

RISK MANAGEMENT PLAN
SURVEIRAMS

ASIA PACIFIC COLLEGE
3 HUMABON PLACE, MAGALLANES
MAKATI CITY, 1232 METRO MANILA

APRIL 2023

TABLE OF CONTENTS

6.9. Risk Management Plan	1
6.9.1 Introduction	3
6.9.1 Top Three Risks	4
6.9.2 Risk Management Approach	4
6.9.3 Risk Identification	5
6.9.4 Risk Qualification and Prioritization	5
6.9.5 Risk Mitigation and Avoidance	6
6.9.6 Risk Monitoring	7
Sponsor Acceptance	8

Introduction

SurveiRams is a mobile application designed to develop a centralized system for Asia Pacific College's (APC) Information Technology Resources Office (ITRO), Management Office (BMO), and Security Office. The application will assist them in managing incident reports and logs as well as provide insights.

The Risk Management Plan is important for projects following the Agile Methodology to use as a guide on how to identify and respond to risks. The team must enumerate potential risks, plan for responses, and monitor and control said risks from the project's start to finish. Upon completion, the plan will be used every day, and may be revised to fit the project's needs better, thus ensuring that the objectives of the project are achieved on time within budget.

Contents of this document include a summary of the risk management process, describing the sequence of steps as well as who is assigned to do so. Next is a guide for what constitutes as a risk and their hierarchy. Followed by this is the monitoring and controlling process for the risks, and last is the risk register.

To further develop a risk management plan for the SurveiRams System, the following information should be considered:

Top Three Risks

Every project has risks whether foreseen or not. However, in the situation of the SurveiRams project, the three biggest foreseen risks are the following:

1. **Technical Risks** – Risks that are brought by evolving technology, such as failure from either or both software and hardware and cyberattacks resulting in data loss and/or security breaches.
2. **Insufficient Resources** – Risks that are brought by the lack of project resources such as exceeding the project timeline or going over budget, which may delay the completion.
3. **Human Error** – Risks that are brought by the unavoidable mistakes made by humans involved in the project such as the project team, stakeholders, and personnel.

Risk Management Approach

Agile risk management values lean thinking and efficient communication. This means that for the SurveiRams risk management strategy, the focus will be data gathering and analysis before deciding on a course of action. Stakeholders, sponsors, and the project team must cooperate with each other for the risk management approach.

Specifically, these are the steps to be followed:

- **Risk Identification:** Meetings will be held to discuss relevant risks encountered based on experience from other projects, and a Risk Register will be put together.
- **Risk Assessment:** A Risk Assessment Matrix will be constructed to rank the risks discussed based on the probability of their occurrence as well as the gravity of its impact on the project.
- **Risk Mitigation:** Mitigation plans will be made for the risks that have a high probability and extreme gravity, which include how to prevent them and minimize their impact.
- **Risk Monitoring:** There might be unforeseen risks that could arise. To be ready to minimize or eliminate them, there will be a bi-monthly examination of the Risk Register, as well as another round of brainstorming for possible risks that haven't been discussed. New risks discovered will be added to the Risk Register.

- **Risk Communication:** All stakeholders must regularly keep contact to be informed about the occurrences of risks and how they are handled. They must also be updated regarding changes in the risk management plan and process.

Risk Identification

After a thorough discussion with the project team, risks to SurveiRams were identified. The team organized these risks into the following categories:

- **Technical:** Risks related to technology
- **Cost:** Risks related to the project budget
- **Schedule:** Risks related to the project timeline
- **Communication:** Risks related to communication among all stakeholders
- **Skills Resource:** Risks related to the project team's skills and expertise
- **External Hazard:** Risks related to nature, society, and the government

These are all the possible types of risks that could affect the project. Updates will be made in the event that another type is discovered. Specific risks under some of these categories will be discussed in the Risk Register below.

Risk Qualification and Prioritization

A Risk Assessment Matrix based on probability and impact was created to aid in ranking the risks in the Risk Register.

Table 1. Risk Assessment Matrix

		Probability Level		
Impact Level		1	2	3
	1	Low	Low	Medium
	2	Low	Medium	High
	3	Medium	High	High

As shown in Table 1, there are three levels each for the probability and impact of a risk. The lowest level is 1 and the highest is 3. The assessments are the following:

- Low – These are risks with low impact and low probability. Risks assessed as low are negligible and are low priority.

