**Risk Management Plan**

Table of Contents

[1.1. Introduction 2](#_Toc138965576)

[1.2. Risk Management Approach 2](#_Toc138965577)

[1.3. Risk Identification 3](#_Toc138965578)

[1.4. Risk Qualification and Prioritization 4](#_Toc138965579)

[1.5 Risk Monitoring 6](#_Toc138965580)

[1.6. Risk Mitigation and Avoidance 6](#_Toc138965581)

[1.7. Risk Register 8](#_Toc138965582)

### 1.1. Introduction

RAMS Corner Ticketing System aims to modernize and introduce a more efficient and manageable workflow for the Information Technology Resource Office of Asia Pacific College by replacing their current email-based reporting system into a more organized ticketing system that addresses all inquiries or incidents that needs the ITRO expertise.

By following a hybrid model of project lifecycle, this risk management plan will follow specific steps that will be consolidated upon sprints. This includes identifying potential risks, developing quick risk response techniques, controlling, and monitoring the potential risks, that will help the entirety of project to adhere to the allotted time and budget, as well as to mitigate the risk whilst continuing to provide the solution aimed by the project.

This risk management plan will include the risk assessment, risk response, risk control, risk monitoring, while having all these details further reviewed and revised based on the recent technology advancements and how they will affect the execution of the application that will enable the team to mitigate, or minimize the risk involved in a ticketing system.

### 1.2. Risk Management Approach

This risk management plan will follow these steps:

* Risk Identification – this is the first, and most crucial step to be able to analyze the potential risks that will affect the deployment of RAMS Corner Ticketing System greatly. This can include technical problems, Staff problems, customer management problems, or the security problems.
* Risk Assessment – during this step, the prioritization of risk-handling will occur. After identifying the risk, they will be analyzed to see which is most likely to occur. In this sense, the focus of the allotted time and budget can be given to a risk with higher potential.
* Risk Analysis – after having put the risks in hierarchy, analysis of the possible root causes for these potential risks will undergo this process. This will help in assessing the possible impacts of certain risk factors and update the existing control measures or create a new plan.
* Risk Treatment – once the risks are analyzed one-by-one, an appropriate contingency plan will be created based on the risk factors.
* Risk Monitoring and Review – it is important to keep the risk under control, so the monitoring and review will help in further improving the risk mitigation strategies or the contingency plan based on the different circumstances
* Communication with the Team and the Stakeholders – regular reporting of progress in risk mitigation will be held so that each and every one of the team members as well as the stakeholders will be informed of what is going on within the system, and what to expect upon the existing risk mitigation procedures.
* Documentation – lastly is to document all the risk mitigation processes that the project has undergone. It is important to have historical data as a reference if the risk management plan adhered to the rules set to the project.

By following these steps, this will ensure that the RAMS Corner will run smoothly and efficiently, with less-to-no potential risk, and produce a satisfactory result for customer service that is one of the aims of the project.

### 1.3. Risk Identification

Top three Risk in RAMS Corner Ticketing Service System

After identifying the risk, they are categorized intro three major types, these are:

1. Vulnerabilities in System Security – as a ticketing system, this application will typically handle sensitive information of its customers such as their personal details. A weak authentication system may not be able to withstand data breaches, that will probably cause not only operational losses for the ITRO, but also reputational damage with its clients.
2. System Failure – since a ticketing system acts mainly as a customer support channel, it is very crucial for the RAMS Corner service to be up all the time, especially if it is within school hours. In the instances where the system is down, maybe due to some technical problems or external problems, the inability to cater to the client’s tickets will have a negative impact on the ITRO services as a whole.
3. Performance Issue – this is both true for the hardware and peopleware. A ticketing system is expected to handle a large volume of tickets, maybe not every day, but to a certain point in time. In that instance, it is possible to have performance issues both with the hardware that is being used (be it crashes, slow response time, etc.), and peopleware issues such as taking a long time resolving one ticket. If the ticketing system and its staff were not able to handle a surge of requests and incidents from their customers, there is the operational and reputational risk for the ITRO.

