EXPERIMENT 04

CLASS: TE CMPN A PID: 182027

NAME: REBECCA DIAS ROLL NO. : 19

Aim:

Risk Analysis for **Hospital Management System**

Theory:

1. What is Risk and types?

Risk is an expectation of loss, a potential problem that may or may not occur in the future. It is generally caused due to lack of information, control or time.A possibility of suffering from loss in software development process is called a software risk. Loss can be anything, increase in production cost, development of poor quality software, not being able to complete the project on time. Software risk exists because the future is uncertain and there are many known and unknown things that cannot be incorporated in the project plan. A software risk can be of two types (a) internal risks that are within the control of the project manager and (2) external risks that are beyond the control of project manager. Risk management is carried out to:

1. Identify the risk
2. Reduce the impact of risk
3. Reduce the probability or likelihood of risk
4. Risk monitoring

A project manager has to deal with risks arising from three possible cases:

1. Known knowns are software risks that are actually facts known to the team as well as to the entire project. For example not having enough number of developers can delay the project delivery. Such risks are described and included in the Project Management Plan.
2. Known unknowns are risks that the project team is aware of but it is unknown that such risk exists in the project or not. For example if the communication with the client is not of good level then it is not possible to capture the requirement properly. This is a fact known to the project team however whether the client has communicated all the information properly or not is unknown to the project.
3. Unknown Unknowns are those kind of risks about which the organization has no idea. Such risks are generally related to technology such as working with technologies or tools that you have no idea about because your client wants you to work that way suddenly exposes you to absolutely unknown unknown risks.

Software risk management is all about risk quantification of risk. This includes:

1. Giving a precise description of risk event that can occur in the project
2. Defining risk probability that would explain what are the chances for that risk to occur
3. Defining How much loss a particular risk can cause
4. Defining the liability potential of risk

Risk Management comprises of following processes:

5. Software Risk Identification
6. Software Risk Analysis

7. Software Risk Planning
8. Software Risk Monitoring

2. Steps for Risk Analysis

Risk Management is an important part in project planning activities. It involves identifying and estimating the probability of risks with their order of impact on the project.

a. Risk Identification

Risk identification involves brainstorming activities. it also involves preparation of risk list. Brainstorming is a group discussion technique where all the stakeholders meet together. this technique produces new ideas and promote creative thinking.
Preparation of risk list involves identification of risks that is occurring continuously in previous software projects.

b. Risk Assessment

It is a process which consist of following steps:

- Identifying the problems causing risk in projects
- Identifying the probability of occurrence of problem
- Identifying the impact of problem
- Assigning values to step 2 and step 3 in the range of 1 to 10
- Calculate the risk exposure factor which is product of values of step 2 and step 3
- Prepare a table consisting of all the values and order risk on the basis of risk exposure factor

For example,

Risk No	Problem	Probability of occurrence of problem	Impact of problem	Risk exposure	Priority
R1	Issue of incorrect password	2	2	4	10
R2	Testing reveals lot of defects	1	9	9	7

R3	Design is not robust	2	7	14	5

c. Calculate Risk Exposure for your system

Risk Avoidance and Mitigation:
The purpose of this technique is to altogether eliminate the occurrence of risks. so the method to avoid risks is to reduce the scope of projects by removing non-essential requirements.

Risk Monitoring:
In this technique risk is monitored continuously by reevaluating the risks, the impact of risk and probability of occurrence of risk.
This ensures that:

- Risk have been reduced
- New risk are discovered
- Impact and magnitude of risk are measured

3. Identify any two risks of your own system under development and prepare RMMM for the same.

Risk	Category	Probability	Impact	RMMM
Customer will change requirements	PS	60%	2	1.1
Lack of Training on Tools	DE	80%	3	1.2
Technology will not meet expectations	TE	40%	1	1.3
Lack of Testing on Mobile Phones	DE	60%	2	1.4
Predicting wrong Output	TE	20%	2	1.5
End users resist system	BU	70%	3	1.6
Computer Crash	TE	70%	1	1.7
Website Hacked	TE	40%	1	1.8

RISK INFORMATION SHEET			
Risk ID: 1.5	Date: 01/04/201	Probability: 20%	Impact: 2
Description: There is a good amount of probability that the training algorithm used for machine learning can predict wrong output and which has to be taken care of.			

Refinement/Context: The website is made to predict if the message is spam or not and if the prediction is wrong then there is no use of using this website as a preventive measure to stay away from cybercrimes.	
Mitigation/Monitoring: 1. Prepare better algorithms for training the machine learning model. 2. Monitor the predictions of the website and try to understand if the prediction is correct as per human thinking of a cyber security expert.	
Management/contingency plan/trigger: Get a new training algorithm for the website so the users get better predictions.	
Current status: 06/04/2021: Website is being monitored for predictions	
Originator: Rebecca Dias	Assigned: Delicia Fernandes

RISK INFORMATION SHEET			
Risk ID: 1.8	Date: 01/04/2020	Probability: 40%	Impact: 1
Description: Every software built is viable of being hacked, so to handle this risk some precautions are already taken into consideration.			
Refinement/Context: The website has user credentials stored, if the website is hacked there is a probability of data leaks.			
Mitigation/Monitoring: 1. Contact third-party network professionals for penetration testing. 2. Build proper hashed user credentials to be safe from normal brute-force attacks.			
Management/contingency plan/trigger: Shut Down the website if found being hacked to prevent the data leaks			
Current status: 06/04/2021: All steps completed			
Originator: Rebecca Dias			Assigned: Chelsea Dsouza

Conclusion:

From this experiment, we learned about risk analysis in software engineering.We understood the concept of risk tables and risk information sheet(RIS) where in the risk table we will list all the potential risks of the software with the category of the risk, probability,impact of the risk and RMMM number. Risk information Sheet will have the Context, mitigation, monitoring, management plans of RMMM is that risk occurs.We implemented the same for our project software.