NTUCOLLAB

RISK MANAGEMENT PLAN

Version 2.1

03/06/2021

Team Eagles

Dandapath Soham – Project Manager, Back-end Developer

Gupta Jay – Lead Developer, Release Engineer

Kanodia Ritwik – Front-end Developer, Release Engineer

Mundhra Divyesh – Front-end Lead Developer

Bhatia Ritik – Back-end Lead Developer

Somani Palak – QA Manager, QA Engineer

Bansal Aditya – QA Engineer

School of Computer Science & Engineering
Nanyang Technological University, Singapore

VERSION HISTORY

Version #	Implemented By	Revision Date	Approved By	Approval Date	Reason
1.0	Somani Palak	02/23/21	Soham Dandapath	02/24/21	Initial Risk Management Plan draft
1.1	Bansal Aditya	02/25/21	Somani Palak	02/27/21	Add Qualitative & Quantitative Risk Analysis
1.2	Somani Palak	02/26/21	Dandapath Soham	02/27/21	Add additional requirement changes and estimation risks
1.3	Somani Palak	02/28/21	Dandapath Soham	02/28/21	Revise risk monitoring practices and methods
2.0	Bansal Aditya	03/01/21	Somani Palak	03/04/21	Add additional Risk Response Planning Matrix & Table
2.1	Bansal Aditya	03/06/21	Dandapath Soham	03/10/21	Final Draft and Complete Risk Management Plan

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. These threats, or risks, could stem from a wide variety of sources, including financial uncertainty, legal liabilities, strategic management errors, accidents, and natural disasters. Every business and organization faces the risk of unexpected, harmful events that can cost the company money or cause it to permanently close. Risk management allows organizations to attempt to prepare for the unexpected by minimizing risks and extra costs before they happen. By implementing a risk management plan and considering the various potential risks or events before they occur, an organization can save money and protect their future. This is because a robust risk management plan will help a company establish procedures to avoid potential threats, minimize their impact should they occur and cope with the results. This ability to understand and control risk enables organizations to be more confident in their business decisions.

Below are a few of the benefits of having a risk management plan:

- Creates a safe and secure work environment for all staff and customers.

- Provides protection from events that are detrimental to both the company and the environment.

- Increases the stability of business operations while also decreasing legal liability.

- Helps establish the organization's insurance needs in order to save on unnecessary premiums.

- Protects all involved people and assets from potential harm.

Below are few of the main classifications of risks which can affect a software project:

1.1.1   Project risks

Project risks concern differ forms of budgetary, schedule, personnel, resource, and customer-related problems. A vital project risk is schedule slippage. Since the software is intangible, it is very tough to monitor and control a software project. It is very tough to control something which cannot be identified.

1.1.2   Technical risks

Technical risks concern potential method, implementation, interfacing, testing, and maintenance issue. It also consists of an ambiguous specification, incomplete specification, changing specification, technical uncertainty, and technical obsolescence. Most technical risks appear due to the development team's insufficient knowledge about the project.

1.1.3   Business risks

This type of risks refers to the risks of building an excellent product that no one need, losing budgetary or personnel commitments, etc.

1.1.4   People risks

Risks that are connected with the person in the development team.

1.1.5   Estimation risks

These risks include risks that assume from the management estimates of the resources required to build the system.

1.1.6   Requirement risks

These are risks that arise from the changes to the customer requirement and the process of managing the requirements change.

1.1.7   Tools risks

These are risks that arise from the software tools and other support software used to create the system.

When a risk occurs, the corresponding mitigation response should be taken from the risk management plan.
Mitigating options include the following:

- **Accept**

  Acknowledge that a risk is impacting the project. Make an explicit decision to accept the risk without any changes to the project. Project manager approval is mandatory here.

- **Avoid**

  Adjust project scope, schedule, or constraints to minimize the effects of the risk.

- **Control**

  Take action to minimize the impact or reduce the intensification of the risk.

- **Transfer**

  Implement an organizational shift in accountability, responsibility, or authority to other members that will accept the risk.

- **Continue Monitoring**

  Often suitable for low-impact risks, monitor the project environment for potentially increasing impact of the risk.

This Risk Management Plan defines how risks associated with the NTUCollab project 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, project sponsor and management.

2   RISK MANAGEMENT PROCEDURE

2.1   PROCESS

The project manager working with the project team and project sponsors will ensure that risks are actively identified, analyzed, and managed throughout the life of the project. Risks will be identified as early as possible in the project so as to minimize their impact. The steps for accomplishing this are outlined in the following sections. The project manager will serve as the Risk Manager for this project.

The team plans to take the below mentioned steps to manage risk:

2.1.1   Risk Identification

The first step is to identify the risks that the project is exposed to in its operating environment. There are many different types of risks – legal risks, environmental risks, market risks, regulatory risks, and much more. It is important to identify as many of these risk factors as possible. We plan on noting down these risks manually for our project.

2.1.2   Risk Analysis

Once a risk has been identified it needs to be analyzed. We plan to determine the scope of the risk in this stage of the process. It is also important to understand the link between the risk and different factors within the organization. The number of business functions affected by the risk will determine the severity and seriousness of the risk.

There are risks that can bring the whole project to a standstill if actualized, while there are risks that will only be minor inconveniences in the analysis.

2.1.3   Risk Planning, Evaluation & Ranking

Risks need to be ranked and prioritized in any project. A risk that may cause some inconvenience is rated low; risks that can result in catastrophic loss are rated the highest. It is important to rank risks because it allows the members to gain a holistic view of the risk exposure of the whole project. The project may be vulnerable to several low-level risks, but it may not require intervention by all the members within the team. On the other hand, just one of the highest-rated risks is enough to require immediate intervention.

2.1.4   Risk Treatment

Every risk needs to be eliminated or contained as much as possible. The discussion regarding the risk and its possible solution is discussed with each member within the group. Instead of everyone contacting each other to get updates, everyone can get updates directly from MS Teams.

2.1.5   Risk Monitoring and Review

Not all risks can be eliminated – some risks are always present. For our project, monitoring happens under the supervision of the project manager. The project manager makes sure that he keeps a close watch on all risk factors. Monitoring risks also allows the project to ensure continuity and timely delivery.

To conclude, we have identified three main stages for developing risk approaches for software performance improvement, including initial stage, iterating stage, and closing stage.

Initializing stage

In the initial stage, project members assess the problem situation based on the area of concern such as users with negative attitudes, system requirements not adequately identified, project involved the use of new technology, lack of an effective project management methodology, team members lack specialized skills required by the project, employee's turnover, organization undergoing restructuring during the project. Goals of risk management is another factor should be considered when assessing the problem situation. After evaluating the problem situation, project manager and other team members will select a risk approach based on existing risk documents.

Iterating stage

In this stage, it is a continuous process including a repeating set of activities. The first iteration is to develop a risk framework. For instance, we select risk list approach. We then identify the risk items in it, and also think about how to avoid, mitigate, or transfer this risk items. The second iteration is to design the risk process. This iteration includes reformulating risk items and introducing a first step in which the software development team should interpret the risk model in their particular context. The third iteration is to apply the risk approach based on the first two iterations and the lessons learned from first two iterations. The iteration step in this stage is to evaluate experience and then the risk approach was used again without any changes (Iversen et al., 2004). The core of iterating stage is communication between different project members. Through the communication, software development team and project managers can get feedbacks and can in turn improve and refine risk management approach.

Closing stage

Two situations can exit software risk management cycle. One is that software development project is finished. The other one is that software development project is stopped in the middle way. Both of the two situations can provide valuable experience to software risk management. In this stage, we need update the risk management documents either from successful experience or failed experience which can help the team better manage software risk management in the future.

2.2   RISK IDENTIFICATION

Risk identification will involve the project team, appropriate stakeholders, and will include an evaluation of environmental factors, organizational culture and the project management plan including the project scope. Careful attention will be given to the project deliverables, assumptions, constraints, WBS, cost/effort estimates, resource plan, and other key project documents.