To be specific, here are the possible risks that are identified for the RAMS Corner:

1. Security Breaches – personal information that are stored and is being used in a ticketing system is at risk when there is weak security for the system.
2. Downtime – system downtime can greatly reduce the trust of the client to the ITRO because they will not be able to raise their concerns timely.
3. Inadequate Scalability and Elasticity – a ticketing system is expected to handle customer support efficiently. If the system is not scalable or elastic enough that it will not be able to handle the increase or decrease in the volume of tickets received daily, the system is bound to produce customer dissatisfaction.
4. Lack of Integration – since RAMS Corner will be adapted by the ITRO, it is expected to be able to integrate well with the current software and hardware equipment that is used by the ITRO, as well as the Asia Pacific College Residents being the clients. Inability to integrate means a decrease in productivity, that will therefore cause operational damage.

To mitigate these aforementioned risks, the team developed a contingency plan that will allow the ITRO to address these issues in a considerable amount of time. Training before deployment is also a necessary step to familiarize the staff with how they are going to navigate the system. A regular reporting of the progress in risk mitigation will also be held in one-week sprints so that the system can remain up to date to the growing risk potentials and the possible ways to minimize it.

### 1.4. Risk Qualification and Prioritization

After Identifying the risk for the RAMs Corner, we are able to categorize them based on how likely these risks will occur, and how much are its impact both on the ITRO and their client. We have come up with an impact-probability matrix that can help in prioritizing which type of risk needs a focused mitigation strategy.

In the matrix, the probability of risk occurring, and its impact is described as below:

* Extreme: these are the risks that pose highest level with highly likely to occur and has catastrophic impacts for the ITRO.
* High: these are the risks that pose substantial risk that can lead to disastrous outcomes.
* Medium: these are the risks that has a moderate likelihood of occurrence and can result to negative impacts within the ITRO
* Low: these are the risks that has a lower likelihood of occurrence, but there is still noticeable impact to the ITRO
* Negligible: these are the risks that are not likely to occur and have insignificant impact on the ITRO if it were to happen.

The table below depicts the matrix of impact-probability of the risk identified:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Risk Assessment – Impact-Probability Matrix** | | | | | |
| Impact | Insignificant | Minor | Significant | Disastrous | Catastrophic |
| Probability |
| High | **N** | **L** | **M** | **H** | **E** |
| Medium | **N** | **L** | **M** | **H** | **E** |
| Low | **N** | **N** | **L** | **M** | **H** |
| Very Low | **N** | **N** | **N** | **L** | **M** |

Table : Risk Assessment - Impact-Probability Matrix

The identified risks are prioritized as follows:

1. Lack of Integration – Medium probability with significant impact
2. Downtime – medium probability with disastrous impact
3. Inadequate Scalability and Elasticity – medium probability with disastrous impact
4. Security Breaches – medium probability with disastrous impact

After the assessment, we will focus on developing solutions for the risks that are considered in extreme and high priority. The risks on the low to medium priority will be constantly monitored as well, and there are no negligible risks since we firmly believe that all risks must be considered and should have a minimum possible solution whenever they occur.

This risk assessment is subject to revisions after reviews and monitoring. This process will happen during sprint meetings so that all the team members and the stakeholders are up to date with the current risk management plan should there be any changes to be made.

### 1.5 Risk Monitoring

Risk monitoring is a very important step in risk management of the RAMs Corner. It will allow the team, as well as the stakeholders, to be involved in the ongoing risk management process that could impact the achievement of the long-term goals of the project. This is also to ensure that the identified and assessed risks are being reviewed and monitored thoroughly so that the ITRO can make informed decisions to make timely actions in preventing or minimizing a risk potential.

In this step, the project manager and the development team will be the overseer for the risk management. They will be the one responsible for overseeing the ongoing risk mitigation process, continuously monitoring the system logs, security alerts, and performance metrics. They will also provide the team with reviews for user feedback, support ticket, bug reports, and implement Key Performance Indicators to measure how effective is the current risk mitigation.

They are expected to report on the status of ongoing risk management regularly in every sprint meeting. After the assessment from the report, the team will then collaborate for further reviews if there are risk mitigation plans that should be changed, should be added, or should be maintained.

To sum it all up, having an effective risk monitoring that incorporates the agile methodology, the ITRO can have an early risk detection, which will lead onto improved decision-making when dealing with potential risks, that can also therefore improve the operational efficiency of the system in servicing its clients, and continuous improvement of the system as a whole.

### 1.6. Risk Mitigation and Avoidance

As mentioned in the previous risk management plan sections, the risk mitigation will be based upon the identified risk and their prioritization as described in the hierarchy from the risk assessment. The risks labeled as Extreme will be given the highest priority when allocating resources, down until the risks labeled Low. This step will allow the team to have an overview of the suitable mitigation plan per assessed risks while continuing to improve, monitor, and review the overall health of the system.

