BHARTIYA VIDYA BHAVANS

SARDAR PATEL INSTITUTE OF TECHNOLOGY

Bhavan's Campus, Munshi Nagar, Andheri (West), Mumbai

Software Engineering Lab

Group Members:

Shreya Shetty 2019140059

Shruti Shetty 2019140060

Topic: Resort Property Management System

Experiment No. : 5

Aim : Develop Risk Mitigation, Monitoring and Management Plan for the your case study

Problem Statement : The main objective of this project is to build a resort management system that consists of all the features and functions required for effectively managing a chain of resorts and to have an online presence that makes the reservation process easier and delivers outstanding customer service. The Resort Property Management System will permit employees to manage the daily administrative tasks of the resort and ensure smooth functioning of the resort. The system will be able to handle many services to take care of all customers in a quick manner. As a solution to the large amount of file handling happening at the resort, this software will be used to overcome those drawbacks.

RISK TABLE :

Risk ID	Risk	Category	Probability	Impact
1	System crash	Technical Issues	70%	1
2	The project is not completed on time	Business Impact Risk	40%	1
3	Poor comments in code	Technical Issues	25%	4
4	Improper estimation of budget	Financial Risk	30%	3
5	The employees lack of knowledge, training and experience	Staff Size and Experience Risk	40%	1
6	Insufficient resources	Development Environment Risk	20%	3
7	Internet Issue	Technical Issues	45%	3
8	Loss of integrity, confidential information	Security Privacy Issue	35%	1
9	Data Loss	Technical Issue	20%	2
10	Risks related to dispute	Project Risk	35%	2
11	Testing Failure	Technology Issue	25%	2

Impact Values Description :

1. Catastrophic
2. Critical
3. Marginal
4. Negligible

RISK INFORMATION SHEET:

Risk Id: 1	**Date:** 1.11.2021	**Probability:** 70%	**Impact:** 1
Description: When server crashes, the website, software application, or operating system stops functioning and does not get displayed.			
Context: Considering that the servers of the software are already down due to one of the possible reasons, the reliability is affected along with the productivity and the counter measures need to taken immediately.			
Mitigation Plan: Creating multiple backup copies of the software in development and all documentation associated with it.			
Monitoring Plan: The employees should always be aware of the stability of the computing environment they're working in and should monitor all the changes closely. Any changes in the stability of the environment should be recognized, reported and taken seriously.			
Management Plan: System crash is extremely hazardous to a software development team. It can lead to great losses. In case of such failure, the development team should cease work on that system until the environment is made stable again, or should move to a system that is stable and continue working there.			
Status: Mitigation steps initiated			
Originator: Server Administrator (Owner)		**Assigned:** Developer	

Risk Id: 2	**Date:** 1.11.2021	**Probability:** 40%	**Impact:** 1
Description: The project is not completed and delivered to the client in the given deadline.			
Context: 1. Insufficient project tracking 2. Lack of coordination and communication 3. Not reserving time to deal with unexpected issues			
Mitigation Plan: Keeping regular tabs on the development team to ensure they are working and holding regular meets to discuss about the progress. Give each task a due date and assign them to team members. Every task that is completed is one step closer to reaching the final goal. Completing daily and weekly tasks will also help promote a sense of accomplishment within the team members and boost team morale.			
Monitoring Plan: A timeline should be formulated keeping the deadline in mind so as to monitor project status accordingly. The timeline should be followed strictly at all times and in all development stages for timely completion of project.			
Management Plan: Requesting the client to extend the deadline.			
Status: Mitigation steps initiated			
Originator: Client		**Assigned:** Shreya Shetty	

Risk Id: 3	**Date:** 1.11.2021	**Probability:** 25%	**Impact:** 4
Description: There are no or minimum comments in the code or the comments are not easy to interpret by others and the code will be difficult to maintain and update.			
Context: The developer didn’t put appropriate efforts to write the comments.			
Mitigation Plan: To minimize the poor code comments, commenting standards should be created and conveyed for understanding and improving quality of comments in all the code.			
Monitoring Plan: There should be careful monitoring to minimize the impact of poor commenting			
Management Plan: Appropriate time be given to make the required changes and make the commenting appropriate according to the standard specified.			
Status: Mitigation steps initiated			
Originator: Admin		**Assigned:** Shruti Shetty	

Risk Id: 4	**Date:** 1.11.2021	**Probability:** 30%	**Impact:** 3
Description: Improper estimation of the budget or allocations in order to support software development and project. The monetary budget provided by the client is insufficient.			
Context: 1. Underestimation of future costs (or the making of overly optimistic estimates) 2. Disputes related to budget with client 3. Poor resource coordination			

4. Project not completed on time leading to increase in rental costs, resources etc.	
Mitigation Plan: Proper budget should be created in the beginning and be approved by the client. All the one-time, ongoing and outgoing cost where the fund spent should be filed in a report properly.	
Monitoring Plan: Monitor costs and commitments of large and high-risk incentives. Share timely information on incentives across relevant team and people.	
Management Plan: Be responsive to the customers and subcontractors and talk to the team honestly and agree on the priorities. To regain additional budget, negotiate better pricing or terms for materials, works, renegotiate contracts with subcontractors, etc	
Status: Mitigation steps initiated	
Originator: Client	**Assigned:** Shreya Shetty

Risk Id: 5	**Date:** 1.11.2021	**Probability:** 40%	**Impact:** 1
Description: Employees lack required technical knowledge and exposure to the industry for developing the project.			
Context: 1. The employees with the right knowledge are not available or busy with other projects 2. While selecting the project members, the required skills were not taken into consideration 3. The employees are freshers			
Mitigation Plan: Assign project to developers well acquainted with the required technical skills and knowledge. Provide required training to them before the project starts.			
Monitoring Plan: Check the status of the project and monitor each assigned employees work regularly.			
Management Plan: Recruit new team members with more knowledge of the technical skills and experience required for the project to provide assistance and training to the original project team.			
Status: Mitigation steps initiated			
Originator: Employee		**Assigned:** Shruti Shetty	

