“Advanced AI Powered SaaS Platform for Image Processing”

Final Risk Assessment Report

DevFusion

Prepared by:

P.U.Nisansa (Risk Manager)
12th August 2024

TABLE OF CONTENTS

RISK ASSESSMENT REVIEW SHEET

This Risk Assessment has been updated and approved on the following dates to account for the latest changes. This task will be completed at least annually.

Approval Date	Name & Designation	Signature of Security Officer
12/08/2024	Ranali Mayadunne (Project Manager)	ranali

1.0 Introduction

This document describes the risk assessment conducted throughout the entire project life cycle for the “Advanced AI Powered SaaS Platform for Image Processing", developed by the DevFusion team. Although risks cannot eliminate entirely, they can be minimized and manages through the application of IT security controls and by responsible personnel. This risk assessment describes the system’s vulnerabilities and associated threats based on technical guidelines, and outlines the risk management strategies and methods used.

Risk assessment is a critical tool for identifying and evaluating potential risks, as well as determining the potential for loss to organizational operations and stakeholders. By identifying risks early and applying appropriate mitigation methods, the project was successfully completed without any delays. Enabling risk management for the AI Powered SaaS Platform system focuses on identifying potential risks throughout the project life cycle, analyzing these risks and threats, and finally mitigating and monitoring them. Through this risk assessment the team aims to meet the client expectation and minimize financial costs to deliver the project successfully to meet the client expectation. This includes assessing and controlling financial risks, market risks, technical risks and security risks.

1.1. Purpose

The purpose of this report is to present threats and vulnerabilities applicable to project "Advanced AI Powered SaaS Platform for Image Processing" which ran throughout four months. It also describes the each risk, evaluates the likelihood that vulnerability can be exploited, assesses the impact associated with these threats and vulnerabilities, and identifies the overall risk level. This report documents risk assessment activities conducted by risk manager from Start Date to End Date, and will help Operating Administration management understand risks.

1.2. Scope

The scope of this risk assessment is to evaluate risks to "Advanced AI Powered SaaS Platform for Image Processing" in the areas of operational, technical, client expectations, documenting and financial. This risk assessment is limited to project boundary. Furthermore at the moment risks regarding to information security are not considered and those will be implemented and identified when the product go live.

1.3. Testing Methods

Techniques and strategies to assess and evaluate the risk management are the testing methods for risks and threats. Identifying those potential risks before explode is crucial for a successful project delivery. In this section those methods use in "Advanced AI Powered SaaS Platform for Image Processing" will be discussed.

- **Check lists and Inspections**

  The software development methodology used for this project is “Agile” and at the beginning of each Sprint a predefined checklist that can associate with the project was created to ensure that the all risk factors are considered. This method helped to keep consistency in in risk management and assessment throughout the project life cycle.

- **Expected Monetary Value (EMV) Analysis**

  This is the method used to perform quantitative risk analysis of the project. By calculating the necessary input variables, EMV and the total risk exposure were calculated for the all risks.

1.4. Document Structure

This document is organized into five sections:

- Section 1.0 provides the introduction, purpose, and scope of this risk assessment.
- Section 2.0 provides an overview of the risk assessment methodology.
- Section 3.0 provides a system description
- Section 4.0 provides the methodology to calculate risk, which includes identifying threats, likelihood, and impact.
- Section 5.0 provides the risk assessment results.

2.0 Risk Assessment Methodology

Risk analysis methodology is structured as following phases:

- Risk analysis threats and vulnerabilities.
- Management decisions to implement security countermeasures.
- Implementation of countermeasures.
- