CASHTRACK

RISK MANAGEMENT PLAN

Version 1.3

8th March 2021

By:
Team Runtime Terror
Ravishankar Amrita (U1822377F)
Datta Anusha (U1822948G)
Kumar Mehul (U1822146E)
Alex Leong (U1921599D)
Nicklaus Tan (1403385F)
Elliott Ong (U1922981C)
Daniel Loe (U1921408A)
S Sri Kalki (U1921575L)

VERSION HISTORY

Version #	Implemented By	Revision Date	Approved By	Approval Date	Reason
1.0	Alex Leong, Ravishankar Amrita, Anusha, Daniel Loe, Elliott Ong, S Sri Kalki, Kumar Mehul	17th February 2021	Nicklaus Tan	21st February 2021	Initial Risk Management Plan draft
1.1	Nicklaus Tan	22nd February 2021	Daniel Loe	24th February 2021	Revision in Purpose and Appendix A
1.2	Elliott Ong	1st March 2021	Nicklaus Tan	2nd March 2021	Revision in Risk Analysis
1.3	Alex Leong, Ravishankar Amrita, Anusha, Daniel Loe, Elliott Ong, S Sri Kalki, Kumar Mehul	8th March 2021	Nicklaus Tan	8th March 2021	Final changes & revision for all sections

TABLE OF CONTENTS

1   INTRODUCTION

1.1   PURPOSE OF THE RISK MANAGEMENT PLAN

The purpose of this document is to identify the potential risks during the development of the CashTrack Application. 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 CashTrack 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 CashTrack project and is monitored and updated throughout the project.

1.2   INTENDED AUDIENCE

The intended audience of this document is the project team, project sponsor and management.

2   RISK MANAGEMENT PROCEDURE

2.1   PROCESS

The following five risk management process steps will be utilized to deliver a simple yet effective risk management process.

1) Identify the Risk
During this step, the project manager alongside their team will discover, recognize and describe risks that might affect the project or its outcome.

2) Analyze the Risk
Once the risks have been identified, the likelihood and consequence of each risk must be determined.

3) Evaluate the Risk
Using the risk magnitude, which is the combined result of the likelihood and consequence of each risk determined, a ranking will be made to evaluate the severity of how much each risk impacts the project. Using these rankings, the team is able to determine which are the risks that have to be pursued and responded to immediately.

4) Treat the Risk
Create risk mitigation strategies, contingency plans, preventive plans and risk treatment measures for the highest ranking risks identified.

5) Monitor and Review the Risk
Monitor the development of the project while keeping track and reviewing the risks identified. By ensuring that there is a framework to fall back on, this alleviates the

uncertainty factor of what to do in the event of a risk occurring. The end result being the minimization of impacts of potential project threats.

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.

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 at Wiki.

Risks identified will be classified into one of the six following categories respectively, namely, Technology, People, Organisational, Tools, Requirements, Estimation.

- **Technology Risks** – Risks that are derived from both software and hardware technologies used in the development of the system.
- **People Risks** – Risks that occur due to people related issues including team member's availability, competency, medical condition, attitude and etc.
- **Organizational Risks** – Risks that are caused by the environment where the system is being developed.
- **Tools Risks** – Risks that are related to the availability, usability and reliability of the supporting tools used for the development of the system.
- **Requirements Risks** – Risks that occur due to abrupt changes in requirements where major rework is needed or lack of the impact caused by these changes.
- **Estimation Risks** – Risks that appear from the inaccurate estimation of size of project, effort, duration and the resources required for the project.

The below table states the potential types and descriptions of risks identified during the development of the project.

	Risk Type	**Risk Description**
1	Technology	Software used is not compatible with other technical components (Hardware/Software) of the system.
2	People	Key team members are unavailable often at critical timings.
3	Organization	The organization is restructured so that different management

		teams are responsible for the project.
4	Tools	Defects/malfunctions/unreliability in supporting tools used for the development of the system
5	Requirements	Difference between functional requirements documented and functional requirements developed.
6	Estimation	Milestones/Deadline completion variability due to the four classic mistakes, people-related mistakes, process-related mistakes, product-related mistakes and technology-related mistakes.

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.
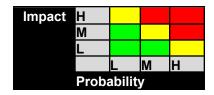
2.3.1 Qualitative Risk Analysis

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:

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.

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 based on this analysis, and then documented in this section of the risk management plan.

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.

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.

