**Indian Institute of Information Technology Pune**

NAME: Deepesh Patil

GROUP: 2

MIS: 112215055

YEAR/SEM: 3rd Year/5th Sem

TASK-3:

Preparation of documents related to Software Configuration Management and Risk Management activities.

1. Software Configuration Management Document

1.1 Introduction

Purpose: The intention of this document is to highlight the course of action, the method of execution, and the tools to be used in the management and regulation of the configurations of the Online Course.

• Scope: This document applies to all aspects of the software development life cycle that involves requirements, design, implementation, testing, deployment, and maintenance of the CMS system.

1.2 Configuration Management Plan

1.2.1 Configuration Identification

Components

Source Code (Frontend, Backend)

Database Schemas

Configuration Files (Server settings, environment variables)

Documentation (SRS, Design Documents, User Manuals)

Test Cases and Scripts

Naming Conventions

Source code files: (e.g., course\_reservation\_v1.0.py)

Naming convention – The name of modules for a project.

version - The version of the file.

Example

* Development branch for on-going development
* Feature branches for specific functionalities, for example, feature-user-auth.

1.2.3 Configuration Control

• Change Request Process

o All Change requests need to be documented and approved by Configuration Control Board, CCB, before their implementation.

• Impact Analysis:

- To establish the impact of the proposed changes upon existing configurations, project time schedules and use of resources

• Implementation of the Change

- Changes are introduced in the Development Environment and tested before being merged into the main.

1.2.4 Configuration Status Accounting

• Documentation:

* Status report of configurations with present version, history, and the status of each configuration item.

•Tools to Track:

o Tracking of change requests and configuration status using issue tracking systems like Jira, Trello, etc.

1.2.5 Configuration Audit

•Audits Schedule:

o An audit should be scheduled frequently, e.g., quarterly, to ensure that changes are as per the SCM.

•Process of audits:

o Validations of Configuration items, change requests, and version histories against the SCM plan.

• Configuration Manager: Sole authority over the SCM process. Grants approval for the changes and has enterprise-level control over the configuration repository.

•Development Team: actual making changes, exercises version control, documents modifications.

•Quality Assurance Team: checks whether configurations are as per requirements/specifications. Audits

1.4 Tools and Technologies

Version Control: Git

Issue Tracking: Jira/Trello

Build Automation: Jenkins/Travis CI

Documentation: Confluence/Google Docs

2. Risk Management Document

2.1 Introduction

• Purpose: To identify, assess, and manage the risks associated with the development and deployment of the Online Course Reservation System.

• Scope: This document deals with the risks related to the project management and software development and deployment and maintenance phases.

2.2 Risk Identification

• Technical Risks:

o Tech Integration Issues: System integration with third-party payment gateways or any other third-party API.

o Vulnerability to Security: Possible security flaw in user authentication, data storage, and payment processing.

Performance Bottlenecks: It may not handle large traffic or big data sets.

• Project Management Risks:

o Scope Creep: Uncontrolled changes or continuous growth in project scope leading to delays and budget overruns.

o Resource Availability: The non-availability of skilled developers, testers, or any other critical resource.

o Timeline Slippage: Missing deadlines, delays in achieving milestones.

• Operational Risks:

o Data Loss: A chance of data loss due to software bugs, database corruption, or hardware failure.

o User Acceptance: Lousy approval of the solution from the audience due to usability issues or even not being aware.

• External:

o Regulatory: Non-compliance to acts like GDPR or the Payment Card Industry- Data Security Standard

o Third Party: Reliability on third-party vendors for value-driven services such as a payment gateway.

2.3. Risk Analysis

|  |  |  |  |
| --- | --- | --- | --- |
| **Risk Probability** | **Impact** | **Rating** | **How to Handle** |
| Integration Issues | Medium | High | early integration testing, modular design |
| Security Loopholes | High | High | frequent security audits, secure coding |
| Resource Availability | Low | High | Cross-train team members, do resource planning |
| Slippage in timeline | Medium |  | Use Agile development methodology, conduct progress reviews frequently |
| Loss of Data | High | High | Take regular backups, ensure redundancy |
| User Adoption | Medium | Medium | Train users and keep a feedback loop |
| Compliance Issues | Medium | Medium | Hire legal consultants and check compliance at regular intervals |

2.4 Strategies to Mitigate the Risk

• Problem in Integration : Use a modular design strategy, and.

• Performance Bottlenecks: Load testing and performance tuning of code. Develop using flexible architecture that scales.

• Scope Creep: Enforce good change management practices and maintain a clear, detailed record of requirements.

• Resource Availability: Ensure availability of back-up resources and cross-train to reduce disruption from resource unavailability.

•Timeline Slippage: Agile development methods with regular sprints and progress checks to stay on track.

• Data Loss: Periodic data backup, storage redundancy, and exercises around disaster recovery

• User Adoption: User-training sessions, feedback during development with continual improvement

• Compliance Issues: Consult law practitioners for compliance advice and regular review

• Vendor Dependence: Alternate vendor contingency planning to provide resistance against vendor dependence

2.5 Risk Monitoring and Reporting

• Monitoring: Monitor the status of the risk and mitigation strategies using the regular project meetings

• Reporting: Log all identified risks, their status as well as the actions taken in the risk register. Regular update of stakeholders

2.6 Roles and Responsibilities

• Project Manager: Responsible for the risk management process. To ensure that the risk mitigation strategies are applied

•Risk Management Team: Identifies, assesses and monitors risks through the project lifecycle.

• Development Team: Applies the risk mitigation strategies in the development process.

• QA Team: To test the system for any weaknesses and to oversee it complies with the required security and performance standards.