Risk Id: 6	**Date:** 1.11.2021	**Probability:** 20%	**Impact:** 3
Description: No proper resources are available or lack of it affecting the project			
Context: 1. Lack of planning of the entire project 2. There might be another project that ends up combining with this project and some of the resources are pulled from this work to another projects. 3. Improper planning of budget leading less funds for required resources			
Mitigation Plan: Prevent the lack of resources by collecting the requirements, defining scope, analysing risks, defining and estimating activities, and creating a realistic schedule. Make a good resource plan.			
Monitoring Plan: In order to control our progress, regular checks should be made to ensure the schedule is followed and re-estimate the resources needed to check if the initial estimations are updated.			

Management Plan: Try to reduce the resources needed by reusing previous design or existing assets.			
Status: Mitigation steps initiated			
Originator: Client		**Assigned:** Shreya Shetty	

Risk Id: 7	**Date:** 1.11.2021	**Probability:** 45%	**Impact:** 3
Description: Internet issue effects on connectivity. Since we are connecting users from different devices, so if the user has an internet issue, then they might not be able to connect to the software.			
Context: 1. Insufficient bandwidth 2. Further away from the router leading to internet issues			
Mitigation Plan: To prevent it downtime, have a backup plan. Setup a network redundancy. Network redundancy means there are multiple data paths between network locations, so if one fails, an alternate is available.			
Monitoring Plan: Monitoring internet connectivity on regular time intervals.			
Management Plan: Follow the recovery plan step by step.			
Status: Mitigation steps initiated			
Originator: Client		**Assigned:** Developer	

Risk Id: 8	**Date:** 1.11.2021	**Probability:** 35%	**Impact:** 1
Description: Failure to ensure that data is properly protected and in accordance with the law can lead to lawsuits as well as damage the reputation and loss.			
Context: 1. Considering that the account details have been leaked either by mistake from the user or through the corruption of the database. 2. If data corruption happens due to some cyberattack or some major technical failure, the privacy has been jeopardized. 3. If the login credentials has been compromised either by user's mistake or due to data leak, it can jeopardize the privacy of the users' accounts and their details thus leading to misuse.			
Mitigation Plan: Ensuring data in the database to be safe from any type of attacks along with periodic data backups. The user should be notified to take precautionary measures at all times. A strong education and training program for the employees about protecting confidential information. Conducting information security training sessions on specific topics to keep information security top of mind and having employees well trained and aware of proper protocols.			
Monitoring Plan: When using passwords to control access to confidential information, it should be ensured that they're both secure and changed regularly. There should be regular monitoring of activities on user's account to detect any unusual practice.			
Management Plan:			

Delete the concerned portion of the database related to the respective details and replace it with the backed up data	
Status: Mitigation steps initiated	
Originator: Client	**Assigned:** Developer

Risk Id: 9	**Date:** 1.11.2021	**Probability:** 20%	**Impact:** 2
Description: While storing the data into database there might chances of data loss while transferring of data or while connecting to database			
Context: 1. Internet loss while connecting to database. 2. Multiple times logging with incorrect credentials leading to automatic loss of data since the system perceives it as a threat.			
Mitigation Plan: Ensuring data is backed up regularly and transferred safely and carefully. Also, backup should be taken before any transfer of data.			
Monitoring Plan: Checking if multiple backups of data are regularly taken and monitoring closely while transferring the data.			
Management Plan: Restore data from the backup taken before the loss.			
Status: Mitigation steps initiated			
Originator: Server Administrator		**Assigned:** Developer	

Risk Id: 10	**Date:** 1.11.2021	**Probability:** 35%	**Impact:** 2
Description: A project is handled by many people and it is likely to happen that disputes can arise due to different thoughts, different, and different expectations. So, therefore, this is included in the project risk examples.			
Context: 1. Meeting agendas not covered properly 2. Project details not disclosed with the client properly 3. Client does not have a clear idea about the requirements 4. Different views and approach on how the project should carried on and the deadline			
Mitigation Plan: The way to avoid such risks is to conduct meetings on a regular basis and let all the team members and project related personnel participate so that the issues can be discussed openly and a relevant solution is provided as soon as possible.			
Monitoring Plan: Regular reports generation after each meeting and sending it to all members and taking their approval.			
Management Plan: Discussing the issue openly with all the concerned parties and sorting the issue as soon as possible. Also, taking opinion from third party to sort the issue.			
Status: Mitigation steps initiated			
Originator: Client		**Assigned:** Shruti Shetty	

Risk Id: 11	**Date:** 1.11.2021	**Probability:** 25%	**Impact:** 2
Description: In case of Testing Failure, the software’s reputation will be at risk. The test taken by the user might fails due some technical reason.			
Context: Considering a test being taken by the user fails due some technical reason.			
Mitigation Plan: Ensuring that the server is running properly, connection to the database is well established, and verifying the details entered for the test are valid.			
Monitoring Plan: Look out for the servers, connections while the transfer of data is being processed.			
Management Plan: Notify the user immediately on failure and give the leisure to re-take the test whenever possible.			
Status: Mitigation steps initiated			
Originator: Client		**Assigned:** Developer	

Conclusion: In this experiment, we identified risks based on the probability and their impact for our case study and created Risk Information Sheet. A RMMM plan for the risks pertaining to our case study was also written. 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.