Dhruvin Chawda
60004210159
C22

SE Experiment 8

Aim: To create a RMMM plan for a case study (Virtual connect)

Theory:

* Risks for online Meeting Software:

① Server Downtime: Unexpected server outages due to hardware failure, any software bugs or cyberattacks. This can lead to inaccessible meetings.

② Inaccurate Estimation: Underestimation of size of software leading resource storage and schedule delays.

③ Bandwidth limitation: Insufficient network bandwidth leading to degraded audio/video quality and dropped calls. This can happen due to large number of users getting connected.

④ Integration Problems with Third party APIs: Difficulties in in tegration of software with apis, also change in policy of APIs, problems in APIs can effect the software too.

⑤ Security Breaches: Unauthorized access, data breaches, or security vulnerabilities comprising user data and trust. This can lead to potential legal implication & impacting user acquisition.

(6) Changes in Requirements: Regulatory changes requiring updates to software to maintain compliance.

(7) Inadequate Testing Procedure: Insufficient testing of software before deployment, leading to undetected bugs and glitches.

(8) Compatibility Issues: Software is not fully compatible with various devices or operating system, limiting user accessibility which effects user experience.

(9) Late Delivery: Late Delivery of software updates or new features can lead to missed opportunities, customer dissatisfaction and decreased competitiveness.

(10) Poor Comments in Code: This can hinder understanding maintenance, collaboration among developers leading to bugs and errors. This can in turn degrade product quality, slower innovation and increase likelihood of bugs and vulnerabilities.

Risk table:

TI → Technical Issue
TE → Technology Risks
PR → Process Risk
CR → Customer Related Risk
BU → Business Impact Risks

Risk table:

	Risk	Category	Probability	Impact
①	Server Downtime	TI	20	1
②	Inaccurate Estimation	PR	20	3
③	Bandwidth Limitation	TI	25	2
④	Integration Problems	TI	20	2
⑤	Security Breaches	CR	30	1
⑥	Changes in Requirement	BU	30	2
⑦	Inadequate Testing Procedure	PR	15	3
⑧	Compatibility issues	TE	25	2
⑨	Late Delivery	BU	15	3
⑩	Poor Comments in Code	TI	20	4

Let the cut off here be probability 20% and impact being 2, so for RIS we choose Integration problems and made RIS for that Risk.

Conclusion: Hence we understood what is RMMM plan and How to make it and made one for our case study. Also we identified 10 Risks and understanding this Risk, SD can mitigate potential challenges.

Team Members :

Riddhi Shah-60004210161

Dhruvin Chawda-60004210159

Implementation :

Risk Table :

Risk	Category	Probability (%)	Impact
Server Downtime	Technical Issues	15	2
Inaccurate Estimation	Process Risks	20	3
Bandwidth Limitation	Technical Issues	25	2
Integration Problems	Technical Issues	20	2
Security Breaches	Customer Related Risks	30	1
Changes in Requirement	Business Impact Risks	25	2
Inadequate Testing Procedure	Process Risks	20	3
Compatibility Issues	Technology Risks	20	2
Late Delivery	Business Impact Risks	15	3
Poor Comments in Code	Development Environment Risks	15	2

Impact Values:

1 – Catastrophic

2 – Critical

3 – Marginal

4 – Negligible

Academic Year: 2023_24

Risk Information Sheet :

RISK INFORMATION SHEET			
RISK ID: P09-45	Date: 02/04/2024	Prob: 20%	Impact: Critical(2)

Description:

Integration problems may occur during the development, deployment, or ongoing operation of the online meeting software, leading to challenges in seamlessly connecting with third-party applications or services. These problems could result from issues such as incompatible APIs, data format inconsistencies, or communication failures between integrated systems.

Refinement/context:

Sub Condition 1: Lack of compatibility between the online meeting software and existing third-party tools or platforms.

Sub Condition 2: Issues with API communication or data interchange protocols between the software and external systems.

Sub Condition 3: Challenges in synchronizing data or functionalities across integrated systems, leading to inconsistencies or errors.

Mitigation/monitoring:

1. Conduct thorough compatibility testing with various third-party applications and platforms during the development phase.
2. Establish clear communication channels with third-party vendors or service providers to address integration issues promptly.
3. Implement robust error handling and logging mechanisms to monitor and troubleshoot integration failures in real-time.

Management/contingency plan/trigger:

1. Allocate additional resources or expertise to resolve critical integration issues that pose a significant risk to project timelines or functionality.
2. Explore alternative integration solutions or workarounds if the initial integration approach proves unsuccessful.
3. Communicate transparently with stakeholders about the status of integration efforts and any potential delays or challenges.

Current status:

10/04/2024: Mitigation steps initiated

Originator: Riddhi Shah	Assigned: Dhruvin Chawda