**Risk Management Plan**

**<Project Name>**

**Company Name**

**Address**

**Date**

**Table of Contents**

[Introduction 3](#_Toc332278598)

[Top Three Risks 4](#_Toc332278599)

[Risk Management Approach 4](#_Toc332278600)

[Risk Identification 5](#_Toc332278601)

[Risk Qualification and Prioritization 6](#_Toc332278602)

[Risk Monitoring 6](#_Toc332278603)

[Risk Mitigation and Avoidance 7](#_Toc332278604)

# Introduction

The Barangay South Signal Village Web Application project aims to develop a web application for the Barangay South Signal Village residents that can access online services of the barangay including the online document request and submitting concerns. The web application’s primary goal is to provide information about the barangay and online service/s for their community more efficiently, effectively, and transparently.

In an agile project, the risk management plan is required to incorporate by the project team because it aims to aims to detect and evaluate possible risks, as well as develop risk response techniques, as well as risk monitoring and control throughout the project's life cycle. The strategy will be integrated into the daily operations of the project and evaluated and revised as needed.

The project team may guarantee that risks are mitigated, and the project's objectives are met within the budget and timetable by proactively managing risks.

The risk management plan will contain the possible project risks, the approach to managing risks, the process of identifying and evaluating risks, monitoring risks, implementing risk mitigation and avoidance measures, and maintaining a risk register. This management strategy will clearly define the methods for addressing risks and overseeing their progress. The effectiveness of the plan will be assessed based on how promptly risks are identified and resolved, and whether the project's goals are successfully met.

# Top Three Risks

The following are the risks for the Barangay South Signal Village Web-Application identified by the team. The project manager will choose and use the proper risk reduction and avoidance measures to reduce the likelihood of these hazards.

1. **External Security Threats** - External attacks may compromise the web application's security. Malicious assaults, hacking efforts, and unauthorized access to sensitive information are examples of such risks.
2. **Data Theft or Loss** - Data theft or loss is possible due to potential security breaches. Unauthorized access or security breaches in the web application might compromise or lose sensitive data, such as the residents' and barangay information needed for protection.
3. **Internet or Power Outages** - The project team is aware of the possibility of a work disruption due to internet or power disruptions. These interruptions may prevent the barangay employee and the resident from using the web application or managing online services.

# Risk Management Approach (Kins)

After identifying potential risks that the project team may encounter, the team will then proceed to discuss these risks with the project sponsor. The team will collaborate with the project sponsor on the ideal response that the team will implement. After the discussion and the implementation, the team will analyze the mitigation response and will apply improvements if deemed necessary.

# Risk Identification (Kins)

* Project Team Meeting
* Meeting with Project Sponsor
* Assessing Project Security
* Project Scope Checklist

# Risk Qualification and Prioritization (Cess)

Once risks are identified it is important to determine the probability and impact of each risk in order to allow the project manager to prioritize the risk avoidance and mitigation strategy. Risks which are more likely to occur and have a significant impact on the project will be the highest priority risks while those which are more unlikely or have a low impact will be a much lower priority. This is usually done with a probability – impact matrix. This section explains risks were qualified and prioritized for this project. For more information on how to qualify and prioritize risks refer to our ***Risk Assessment Meeting Guide.***

# Risk Monitoring (Dale)

The Risk Monitoring approach provides active management of risks throughout the project, it is important to maintain continuous monitoring throughout the project's life cycle and comprehensively record the process, including identifying conditions for risks.

According to the plan, the project manager will incorporate scoring risks into the project schedule and assign a dedicated risk manager to oversee their monitoring. This enables the project manager to specify when risks require immediate attention and when the risk manager should provide updates during the weekly team meetings.

During the team meetings, the risk manager will report on the status of identified risks, any new risks found, and the effectiveness of mitigation plans. Any new changes to the Risk Management Plan will be made with the project team.

Overall, the project team will implement an agile risk management methodology that emphasizes continuous progress and flexibility. The effectiveness of the risk management plan will be assessed and adjusted as needed. This ensures that the project passes the quality standards.

# Risk Mitigation and Avoidance (Rark)

When developing a web application, it is important to identify and mitigate potential risks to ensure the security, reliability, and performance of the application. Incorporating these risk mitigation and avoidance strategies into the web application development process, you can help minimize vulnerabilities, ensure a secure and reliable application, and mitigate potential risks throughout the lifecycle of the application.