Documentation of Risks

The following items will be documented during the risk monitoring and control process:

● Risk Management Plan

● Risk Log

  ● Risk Type - Type of risk identified

  ● Risk Description - Description of the risk

  ● Occurrence
    ➢ High

- ➢ Medium
- ➢ Low

- Severity of risks
  - ➢ Catastrophic
  - ➢ Serious
  - ➢ Tolerable
  - ➢ Insignificant

- Priority of risks
  - ➢ High
  - ➢ Medium
  - ➢ Low

- Mitigation / Contingency Plan - Steps taken to either mitigate the risk or handle the risk when it occurs

- Status of active risks

  - ➢ Triggered: Identified risk(s) have occurred
  - ➢ Resolved: Realized risk has been settled
  - ➢ Retired: Identified risk no longer requires active monitoring (e.g. risk trigger has passed)

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. An extracted view of the Risk log can be viewed as follows:

	Risk Type	Risk Description	Occurrence	Severity	Priority	Mitigation / Contingency Plan	Status
1	People	Key personnel unavailable during time critical period	High	Serious	High	Get available personnel (i.e. working on low priority tasks) that understands task at hand to temporarily take over key personnel role	Retired

2	Tools	Possibility of single point failures, such as data corruption or tool used for coding malfunctions	Medium	Serious	High	Have modularity and portability in design so that modules can be independent shifted around	Resol ved
3	Techn ology	Software and hardware components used for development are not compatible	Medium	Catastro phic	High	Research extensively prior on the compatibility issues between components to be used as well as to ensure portability	Resol ved
4	Organi zation al	Restructuring of organization such that separate teams are now working on the system	Low	Tolerabl e	Medi um	Use of source code management and version control via Github	Resol ved
5	Requir ement s	Contrast between functional requirements documented and functional requirements developed.	High	Tolerabl e	Medi um	Use of collaboration tools like Jira to ensure that the functional requirements developed are consistent with the ones which were documented	Trigg ered
6	Estima tion	Inaccurate estimations that are either overly optimistic or unrealistic	High	Tolerabl e	Low	Break the work down into smaller pieces/activities then perform estimation for a more accurate and realistic estimation	Retir ed

RISK MANAGEMENT PLAN APPROVAL

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

Signature: Date: 03/01/2021

Print Name:	Nicklaus Tan
Title:	Project Manager
Role:	Overall delivery of product

Signature: Date: 03/01/2021

Print Name:	Kumar Mehul
Title:	Lead Developer
Role:	Overall technical lead, responsible for technical aspects of product release

Signature: Date: 03/01/2021

Print Name:	S Sri Kalki
Title:	QA Manager
Role:	Overall product and process quality, implementation of QA processes

Signature: Date: 03/01/2021

Print Name:	Daniel Loe
Title:	QA Engineer
Role:	Device test plans, conduct tests

APPENDIX A: REFERENCES

The following table summarizes the documents referenced in this document.

Document Name and Version	Description	Location
Use Case Descriptions (Version 1.3)	*Formal description of system behavior with regards to user's request.*	*Wiki*
Quality Plan (Version 1.4)	*Specify quality standards, practices, resources, specifications, and the sequence of activities*	*Wiki*

APPENDIX B: KEY TERMS

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

Term	Definition
Activity	An activity is a term used by the SDN to distinguish a service that is provided by the SDN within a particular service that is being accessed by users. An example of an activity could be accessing a particular application, downloading training materials, uploading a data file. All of these activities, if performed for a particular branch or project, would be contained within one program within the SDN.
Deliverable	Deliverable - Any unique and verifiable product, result, or capability to perform a service that must be produced to complete a process, phase, or project.
Gantt Chart	A bar chart that depicts a schedule of activities and milestones. Generally activities (which may be projects, operational activities, project activities, tasks, etc.) are listed along the left side of the chart and the time line along the top or bottom. The activities are shown as horizontal bars of a length equivalent to the duration of the activity. Gantt Charts may be annotated with dependency relationships and other schedule-related information.
Goal	A one sentence definition of specifically what will be accomplished, while incorporating an event signifying completion.
Meeting Minutes	Meeting Minutes are a written record of what transpired during a meeting. Meeting minutes provide the purpose of a meeting, list of attendees, topics discussed, decisions made, the status of actions from the previous meeting, new action items and the individuals assigned responsibility for the actions.
Non-Functional Requirements	Non-functional requirements specify the criteria that are used to judge the operation of a Business Product, rather than specific behaviors (in contrast to functional requirements, which describe behavior or functions). Typical non-functional requirements are reliability, scalability, accessibility, performance, availability, and cost. Other terms for non-functional requirements are "constraints", "quality attributes", and "quality of service requirements". Non-functional requirements also specify the laws, regulations, and standards with which the Business

	Product must comply. How the Business Product must comply with laws, regulations, and standards.
Requirement	A condition or capability that must be met or possessed by a system, product, service, result, or component to satisfy a contract, standard, specification, or other formally imposed documents. Requirements include the quantified and documented needs, wants, and expectations of the sponsor, customer, and other stakeholders (PMI PMBOK). Requirements specify what should be produced. They are descriptions of either how the Business Product should behave (functional requirements), or of how the Business Product must comply with laws, regulations, and standards (non-functional requirements)
Risk	A risk is defined as an uncertain event or condition that, if it occurs, has a positive or negative affect on a project's objectives. An uncertain event that may affect the performance objectives (i.e., cost, schedule, scope or quality) of an investment, usually negatively.
Use Case	A description of system behavior, in terms of sequences of actions. A use case should yield an observable result of value. A use case should contain all alternative flows of events related to producing the intended observable value.
Workflow	Order in which specific work is performed. Often represented graphically.