| **SOEN 390:**  **SOFTWARE ENGINEERING TEAM DESIGN PROJECT** |
| --- |
|  |
|  |
|  |
| **Condo Management System**  **Risk Management Plan** |
| **(Sprint 3)** |
|  |
|  |
| **Team 14** |
| **Instructor: Dr. Jinqiu Yang  Date: March 4th, 2024** |
| **Winter 2024** |

**History Backlog**

| **Date** | **Authors** | **Changes** |
| --- | --- | --- |
| 24/02/2024 | Jason Novio | Addition of **Risk ID 21, 22 & 23** |
| 20/03/2024 | Jason Novio | Implementation of the **Criteria for Defining Impact and Probability Levels** section |

**Risk Assessment and Management Plan (RMP)**

**Purpose of the Risk Management plan**

The objective of the Risk Management plan is to outline a strategy for identifying, assessing, and prioritizing potential risks that could affect a software development project. This document aims to assist project managers and team members in foreseeing, preventing, or mitigating any adverse impacts these risks may have on the project's schedule, budget, and overall success. Having a RMP enhances project planning and decision-making. In addition, it provides project visibility and tracking of issues. Finally, it decreases project costs through proactive risk mitigation

**Identification of risks and assessment**

Implementation during Sprint 1 involved the team effectively identifying and assessing potential risks through a combination of brainstorming sessions and a checklist-based approach. In these collaborative sessions, team members discussed and identified potential risks based on their individual knowledge and past experiences. These methods enabled the team to comprehensively identify and document potential risks that could impact the project during Sprint 1.

**Risk charts**

| Impact  Probability | Low | Medium | High |
| --- | --- | --- | --- |
| Low | 6, 21 | 3, 15, 20 | 12, 13, 19 |
| Medium |  | 1, 4, 5, 9, 14, 16 | 7, 8, 10, 13, 18 |
| High |  | 11, 17, 22 | 2, 10 |

**Table 1:** Risk management chart

**Criteria for Defining Impact and Probability Levels**

It is essential to establish precise criteria for the effect and likelihood levels of hazards that have been discovered in order to guarantee a consistent and impartial approach to risk assessment. With the help of these criteria, the project team may precisely assess and classify each risk, enabling the use of efficient risk management techniques.

**Impact Levels**

* High Impact:

Risks that, if they came to pass, would seriously disrupt the project and might result in large delays, large cost overruns, or a serious compromise of the project's goals. These hazards may need a thorough review of the project's timelines, money, and scope.

* Medium Impact:

Hazards that could cause a minor amount of disruption, which could lead to delays or extra expenses that are controllable within the project's backup plans. Although these risks might need alterations to the project plan, they do not pose a threat to the project's overall success.

* Low Impact:

Risks whose effects would be easily mitigated by the project's current contingencies and whose influence would be negligible. These risks don't have a major impact on the project's overall goals or deliverables, but they could lead to tiny delays or slight cost increases.

**Probability Levels**

* High Probability:

Hazards that, given the state of the project, past performance, or professional opinion, are highly likely to materialize. In order to reduce the possible effects of these hazards, timely attention and planning are needed.

* Medium Probability:

Risks with a reasonable chance of occurring. While not certain, these risks are plausible enough to warrant consideration and preparation in the project's risk management strategy.

* Low Probability:

Risks that are unlikely to occur, given the current understanding of the project environment and external factors. These risks are monitored but are considered low priority for immediate action.

**Decision-Making Criteria**

The determination of impact and probability levels for each identified risk involves a combination of quantitative analysis and qualitative judgment. The project team employs a systematic approach, incorporating the following:

* Historical Data: Analysis of similar projects or past phases within the current project to identify trends and outcomes related to specific risks.
* Expert Judgment: Input from team members, stakeholders, and external experts, drawing on their experience and understanding of the project's context.
* Project Specifics: Consideration of the unique aspects of the current project, including scope, resources, and external factors, that might influence the likelihood and impact of risks.