The following are the available mitigation plan that is ongoing or to be implemented:

* Contingency Plan – It is important to develop contingency plans that outline the steps that should be taken should there be any security mishaps or some kind of operational disturbance within the system. To make sure that there is an effective contingency plan, the project manager will supervise all of the development and execution phase of the project.
* Regular Assessments and Audits – It is also absolutely crucial that there is a periodic review of the current plans. This will be attained by applying the Hybrid(Waterfall-Agile) Methodology, wherein the team must follow the specific steps in risk management while also submitting reports regarding monitoring and reviewing of currently implemented actions every sprint meeting.
* Implement robust access controls – while the users are already defined for the RAMS Corner, it is still imperative to have a definite access control to ensure that there would be no unauthorized access to the ticketing system. This will include user authentication, requiring using strong passwords, role-based access controls, and periodic access reviews by the assigned ITRO Staff.
* System Backups – consistency in backing up the RAMS Corner data must be implemented to ensure that there will be no information and data loss in an event of system failure, data corruption, and some unforeseen circumstances should occur. Reviewing the restoration process and verifying integrity of the back-up data must also be included in the regular assessments.
* Employee Training – provide a detailed training plan for the employees regarding the use and management of the RAMS Corner Ticketing Service System so that the staffs are educated on the proper handling of tickets, as well as providing them the details for the risk mitigation should there be any threats occur within the system or when using the system.
* Regular Communication – while all other technical aspects are important, communication within the team is also important to ensure that every stakeholder is informed regarding the ongoing plans, especially when tackling about the risk that the system is facing. This is to make sure that no resources are lost while still maintaining the efficacy of the system.
* Change Management Plan – there must be a distinct change management plan for when there are any changes that need to be made to the system. It is important to document and gain the approval of every stakeholder when applying changes within the project. This will allow the team to handle potential risks without creating any ambivalence within the project stakeholders’ ideas.

### 1.7. Risk Register

In the risk register section, the risk management plan that will be intended for the top categories of identified risks will be constantly revised throughout the project. This will include all necessary details such as the probability of these risks occurring, their impacts, and the mitigation and avoidance procedures.

The risk registry will be available for viewing for all the stakeholders to make sure that there is transparency when it comes to risk management. This file will be kept in a shared location where all the stakeholders can access it.

The aim for this risk register is to allow the stakeholders, especially the team, to have an overview of the history of risk management planning for comparison and improvement basis, as well as the ongoing measures taken for risk mitigation. In this way, the RAMS Corner project team will be able to manage the potential risks in a timely and efficient manner.

The following are the list of elements in the Risk Register

* Risk ID – each risk identified will have their own unique identifier
* Risk Description – brief and concise description of the identified risk
* Risk Category – classify the type of risk as Vulnerability in Security, System Failure, and Performance Issues
* Risk Owner – project team member that is responsible for monitoring and reviewing current potential risks
* Probability – probability of risk occurrence scaling from 1 – 4, 1 indicating Very Low Probability and 5 indicating High probability
* Impact – impact of the potential risk scaling from 1-5, 1 having Insignificant impact, and 5 having the Catastrophic impact
* Risk Score – product of probability and impact score
* Mitigation Procedure – specific measures intended for the listed potential risk
* Status – historical status of the risk. It can be Open, Ongoing, or Closed.
* Target Resolution Date – date for the resolution of the listed risk.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Risk ID | Risk Description | Risk Category | Risk Owner | Probability | Impact | Risk Score | Status | Target Resolution Date |
| RID 001 | **Security Breaches** - personal information can be compromised when there is weak security for the system. | Vulnerability in Security | Developer Team | 3 | 5 | 15 | Closed | 12/2022-03/2023 |
| RID 002 | **System Downtime** - inability to raise and resolve tickets in a timely manner | System Failure | Developer Team, Project Manager | 3 | 4 | 12 | Open | 03/2023-06/2023 |
| RID 003 | **Inadequate Scalability and Elasticity** –unscalable or inelastic system will not be able to handle the increase or decrease in the volume of tickets received daily | System Failure | Project Manager | 3 | 5 | 15 | Open | 07/23-09/23 |
| RID 004 | **Lack of Integration** –Inability to integrate means a decrease in productivity, that will therefore cause operational damage. | System Failure | Developer Team | 3 | 3 | 9 | Open | 06/23-08/23 |