A Risk Management Log will be generated and updated as needed and will be stored electronically in the project library located in the project's MediaWiki.

The risk management log will include the following information:

1. Risk ID
2. Risk Type
3. Risk Description
4. Risk probability/Impact/Score
5. Assigned Personnel to deal with the risk
6. Risk mitigation strategy

The risks can be broadly classified into the categories of Technology, People, Organizational, Tools, and Requirements risks

Area of Risks	Details of Risks
Technology	1. The scraper assumes that the data provided from the Stars Planner has a particular structure. Drastic changes in this structure would cause the scraper to not work as per intended 2. The database used in the system cannot process as many transactions per second as expected 3. Server crashes and essential data is lost 4. Google Login API malfunctions 5. Reused software components might have bugs and defects which may break the code

People	1. The developers are occupied with multiple projects at the same time and may be unavailable to attend possible meetings 2. Conflicts between the developers and project manager 3. As the project duration is short, a team member falling ill and needing some time off would drastically delay project milestones 4. Undermined motivation within the team members and developers 5. Inadequate domain knowledge within developers
Organizational	1. The course project might be revamped with different components 2. The project management might be restructured with different people responsible for the different parts
Tools	1. The code generated by mobile SDK might be inefficient for actual deployment 2. The use of Firebase for data storage might be insufficient for the user data 3. The deployment servers might not be scalable enough to meet the demands of peak user traffic
Requirement Changes	1. Changes in requirements are proposed to improve the quality of the software at late stage of development 2. New use cases arise at late stage of development, giving rise to new requirements to be incorporated 3. Customers fail to understand the impact of requirement changes

Estimation	1. The time required to develop the various components of the software is underestimated 2. Abandoning of planning under pressure 3. The rate of bugs and issues in the system might be underestimated 4. The size of the software application with be underestimated 5. The user base of the application might be under or over-estimated, hence adversely impacting the design decisions

Table 1: Risks for NTUCollab Project

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 involves identification and assessment of the probability and seriousness of each risks based on consideration of several contributing factors. Probability may be classified into three categories of low, moderate, or high for analyzing the associated risk, depending on the likelihood of the risk. Similarly risk effects can be bifurcated into low, medium, and high, depending on the severeness of the consequences of the risk.

2.3.1   Qualitative Risk Analysis

The agreement of risk level would be brought up by experienced team members and agreed collectively by the team. The probability and impact of occurrence for each identified risk will be assessed by the project manager, with input from the project team using the following approach: The following Impact-Probability matrix will aid in assessing the likelihood and consequences of the risks.

		Low	Medium	High
Impact	**High**	1. Server Crash 2. Non-scalable deployment servers 3. Inefficient Code 4. Underestimation of Project Size	1. Reused Software Component Issues 2. High Rate of bugs & issues	
	Medium	1. Database Limits 2. API Malfunction 3. Developer Management Conflict 4. Undermined Motivation 5. Project Restructure 6. Inadequate Domain Knowledge 7. Planning Abandonment in high pressure 8. Under/Over Estimation of user base	1. Insufficient Firebase Storage 2. Requirements Changes 3. New use cases 4. Ill Staff 5. Time Underestimation 6. Multiple Commitments of Staff 7. Customer incorrect estimation of changes	
	Low	1. Scraper failure 2. Project Management Restructure	1. Course Structure Revamp	
		Low	**Medium**	**High**
			Probability	

Fig. 1 Impact-Probability Matrix for NTUCollab

Probability
- **High** – Greater than **70%** probability of occurrence
- **Medium** – Between **30%** and **70%** probability of occurrence
- **Low** – Below **30%** probability of occurrence

Impact
- **High** – Risk that has the potential to greatly impact project cost, project schedule or performance
- **Medium** – Risk that has the potential to slightly impact project cost, project schedule or performance
- **Low** – Risk that has relatively little impact on cost, schedule, or performance

Risks that fall within the RED and YELLOW zones will have risk response planning which may include both a risk mitigation and a risk contingency plan. Below is a table classifying the likelihood and seriousness of the consequences of each risk.

