important contribution to the goals of business and presenting reasons why cuts to the project budget would not be cost-effective.
Requirements problems	Alerts customer to potential difficulties and possibilities of delay, investigate buying in components
Staff illness	Reorganize them so that there is more overlap work and people therefore understand each other jobs.
Defective component	Replace defective potential components with bought in component of know reliability.
Requirements change	Replace defective potential component with bough in component of know reliability.
Requirement changes	Derive traceability information to access requirements, change impact, maximizing information hiding in the design.

6.5 Risk Monitoring

A re-planning of the project occurs. New task schedule and milestones are defined. Staffs work on their assigned jobs within the new timelines. In order to prevent this happening, the software will develop for the end user.

The user interface will design in a way to make of the program convenient and pleasurable. Meetings (formal and informal) will be the client regularly. This ensures that the software we are developing solves problems.

The development cost of the software may increase by 20%. During development it is advised to consult with the system analyst during the system analysis, design testing phase of the software project.

Proper coding grammar is followed to make sure that the codes are easily understandable and reusable.

Cost and time will increase and project will be updated. Everything will be at where it all started. (Risk Managment, 2018)