- Medium – These are risks with medium impact and probability. Risks assessed as medium must have mitigation plans at least drafted, and these are medium priority.
- High – These are risks with high impact and probability. Risks assessed as high must have finalized and strong mitigation plans ready and studied by the project team, as these are of high priority.

Risk Mitigation and Avoidance

A Risk Register was made for the project team to have a centralized guide to refer to upon encountering risks. This will be disseminated to all the stakeholders for easy access, so they can be prepared with their tasks and responsibilities when the time comes. Although there are numerous risks that could possibly happen, only the five most likely ones to occur for the SurveiRams project are listed below.

Table 2. Risk Register

Risk ID	Risk Category	Risk Description	Risk Assessment	Owner	Mitigating/Avoiding Action
01	Technical	Data loss	High	Developers	Create backups for the data such as exporting the database contents into a document
02	Technical	System Bugs	Medium	Developers	Revisit and debug source code
03	Technical	Power Failure	Medium	Project Manager	Activate backup electricity generators
04	Technical	Unstable Internet Connection	Medium	Project Manager	Buy load to use mobile data
05	Cost	The project goes over budget	Low	Project Manager	Request for additional budget from Project Sponsors

Table 2, the Risk Register, shows the following information that are needed for managing the risks identified:

1. **Risk ID** – The unique identifier assigned to each risk.

2. **Risk Category** – Each risk is labelled based on the categories listed in Risk Identification it falls under.
3. **Risk Description** – The explanation of what the risk is and its effects.
4. **Risk Assessment** – The assessment of the risk based on the Risk Assessment Matrix.
5. **Owner** – The person/s responsible for taking action for each risk.
6. **Mitigating/Avoiding Action** – Indicates the steps needed to be done by the Owner to mitigate or avoid the risk. Risks assessed as low will have Avoiding Actions, while those assessed as high will have mitigating actions.

When a risk occurs, the Owner must inform all stakeholders between 24-48 hours depending on its impact. Next, they must send a Risk Mitigation Request Form (found in Appendix A) to the Project Sponsors containing the Risk ID, incident, cause, their plan to mitigate the risk, and request for the resources they need to do so. The Project Sponsors shall review the report and approve or provide the requested resources so that the Owner may proceed in mitigating the risk.

In case the system is down due to any risk except when there is no internet connection, the contingency plan is to use Microsoft Forms. The security guards may log their incident reports there instead of going back to manually writing in their log books. When the system is running again, the team can simply download the form's responses and add it to the database. Another option is to input the details in the application.

Risk Monitoring

Risk Management does not stop after mitigating the identified risks. They must be monitored continuously until the end of the project. After the risk's Owner deals with the risk, they must inform all stakeholders of the risk's status and submit a formal incident report to the Project Manager detailing the steps they took to solve the problems the risk caused. The Risk Incident Report format can be found in Appendix B.

Weekly meetings must be held by the project team to review the Risk Register, to ensure that the mitigating/avoiding actions are still effective. Stakeholders must be informed should an update be made for the Risk Register. These meetings must also include review of past risks that occurred to make sure the probability of their future occurrence is lower, identify what might cause this risk to repeat, and create a plan to avoid this.

To conclude, risks must be identified, assessed, mitigated or avoided, and monitored, with all of the stakeholders maintaining open communication. This is to ensure that the Risk Management Plan remains effective and up to date. Having this in this project will lead to an output that not only meets the objectives, but is of high quality.

SPONSOR ACCEPTANCE

Approved by the Project Sponsors:

Date: June 2023

Mr. Jojo F. Castillo

Executive Director, Technical Services

Mr. Jose Manuel V. Garcia

Campus Architect

Appendices

Appendix A: Risk Mitigation Request Form

Risk Details:

Owner	
Risk ID	
Incident Description	
Cause	
Mitigation Plan	

Resource Request Details:

Item	Quantity	Cost

TOTAL	
-------	--

Appendix B: Risk Incident Report Template

Owner	
Risk ID	
Actions Taken	
Budget Used	
Status	