Name : Chirag Khatri
Roll no : 1902076

Experiment 4

Aim: Prepare RMMM plan for the project.

Theory:

Planning the risk management
The proactive strategy for risk estimation is used which helps us in identifying the possible threats that can occur during the project well in advance. Accordingly, steps to avoid, monitor and manage the risk are to be carried out and noted down in the form of RMMM plan.
Example:
THE RMMM PLAN
A risk management strategy can be included in the software project plan or the risk management steps can be organized into a separate *Risk Mitigation, Monitoring and Management Plan.* The RMMM plan documents all work performed as part of risk analysis and is used by the project manager as part of the overall project plan. Some software teams do not develop a formal RMMM document. Rather, each risk is documented individually using a *risk information sheet* (RIS) . In most cases, the RIS is maintained using a database system, so that creation and information entry, priority ordering, searches, and other analysis may be accomplished easily.
Once RMMM has been documented and the project has begun, risk mitigation and monitoring steps commence. As we have already discussed, risk mitigation is a problem avoidance activity. Risk monitoring is a project tracking activity with three primary objectives:
(1) to assess whether predicted risks do, in fact, occur;
(2) to ensure that risk aversion steps defined for the risk are being properly applied;
(3) to collect information that can be used for future risk analysis. In many cases, the problems that occur during a project can be traced to more than one risk. Another job of risk monitoring is to attempt to allocate *origin* (what risk(s) caused which problems throughout the project).

Risk Identification Management Process

Risk Identification and Management Process comprises of the following steps:

1. Risk Identification

2. Risk Analysis

3. Risk Assessment

4. RMMM (Risk Mitigation, Monitoring, Management) plan

Procedure / Approach /Algorithm:

1. Identify at least five risks for the case study you had selected for the first experiment. Analyze the risks, on the basis of type, probability and impact. Rank (prioritize) the risks on the basis of the value of Risk Exposure using the template given below.

Risk Exposure = Probability of occurrence * impact

IT Project Risk Impact Analysis and Ranking

Sr. No.	Risk	Probability	Impact	Risk Exposure	Ranking
1	Heavy traffic	60%	4	Rs. 24,000/yr	High priority
2	System getting attacked	40%	3	Rs. 10,000/month	
3	Loss of data		3	Rs. 3,000/month	Moderate Priority
4	Unauthorized access to assets and tampering with them	50%	2	Rs. 2,500/month	Low Priority
5	Bad User Experience	30%	2	Rs.4,500/month	Low Priority

Impacts: 4 - Catastrophic || 3 - Critical || 2 - Marginal || 1 - Negligible

Risk Exposure:

Risk: The webapp receives heavy traffic.
The webapp can experience heavy traffic in the future, that is, many users can search for the results simultaneously. The performance at that time can drop significantly.

Risk probability: 60%

Risk Impact:
The risk impact can be catastrophic, as this can hamper the webapps user experience very heavily. The users might face very long waiting times for the response to be fetched for a particular search query.

This risk can be mitigated by hosting multiple instances of the various important services that are responsible for the smooth functionality of the necessary features of the webapp. Load balancers can be used to direct the heavy traffic which might be faced by the webapp to redirect the users to the appropriate instance of the service.

For the client side optimization, caching can be used to cache the static files of the webapp. This will make sure that for the consequent requests after the first request, the webapp loads comparatively faster.

The cost to host and maintain can roughly be around Rs.

40,000/yr. **Risk exposure:**

RE = 0.6 x 40000 = Rs. 24000/yr

Risk id: 1	**Date**: 24/08/2021	**Probability:** 60%	**Impact:** catastrophic
Description: The webapp receives heavy traffic. The webapp can experience heavy traffic in the future, that is, many users can login or register simultaneously. The performance at that time can drop significantly.			
Refinement/Context: Sub condition 1: The risk impact can be catastrophic, as this can hamper the webapps user experience very heavily. Sub condition 2: The users might face very long waiting times for the response to be fetched. The users might also face session timeouts very frequently.			

Mitigation/Monitoring: 1. Hosting multiple instances of the various important services. 2. Setting up load balancers to direct the heavy traffic. 3. Caching can be used to cache the static files of the webapp.	
Management: RE computed to be Rs. 24,000/yr	
Current Status: Mitigation steps to be initiated	
Originator: Chirag Khatri	**Assigned:** Jenil Kothari

Risk Exposure

Risk: System getting attacked

Here we have to take into consideration that there might be sensitive information stored by the system, even though there might be a lot of potential threats related to the system. This event might cause a loss of confidentiality and integrity as this has information stored related to the user.

Risk Probability: 40%

Risk Impact:

Here the impact is of critical level as it is not very unlikely to happen but it still holds a possibility. Here it can be categorized into different threats, there could be a loss of availability if there's an attack on the system and the data does not exist or the data cannot be retrieved.

Loss of confidentiality as the system is attacked by external hackers which might give them sensitive information related to the user or if the data is made public without approval. Loss of integrity where the system cannot be trusted anymore with the valuable data or if the data is incomplete or incorrect.

The risk can be mitigated by hiring a penetration tester to test security

and getting DNS verified and buying an SSL certificate for https secure connection.