S. No	Risk	Probability	Effects
1.	**TECHNOLOGY**		
1.1.	The scraper assumes that the data provided from the Stars Planner has a particular structure. Drastic changes in this structure would cause the scraper to not work as per intended	**Low**	**Low**
1.2.	The database used in the system cannot process as many transactions per second as expected	**Low**	**Medium**
1.3.	Server crashes and essential data is lost	**Low**	**High**
1.4.	Google Login API malfunctions	**Low**	**Medium**
1.5.	Reused software components might have bugs and defects which may break the code	**Medium**	**High**
2.	**PEOPLE**		
2.1.	The developers are occupied with multiple projects at the same time and may be unavailable to attend possible meetings	**Medium**	**Medium**
2.2.	Conflicts between the developers and project manager	**Low**	**Medium**
2.3.	As the project duration is short, a team member falling ill and needing some time off would drastically delay project milestones	**Medium**	**Medium**

2.4.	Undermined motivation within the team members and developers	**Low**	**Low**
2.5.	Inadequate domain knowledge within developers	**Low**	**Medium**
3.	**ORGANIZATIONAL**		
3.1.	The course project might be revamped with different components	**Medium**	**Low**
3.2.	The project management might be restructured with different people responsible for the different parts	**Low**	**Low**
4.	**TOOLS**		
4.1.	The code generated by mobile SDK might be inefficient for actual deployment	**Low**	**High**
4.2.	The use of Firebase for data storage might be insufficient for the user data	**Medium**	**Medium**
4.3.	The deployment servers might not be scalable enough to meet the demands of peak user traffic	**Low**	**High**
5.	**REQUIREMENTS**		
5.1.	Changes in requirements are proposed to improve the quality of the software at late stage of development	**Medium**	**Medium**
5.2.	New use cases arise at late stage of development, giving rise to new requirements to be incorporated	**Medium**	**Medium**

5.3.	Customers fail to understand the impact of requirement changes	**Medium**	**Medium**
6.	**ESTIMATION**		
6.1.	The time required to develop the various components of the software is underestimated	**Medium**	**Medium**
6.2.	Abandoning of planning under pressure	**Low**	**Medium**
6.3.	The rate of bugs and issues in the system might be underestimated	**Medium**	**High**
6.4.	The size of the software application with be underestimated	**Low**	**High**
6.5.	The user base of the application might be under or over-estimated, hence adversely impacting the design decisions	**Low**	**Medium**

Table 2: Risk Analysis for NTUCollab

2.3.2   Quantitative Risk Analysis

Analysis of risk events that have been prioritized using the qualitative risk analysis process and their effect on project activities will be estimated, a numerical rating applied to each risk, and then documented in this section of the risk management plan.

Area of Risk	Severity	Likelihood	Level of Control	Significance
Technology	3	2	2	**7**
People	3	2	2	**7**
Organizational	2	1	2	**5**
Tools	2	1	2	**5**
Requirements Changes	3	3	1	**7**
Estimation	2	3	2	**7**

Table 3: Quantitative Risk Analysis for NTUCollab

2.4 RISK RESPONSE PLANNING

Each major risk (those falling in the Red & Yellow zones) will be assigned to a project team member for monitoring purposes to ensure that the risk will not "fall through the cracks".

For each major risk, one of the following approaches will be selected to address it:

- **Avoid** – eliminate the threat by eliminating the cause
- **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 mitigated, the project team will identify ways to prevent the risk from occurring or reduce its impact or probability of occurring. This may include prototyping, adding tasks to the project schedule, adding resources, etc.

For each major risk that is to be mitigated or that is accepted, a course of action will be outlined for the event that the risk does materialize in order to minimize its impact.