1. **Security Risks**:

* The development team needs to implement secure coding practices to prevent common security risks and vulnerabilities.
* Team needs to regularly update and patch the software components, frameworks, and libraries to address security vulnerabilities.
* Use secure authentication and authorization mechanisms to protect the user accounts and sensitive data and information.
* Implement secure communication protocols like HTTPS to encrypt data transmitted between the server and the client in the web application.
* Conduct a penetration testing to identify and address potential vulnerabilities.

1. **Performance Risks**:

* Team needs to conduct performance testing to identify potential bottlenecks and optimize the application’s performance.
* Optimize the database queries and ensure efficient data retrieval and manipulation.
* Monitor and analyze the web application performance in production to identify and address different performance issues.

1. **Compliance Risks**:

* Understand and comply with relevant legal and industry-specific regulations.
* The development team needs to implement necessary security measures and data protection practices to meet compliance requirements.
* The team needs to regularly review, and update compliance practices based on changes in regulations.

1. **Scalability Risks:**

* The team needs to think and design the application with scalability, they need to consider several factors like load balancing, and database scalability.
* They need to regularly monitor application performance and scalability to identify and address scalability issues.

1. **Data loss and Data Breach Risks:**

* Implement a regular data backup and disaster recovery plan to prevent any data loss along the way.
* Encrypt all sensitive data
* Implement access controls and user permissions to restrict unauthorized access to sensitive data.

1. **Third-Party Risks**:

* The team needs to stay updated with security patches and updates provided by third-party vendors.
* Carefully assess the security practices of third-party libraries, frameworks, and services used in the application.
* Regularly review and update third-party components to mitigate potential risks.

**Risk Register** (Carl)

Every project must maintain a risk register in order to track risks and associated mitigation strategies. This section describes the risk register criteria as well as where the risk register is maintained and how these risks are tracked in the project schedule.

The risk register, which will be updated throughout the project, will include a detailed explanation of each risk, its likelihood and potential consequences, as well as any mitigation measures implemented. The risk register will be reviewed and updated on a regular basis to ensure that it accurately reflects the project's current state. The risk registry, which will be housed in a central location, will be accessible to all stakeholders.

This risk management strategy is generally consistent with the Agile methodology, emphasizing early and frequent risk discovery, collaborative risk management, and continual risk monitoring. Team Developmentality can mitigate the consequences of potential risks and increase the likelihood of project success by predicting and resolving them. Furthermore, using a cloud-based project management tool such as Jira, Asana, or Trello, the risk register for the Barangay South Signal Village Web App will be saved in a shared document. This tool will be used by the project team to manage and prioritize risks, allocate responsibilities, and monitor risk mitigation progress.

The following criteria will be used for the risk register:

* Risk ID - each risk will be assigned a unique identifier.
* Risk Description - there will be a clear and concise description of the risk event.
* Risk Category - will classify risks into technical, organizational, or legal categories.
* Risk Owner - will be responsible for monitoring and managing each risk.
* Probability - likelihood of a risk occurring is assessed using a scale of 1 to 5, with 1
* indicating the lowest likelihood and 5 indicating the highest.
* Impact - the risk's potential impact on the project is rated on a scale of 1 to 5, with 1
* indicating the least significant impact and 5 indicating the most significant impact.
* Risk Score - the probability and impact scores are multiplied to determine the overall risk
* score.
* Mitigation Strategy - outlines the specific measures to be taken to mitigate the risk.
* Status -risk's current status, whether it is open, in progress, or closed, is also documented.
* Target Resolution Date - anticipated date for risk resolution to be resolved.

Risk register:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Risk  ID | Risk  Rank | Risk | Description | Category | Destination/  Owner | Probability | Impact | Status |
| RID  001 | 1 | Technical Risks | The Barangay South Signal Village Web App may not work effectively with existing software and hardware systems, resulting in system faults and delays. | Technology | Project Leader | High | High | In Progress |
| RID  002 | 2 | Resource Risks | There is a risk of not having enough resources to execute the project on time, which could lead to delays and budget overruns. | Organizational | Project  Manager | Medium | Medium | In Progress |
| RID  003 | 2 | Security  Risks | Data breaches and cyberattacks pose a threat to sensitive information. | Technical | System  Developer | Medium | Medium | In Progress |

**Sponsor Acceptance**

Approved by the Project Sponsor:

Date:

<Project Sponsor>

<Project Sponsor Title>

# This free Project Risk Management Plan Template is brought to you by [www.ProjectManagementDocs.com](http://www.ProjectManagementDocs.com)