<ENTERPRISE RESOURCE PLANNING>

RISK MANAGEMENT PLAN

Version *<1.0>*
<02/03/2021>
Team 2

VERSION HISTORY

*[Provide information on how the development and distribution of the **Risk Management Plan** up to the final point of approval was controlled and tracked. Use the table below to provide the version number, the author implementing the version, the date of the version, the name of the person approving the version, the date that particular version was approved, and a brief description of the reason for creating the revised version.]*

Version #	Implemented By	Revision Date	Approved By	Approval Date	Reason
1.0	*<Yasaman Fahm, Vithura Muthiah, Neerujah Ledchumanan, Stella Ngyuen>*	*<01/29/21>*	*<Carlin Lee>*	*<02/03/21>*	Initial Risk Management Plan draft
1.1					

UP Template Version: 11/30/06

TABLE OF CONTENTS

1 INTRODUCTION

1.1 PURPOSE OF THE RISK MANAGEMENT PLAN

A risk is an event or condition that, if it occurs, could have a positive or negative effect on a project's objectives. Risk Management is the process of identifying, assessing, responding to, monitoring, and reporting risks. This Risk Management Plan defines how risks associated with the Enterprise Resource Planning system will be identified, analyzed, and managed. It outlines how risk management activities will be performed, recorded, and monitored throughout the lifecycle of the project and provides templates and practices for recording and prioritizing risks.

The Risk Management Plan is created by the project manager in the Planning Phase of the CDC Unified Process and is monitored and updated throughout the project.
The intended audience of this document is the project team and product owner.

2 RISK MANAGEMENT PROCEDURE

2.1 PROCESS

The project manager working with the project team and sponsors will ensure that risks are actively identified, analyzed, and managed throughout the life of the project. In addition to identifying and planning for potential risks, the ability to act upon a risk as early as possible minimizes the impact it has on the project. The goal of this section is to elaborate on the benefits of risk management. The project manager and the front-end development team will take on the role of Risk Manager as a unit. Risk identification and risk analysis are processes that need constant reassessment for each sprint.

Risk assessment consists of risk identification, risk analysis and risk planning. First step in the process of risk assessment is risk identification. Three main categories of risk will be taken into consideration for this project: technical risks, management risks and operational risks. To do so, the team will be using different techniques as mentioned in section 2.2. The second step in the process is risk analysis where the likelihood of occurrence and the level of impact will be analyzed. Impact matrix will be used for qualitative analysis, and risk exposure will be used for quantitative analysis. Last step in risk assessment is risk prioritization which will be done by ranking the risk exposures.

Risk control consists of risk planning, resolution and risk monitoring. Risk responses strategies include acceptance, avoidance, transference and mitigation. Each identified risk will be associated with an appropriate strategy. Acceptance is when the project manager has decided to not modify the project plan to deal with a risk or cannot identify a suitable response strategy. Avoidance is defined as changing the project plan to eliminate the risk. Transference involves shifting the consequence of a risk to a third party. Mitigation involves identifying ways to reduce the probability or the impact of the risk.

2.2 RISK IDENTIFICATION

Risk identification will involve the project team and will include an evaluation of environmental factors, organizational culture and the project management plan including the project scope. A Risk Management Log will be generated and updated as needed and will be stored electronically in the project library.

The techniques used for risk identification are brainstorm meetings and SWOT analysis. Brainstorm meetings consist of project team members meetings where they generate ideas that can be developed into potential risks. SWOT analysis is a technique that separates strengths, weaknesses, opportunities and threats of the project.

During the brainstorming process, the team has identified the main categories of risks:

1. **Technical Risks:**
   - 1.1. Developing the wrong requirements of the software
   - 1.2. Complexity of product implementation
   - 1.3. Change in requirements
   - 1.4. Unexpected change of project scope
   - 1.5. Poor quality code
   - 1.6. Entire team not familiar with the technology used
   - 1.7. Protection of user data
2. **Management Risks:**
   - 2.1. Time distribution
   - 2.2. Poor time estimation
   - 2.3. Time not properly allocated to specific functionalities
   - 2.4. Communication within team members and product owner
3. **Operational Risks:**
   - 3.1. No proper resource planning
   - 3.2. Poor productivity

A SWOT analysis was also done by the team as shown in the table below.