Area of Risk	Approach Selected	Strategy
Technology	Avoid	Sufficient and appropriate investment in high quality technology to ensure robustness and reliability. Investments in highly redundant databases and highly scalable servers will enable to avoid the imminent risks
People	Mitigate	The team will be reorganized so to enable more overlap between work of various team members, this will ensure a substitute in the event of a staff illness A team member will be in

		charge to ensure overall team wellness and cohesion as well as monitor their KPIs
Organizational	Accept	Organizational changes will have to be accepted and appropriate changes will have to be made accordingly
Tools	Mitigate	Thorough analysis and will be done before the agreed use of a tool for the project. Any defective components will not be used and replaces with reliable bought-in tools
Requirements changes	Accept	The requirements are bound to change in due course will have to be accepted, and the necessary changes will have to be made in project timeline and structure on the basis of such CRs
Estimation	Mitigate	Investigate use of a program generate for accurate estimation of timelines and project milestones.

Table 4: Risk Response Planning for NTUCollab

2.5   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 project team 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.
- Management will be notified of important changes to risk status as a component to the Executive Project Status Report.
- Each identified risk will be thoroughly and regularly assessed to monitor any changes in its likelihood
- Each risk will be discussed at the Management Progress Meetings

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.

- Constant monitoring on each risk on a weekly basis will also be done and checked by the project manager to ensure everything is in control.

- Further any risk indicators for each of the risk areas will be closely monitored to

- The risk mitigation strategies will be diligently practiced with frequent reviews and drills to avert any possible or likely risk which might occur during the project.

- At each team meeting all the identified risk will be reviewed and further updates will be made in case of any new risks.

RISK MANAGEMENT PLAN APPROVAL

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

Signature: **Date:**   6 March 2021

Print Name: Bansal Aditya

Role: Quality Engineer

Signature: **Date:**   6 March 2021

Print Name: Somani Palak

Role: Quality Manager

Signature: **Date:**   6 March 2021

Print Name: Dandapath Soham

Role: Project Manager (PM)

APPENDIX A: REFERENCES

The following table summarizes the documents referenced in this document.

Document Name and Version	Description	Location
NTUCollab System requirement specification	The NTUCollab System Requirement Specification (SRS) is the document describing all the requirement specifications, to which this risk management plan refers to	https://172.21.149.196/svn/3002/B2/Eagles/Lab-2/System_Requirement_Specifications.pdf
NTUCollab Quality Management Plan	The Quality Management Plan describes all the Quality Assurance (QA) and management protocols which complement the risk management plan	https://172.21.149.196/svn/3002/B2/Eagles/Lab-2/Quality_Plan.pdf
CDC UP Risk Management Plan Template	The NTUCollab Risk Management Plan has been based on the CDC Up Template	NTU Learn

Table 5: Reference

APPENDIX B: KEY TERMS

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

Term	Definition
Budget	The approved estimate for the project or any work breakdown structure component or any schedule activity.
Change Management Log	A tool used by project teams to document and track the resolution of change requests.
Change Request (CR) -	A request to expand or reduce the project scope, modify policies, processes, plans, or procedures, modify costs or budgets, or revise schedules. Requests for a change can be direct or indirect, externally, or internally initiated, and legally or contractually mandated or optional. Only formally documented requested changes are processed, and only approved change requests are implemented
Data Warehouse	A collection of data designed to support management decision making.
Key Performance Indicators (KPI)	Measurable indicators that will be used to report progress that is chosen to reflect the critical success factors of the project.
Quality Assurance (QA)	The process of evaluating overall project performance on a regular basis to provide confidence that the project will satisfy the relevant quality standards.
Qualitative Analysis	It assesses priority identified by using the probability of occurring, corresponding impact on project objectives, as well as other factors such as the time frame and risk tolerance of the project constraints of cost, schedule, scope, and quality.
Risk Response Planning	The process of developing options and actions to enhance opportunities and to reduce threats to project objectives. Risk response actions may include mitigation, contingency, transfer, avoidance, and acceptance.

Table 6: Key Terms