



---

# **KIM'S CONVENIENCE MODERN CINEMA RISK MANAGEMENT PLAN**

---

*Version 1.1*  
29/09/2021

## VERSION HISTORY

Version #	Implemented By	Revision Date	Approved By	Approval Date	Reason
1.0	Taneja Parthasarathi	29/09/21	Wong Ying	30/09/21	Initial Risk Management Plan draft
1.1	Taneja Parthasarathi	01/10/21	Wong Ying	06/10/21	Finalised Plan

# TABLE OF CONTENTS

<b>INTRODUCTION</b>	<b>1</b>
PURPOSE OF THE RISK MANAGEMENT PLAN	1
<b>RISK MANAGEMENT STRATEGY</b>	<b>1</b>
<b>RISK MANAGEMENT PROCEDURE</b>	<b>1</b>
PROCESS	1
RISK IDENTIFICATION	2
RISK ANALYSIS	2
Qualitative Risk Analysis	2
Quantitative Risk Analysis	2
RISK RESPONSE PLANNING	3
RISK MONITORING, CONTROLLING, AND REPORTING	3
<b>TOOLS AND PRACTICES</b>	<b>3</b>
<b>APPENDIX A: REFERENCES</b>	<b>5</b>
<b>APPENDIX B: KEY TERMS</b>	<b>6</b>
<b>APPENDIX C: EXAMPLE RISK MANAGEMENT LOG</b>	<b>7</b>

# 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 Kim's Convenience Modern Cinema (KCMC) 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 STRATEGY

Kim's Convenience Modern Cinema will employ a proactive risk management strategy. This is accomplished via careful and continuous evaluation of critical project areas in order to identify risk events, work as a cohesive team to determine the potential impact and damage of each identified risk, develop and implement mitigation and avoidance strategies for each identified risk, and monitor the risks until they are resolved.

Proactive risk management aims to identify risks as early as possible to avoid or minimize any adverse impact the risks may have on the project. This strategy will be conducted by the project team on the following principles:

- **Honesty and Transparency:** Risks are to be identified and assessed in an honest and objective manner. Risk exposure should be communicated constantly and completely to project team members.
- **Full Participation:** Every member of the project team must understand the risk management plan, strategy and procedures, as well as to participate in the identification and mitigation of risks, to enable coverage of as many perspectives as possible.
- **Effectiveness:** Risk tracking and measuring techniques should be kept simple, so they are more easily understood by all team members and identification of risks can be done more quickly and efficiently.

## 3 RISK MANAGEMENT PROCEDURE

### 3.1 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. Taneja Parthasarathi will serve as the Risk Manager for this project.

### 3.2 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 team's Google Drive.

Risks identified will be classified into one of the following six categories

- **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 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.

### 3.3 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.

#### 3.3.1 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 75% probability of occurrence
- Medium – Between 25% and 75% probability of occurrence
- Low – Below 25% probability of occurrence

I m p a c t	H		
	M		
	L		
		L	M
Probability			

**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.

**3.3.2 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.

**3.4 RISK RESPONSE PLANNING**

Each major risk (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.

**3.5 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)

## **4 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 KCMC project. Changes to this Risk Management Plan will be coordinated with and approved by the undersigned or their designated representatives.

Signature:



Date: 06 Oct 2021

Print Name:

Wong Ying

Title:

Engineering Manager

Role:

KCMC Project Manager

Signature:



Date: 06 Oct 2021

Print Name:

Hussain

Title:

Senior Software Engineer

Role:

KCMC Lead Developer

Signature:

Taneja

Date: 06 Oct 2021

Print Name:

Taneja Parthasarth

Title:

Senior Project Engineer

Role:

QA Manager



---

**APPENDIX A: REFERENCES**

The following table summarizes the documents referenced in this document.

<b>Document Name and Version</b>	<b>Description</b>	<b>URL or Network Path Location</b>
Project Plan (Version 2.1)	Describes the plan for the development of the KCMC project. Section 8 contains the list of risks for the project.	Project Plan document in Wiki SVN.
Use Case Descriptions (Version 1.3)	Formal description of system behavior with regards to user's request.	Use Case Descriptions document in Wiki SVN.
Quality Plan (Version 1.4)	Specify quality standards, practices, resources, specifications, and the sequence of activities	Quality Plan document in Wiki SVN.
Risk Management Log	As the project proceeds, newly identified risks will go into a separate risk management log document.	The Risk Management Log should use the template in Appendix C of this document. An excerpt is provided for example.

**APPENDIX B: KEY TERMS**

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

<b>Term</b>	<b>Definition</b>
Activity	<i>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.</i>
Deliverable	<i>Deliverable - Any unique and verifiable product, result, or capability to perform a service that must be produced to complete a process, phase, or project.</i>
Gantt Chart	<i>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.</i>
Goal	<i>A one sentence definition of specifically what will be accomplished, while incorporating an event signifying completion.</i>
Meeting Minutes	<i>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.</i>
Non-Functional Requirements	<i>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.</i>
Requirement	<i>A condition or capability that must be met or possessed by a system, product, service, result, or component to satisfy a contract,</i>

	<i>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)</i>
Risk	<i>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.</i>
Use Case	<i>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.</i>
Workflow	<i>Order in which specific work is performed. Often represented graphically.</i>
Risk	<i>An event or condition that, if it occurs, could have a positive or negative effect on the project's objectives.</i>
Risk Exposure	<i>The measure of potential future loss or losses which may occur from an activity or event.</i>
Risk Management	<i>The process of identifying, assessing, responding to, monitoring, and reporting risks.</i>
Risk Management Strategy	<i>A view on the approach towards the identification, assessment, response and monitoring of risks.</i>
Risk Management Process	<i>The defined procedures and methodologies as a series of steps or activities towards the management of risks.</i>
Risk Identification	<i>The process of determining and discovering all possible risks of the project.</i>
Risk Analysis	<i>The process of assessing the likelihood of a risk occurring (probability), and the possible amount of damage that will be done to the project (impact).</i>
Risk Response	<i>The process of planning and deciding the procedures to react to the risks identified for the project.</i>
Risk Monitoring	<i>The process of tracking the level of risk for the project, by tracking the management of identified risks and continual identification of new risks to be managed.</i>

**APPENDIX C: RISK MANAGEMENT LOG (EXAMPLE)**

The following table is an example of risks in the Risk Management Log.

<b>Risk Type</b>	<b>Risk Description</b>	<b>Occurrence</b>	<b>Severity</b>	<b>Priority</b>	<b>Mitigation / Contingency Plan</b>	<b>Status</b>
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	
Tools	Possibility of single point failures, such as the application or the KCMC movie recommendation model malfunctions	Medium	Serious	High	Have modularity and portability in code design and dependencies so that modules can be independent shifted around	
Technology	Software and hardware components used for development are not compatible (for example, choosing a comprehensive tech stack)	Medium	Catastrophic	High	Research extensively prior on the compatibility issues between components to be used as well as to ensure portability	Resolved
Organizational	Restructuring of organization	Low	Tolerable	Medium	Use of source code management and	Resolved

**Revision Date:**29/09/2021

**Risk Management Plan Template**

*Sensitive But Unclassified*

	such that separate teams (roles defined in the Project Proposal and further division of sub teams) are now working on the system				version control via Github for software control. Clear division of work and frequent check-ins (via text/call/internal presentations) for documentation.	
Estimation	Inaccurate estimations and deadlines that are either overly optimistic or unrealistic	High	Tolerable	Low	Break the work down into smaller pieces/activities then perform estimation for a more accurate and realistic estimation through thorough discussions.	Retired