Assuming cost of hiring penetration testers to test security of app and buying an SSL certificate is around Rs. 25,000/month

Risk exposure:
RE = 0.4 x 25000 = Rs. 10000/month

Risk id: 2	**Date**: 24/08/2021	**Probability:** 40%	**Impact:** critical
Description: System getting attacked by external hackers which might lead to sensitive information being public or loss of valuable data or the data cannot be authorised or accessed. Other potential risks that might lead to confidentiality and integrity issues			
Refinement/Context: Sub condition 1: The risk impact can be critical as this might expose information to the public. Sub condition 2: Loss of valuable data or the data being incomplete or incorrect.			
Mitigation/Monitoring: 1. Endpoint protection is designed to detect and terminate these attacks. 2. The software will also alert admins that such an attack has occured. 3. Penetration testers should be hired to test the security of the application. 4. Buy an SSL certificate for https connection.			
Management: RE computed to be Rs. 10,000/month			
Current Status: Mitigation steps to be initiated			
Originator: Isha Khatri		**Assigned:** Muskan Khasturia	

Risk Exposure:
Risk: Loss of database.
The data loss can happen in the case of hardware getting corrupted or it can also happen in a case of human error. The probability of this happening is less.

Risk probability: 20%

Risk Impact:
This risk can be critical as the users of this webapp can be disappointed if all of their data such as yearly ,monthly reports and such data goes missing.

The risk can be mitigated by keeping a copy of the database or by performing regular database backups. Also this risk can be avoided by writing code and testing it inside a development environment by taking the web application down for the maintenance.

Assuming that the cost of any good database backup service is around Rs. 15,000/month.

Risk exposure:

RE = 0.2 x 15000 = Rs. 3000/month

Risk id: 3	**Date**: 10/08/2021	**Probability:** 20%	**Impact:** critical
Description: The data loss can happen in the case of hardware getting corrupted or it can also happen in a case of human error. The probability of this happening is less.			
Refinement/Context: Sub condition 1: This risk can be critical as the users of this webapp can be disappointed if all of their data such as yearly ,monthly reports and such data goes missing Sub condition 2: This can create a sense of disappointment amongst the users.			
Mitigation/Monitoring: 1. Keeping a copy of the database. 2. Performing regular database backups. 3. Writing code and testing it inside a development environment by taking the web application down for the maintenance.			
Management: RE computed to be Rs. 3,000/month			
Current Status: Mitigation steps to be initiated			

Originator: Chirag Khatri	**Assigned:** Isha Khatri

Risk Exposure:

Risk: Unauthorized access to assets and tampering with them

If the network is compromised, intruders can attack or misuse the system.
Legal implications: security or privacy breaches can expose a company to lawsuits from investors, customers, or the public.
Internet Protocol (IP) spoofing: a system is configured to impersonate another system's IP address in an attempt to gain access to the targeted system
Unauthorized software increases the risk of outsiders gaining access to sensitive data. Any software that is not authorized is likely managed without proper patching, updates, configurations, and security protocols

RIsk Probability: 50%

Risk Impact:

Unauthorized disclosure of information: disclosure of confidential, sensitive or embarrassing information can result in loss of credibility, reputation, market share, and competitive edge.
Legal implications: security or privacy breaches can expose a company to lawsuits from investors, customers, or the public.
Disruption of computer services: be unable to access resources when they are needed can cause a loss of productivity. Disruption of services during critical processing time may be disastrous

Approximate charges to build a strong firewall can be around Rs. 5,000/month.

Risk exposure:

RE = 0.5 x 5000 = Rs. 2500/month

Risk id: 4	**Date**: 24/08/2021	**Probability:** 50%	**Impact:** marginal

Description:
Unauthorized software increases the risk of outsiders gaining access to sensitive data. Any software that is not authorized is likely managed without proper patching, updates, configurations, and security protocols

Refinement/Context:
Sub condition 1:
Disruption of computer services: be unable to access resources when they are needed can cause a loss of productivity. Disruption of services during critical processing time may be disastrous

Sub condition 2:
Legal implications: security or privacy breaches can expose a company to lawsuits from investors, customers, or the public.
.

Mitigation/Monitoring:
1. Building strong firewall, good protection of data encryption
2. Ensuring integrity within the company

Management:
RE computed to be Rs. 2,500/month

Current Status:
Mitigation steps to be initiated

Originator: Muskan Khasturia	**Assigned:** Jenil Kothari

Risk Exposure:

Risk: Bad User experience

If our competitors provide a better user experience (UX) then they stand a good chance of landing the sale that we lost.
If the site makes it difficult for the users to calculate daily expenses or it isn't optimized for viewing on different screens, confusing navigation, lack of information or isn't responsive then it all adds to a bad user experience.

Risk Probability: 30%

Risk Impact:
Bad user experience can lead to loss in revenue as customers are more likely to visit rival web applications with a decent user experience.
Bad UX can decrease efficiency among users. This can also cause decreased retention rate.
The app development team's productivity is also negatively affected by poor user experience

Approximate charges of hiring a good UX designer can be around Rs. 15000/month.

Risk exposure:

RE = 0.3 x 15000 = Rs. 4,500/month

Risk id: 5	**Date**: 24/08/2021	**Probability:** 30%	**Impact:** marginal
Description: If our competitors provide a better user experience (UX) then they stand a good chance of landing the sale that we lost.			
Refinement/Context: Sub condition 1: Bad user experience can lead to loss in revenue as customers are more likely to visit rival web applications with a decent user experience. Sub condition 2: The app development team's productivity is also negatively affected by poor user experience			
Mitigation/Monitoring: 1. Hire good UX designers 2. Make sure the features are sufficient for the app.			
Management: RE computed to be Rs. 4,500/month			
Current Status: Mitigation steps to be initiated			
Originator: Jenil Kothari		**Assigned:** Isha Khatri	