S STRENGTHS	W WEAKNESSES	O OPPORTUNITIES	T THREATS
Backend lead and frontend lead had prior knowledge of Spring and React.	Learning curve for the new technologies for some team members.	Developing new strategies	Change in technology
	Students not fully understanding the ERP system	Constant control on workflow data	Security

Table 1: SWOT analysis

2.3 RISK ANALYSIS

All risks identified will be assessed to identify the range of possible project outcomes. Qualification will be used to determine which risks are the top risks to pursue and respond to and which risks can be ignored.

Risk analysis' purpose is to measure the importance of the risks. In other words, this is the step where the identified risks are evaluated to examine the outcomes and goals that may change due the impact of a risk. The risks are then analysed to see if they have a qualitative or quantitative impact on the project. This process helps in evaluating which risks are serious, and possibly volatile, for the project. In addition, the risk manager must give a quantitative assessment, numerical value, for each risk using the researched data. The qualitative techniques that will be used for the risk analysis and risk probability and impact matrix.

2.3.1 Qualitative Risk Analysis

An impact matrix is based on probability and impact and it will show the hierarchy of different risks. In order to complete the analysis, it is important to define the scale of each risk for the probability and impact. In fact, if the probability and impact of a risk are unknown, it is difficult to determine the importance of the risk.

In this case, anything above 5% of the estimated cost and allocated time will be considered to have a very significant impact as shown in Table 1.

		Impact		
Scale	**Probability**	**Time**	**Cost**	**Quality**
Very High	> 90 %	> 5 %	> 5 %	Very significant impact on overall functionality
High	70%-89%	4-5%	4-5%	Significant impact on overall functionality
Medium	50%-69%	2-4%	2-4%	Moderate impact in key functional areas
Low	20%-49%	1-2%	1-2%	Minor impact on overall functionality
Very Low	1%19%	0-1%	0-1%	Very minor impact on overall functionality

Table 2: Scale of Risk of the ERP system

Probability	**Threats**				
Very likely to occur 0.90	0.045	0.09	0.18	0.36	0.72
Likely to occur 0.70	0.035	0.07	0.14	0.28	0.56

50% chance of occuring 0.50	0.025	0.05	0.1	0.20	0.40
Unlikely to occur 0.25	0.0125	0.025	0.05	0.10	0.20
Very unlikely to occur 0.10	0.005	0.01	0.02	0.04	0.08
	0.05	**0.10**	**0.20**	**0.40**	**0.70**
	Very Low	**Low**	**Medium**	**High**	**Very High**

Table 3: Risk Probability and Impact Matrix

2.3.2 Quantitative Risk Analysis

Risk exposure is determined by multiplying risk probability with the impact of a risk. The following table shows the risk exposure of each category.

Risk Categories		**Probability**	**Impact**	**Risk Exposure**
Technical Risks	Developing the wrong requirements	Unlikely	Very high	**0.20**
	Complexity of product implementation	Likely	High	**0.28**
	Poor quality code	Likely	High	**0.28**
	Protection of user data	Likely	High	**0.28**
	Entire team not familiar with the technology used.	50% chance of occuring	High	**0.20**
	Continuous change in requirements	50% chance of occuring	High	**0.20**

Management Risks	Unexpected change of project scope	Unlikely	Low	**0.025**
	Time not properly allocated to specific functionalities	Likely	High	**0.28**
	Communication within team members and product owner	Likely	Medium	**0.14**
Operational Risks	Responsibilities not resolved properly	Unlikely	Medium	**0.05**

Table 4: Risk Exposure for each Category

2.3.3 RISK RESPONSE PLANNING

For each major risk, one of the following approaches will be selected to address it:
Mitigate – Identify ways to reduce the probability or the impact of the risk
Accept – Nothing will be done
Transfer – Make another party responsible for the risk (buy insurance, outsourcing, etc.)

For each risk that will be identified, the project team will identify ways to prevent the risk from occurring or reduce its impact or probability of occurring as shown in the table below.

Risk Response Strategy	Risk Item	Risk Response Planning
Mitigate	Developing the wrong requirements	Hold frequent meetings to ensure the team is on the right track. Go over the requirements after developing each functionality. Quality assurance ensuring the implemented functionality satisfies the use-case.
	Poor quality code	Code review. Use specific coding standards. that the entire team agrees on. Testing.