| **Risk ID** | **Risk Name** | **Risk Type & Description** | **Risk Score** | **Resolved in Sprint** | **Strategy & Effectiveness** |
| --- | --- | --- | --- | --- | --- |
| 1 | Change of Requirements | Requirements-related change may occur during the project lifecycle, impacting deliverables and timelines. | Medium | Sprint 1, 2, 3, 4 | Accept |
| 2 | Unclear Requirements | Lack of clarity in project requirements leading to misunderstanding and rework. | High | Sprint 1, 2, 3, 4 | Avoid |
| 3 | Mobile & Web compatibility | Compatibility issues between mobile and web platforms leading to usability and functionality issues. | Low | Sprint 2, 3, 4, 5 | Mitigate |
| 4 | Resource Restrictions | Insufficient resources (e.g., budget, team members) causing delays and quality compromises. | Medium | Sprint 1, 2, 3, 4 | Accept |
| 5 | Rapid Technology Changes | Rapid changes in technology trends impacting project delivery | Medium | Sprint 1, 2, 3, 4 | Accept |
| 6 | Change in the Leadership Role | Change in project leadership leading to disruption in decision-making and project direction. | Low | Sprint 1, 2, 3 | Accept |
| 7 | Lack of Proper Planning | Inadequate planning leading to missed deadlines, scope creep, and budget overruns. | High | Sprint 1 | Mitigate |
| 8 | Poor Documentation | Incomplete or inaccurate documentation leading to misunderstandings and rework. | High | Sprint 1 | Mitigate |
| 9 | Insufficient Training | Lack of training for team members leading to inefficiencies and errors. | Medium | Sprint 1 | Mitigate |
| 10 | Lack of Proper Testing | Inadequate testing leading to undetected defects and poor software quality. | High | Sprint 2, 3, 4 | Mitigate |
| 11 | Miscommunication & No Communication | Poor communication leading to misunderstandings, conflicts, and delays. | High | Sprint 1, 2, 3, 4, 5 | Mitigate |
| 12 | Lack of Familiarity with Technology | Limited knowledge and experience with technology stack leading to inefficiencies and errors. | Medium | Sprint 1 | Mitigate |
| 13 | Poor Risk Management | Ineffective identification, assessment, and mitigation of risks leading to project failures. | High | Sprint 1 | Mitigate |
| 14 | System Performance | System performance issues leading to user dissatisfaction and decreased productivity. | Low | Sprint 1, 2, 3, 4, 5 | Mitigate |
| 15 | Vulnerable Security | Vulnerabilities in system security leading to data breaches and loss of trust. | Medium | Sprint 4 | Transfer |
| 16 | External Dependencies | Dependencies on external factors leading to delays and project bottlenecks. | Medium | Sprint 1, 2, 3, 4, 5 | Accept |
| 17 | Escalation of Complexity | Project complexity leading to difficulties in understanding, implementation, and maintenance. | High | Sprint 1, 2, 3, 4, 5 | Avoid |
| 18 | Code Scalability | Inability of the system to handle increased workload leading to performance degradation. | High | Sprint 2, 3 | Transfer |
| 19 | Regulatory Law Compliance & Actions | Failure to comply with regulatory laws leading to legal actions and penalties. | Medium | Sprint 4 | Avoid |
| 20 | Poor Data from User Feedback | Receiving unreliable user feedback leading to unnecessary or useless feature adoptions. | Low | Sprint 2, 3, 4 | Mitigate |
| 21 | External and Unpredictable events | External events such as outages, internet service provider issues that can delay the progress of the project | Low | Sprint 2, 3, 4, 5 | Accept |
| 22 | Inadequate encryption key management | Failure to implement robust key management practices can lead to risks by using weak keys, failing to rotate keys regularly, storing keys insecurely, and inadequate protection measures for keys in memory. | High | Sprint 4 | Mitigate |
| 23 | Cyber-attacks | Cyber attacks, such as malware, ransomware, can lead to unauthorized access to the system, data breaches, loss of sensitive information, and significant disruption to operations. | High | Sprint 2, 3, 4, 5 | Mitigate |

**Table 2:** Risk management chart