	Unexpected change of project scope	More frequent meetings with the Product Owner to ensure the project scope hasn't changed.
	Protection of user data	The data is hosted on AWS and currently allows all traffic, and anyone can wipe the entire database. This can be restricted to certain IPs. The database IDs are sequential, and the data can be retrieved by just incrementing the IDs. Instead of sequential IDs, an algorithm can be used to generate unique IDs like UUID.
	Entire team not familiar with the technology used	The lead of backend and frontend each stream while they are coding. This will allow the ones not familiar with the technology to get used to it and learn.
	Continuous change in requirements	Double checking the requirements with the product owner before the start of each new sprint. More frequent meetings to discuss the change in requirements with the product owner to communicate and set more realistic expectations.
	Communication within team members (between backend and frontend) and product owner	Frequent short meetings between frontend team and backend team separately to discuss potential problems. Host sprint planning sessions.
Transference	Complexity of product implementation	Use languages and frameworks that the majority of the team is familiar with.
Acceptance	Time not properly allocated to specific functionalities	Set deadlines within the team for each functionality before the meeting with the Product Owner.

	Responsibilities not resolved properly	Document responsibilities of each team member for every sprint.

Table 5: Risk Response Planning for every Identified Risk

2.4 RISK MONITORING, CONTROLLING, AND REPORTING

The level of risk on a project will be tracked, monitored and reported throughout the project lifecycle. A "Top 10 Risk List" will be maintained by the individuals assigned to the risk manager role and will be reported as a component of the project status reporting process for this project. All project change requests will be analyzed for their possible impact to the project risks.

The document analysis technique will be used for risk monitoring, controlling and reporting. A table will be presented in the documentation which will categorize the elements needed to evaluate the risk in an appropriate manner. Every row will identify the risks' name, description, assessment and priority level. Management department will be notified of important changes to risk status as a component to the Executive Project Status Report.

TOP 10 RISK LIST

1.	Complexity of product implementation
2.	Poor quality code
3.	Protection of user data
4.	Time not properly allocated to specific functionalities
5.	Developing the wrong requirements
6.	Continuous change in requirements
7.	Entire team not familiar with the technology used
8.	Communication within team members (frontend and backend) and product owner
9.	Responsibilities not resolved properly
10.	Unexpected change of project scope

3 TOOLS AND PRACTICES

A Risk Log will be maintained by the project manager and will be reviewed as a standing agenda item for project team meetings.

RISK MANAGEMENT PLAN APPROVAL

The undersigned acknowledge they have reviewed the **Risk Management Plan** for the <Enterprise Resource Planning> project. Changes to this Risk Management Plan will be coordinated with and approved by the undersigned or their designated representatives.

Signature:	MN	Date:	2021/01/25
Print Name:	Muhamad Zubair Nurie		
Title:	Back-end Team Leader		
Role:	monitors back-end team		

Signature:	SN	Date:	2021/01/25
Print Name:	Stella Nguyen		
Title:	Front-end Team Leader		
Role:	monitors front-end team		

Signature:	AS	Date:	2021/02/01
Print Name:	Ayman Shehri		
Title:	Back-end Developer		
Role:	Participate in the entire application lifecycle, focusing on coding and debugging		

Signature:	NL	Date:	2021/01/25
Print Name:	Neerujah Ledchumanan		
Title:	Project Manager		
Role:	plan, control, monitor project		

APPENDIX A: REFERENCES

The following table summarizes the documents referenced in this document.

Document Name and Version	Description	Location
Lecture Notes of Dr. Rodrigo Morales on Risk management	Notes explaining different aspects of Project risk management.	*<https://moodle.concordia.ca/moodle/course/view.php?id=129693>*

APPENDIX B: KEY TERMS

The following table provides definitions for terms relevant to the Risk Management Plan.

Term	Definition
Project manager	Plays the role in planning, monitoring and controlling the project.
Product owner	Project's key stakeholder.
Impact matrix	Visual representation of results from risk probability and impact assessments.
Sprint	3 week period to complete a specific amount of work.
ERP	Enterprise resource planning
SWOT	strength, weakness, opportunities, threats
Jira	Software to plan, track and manage software development projects.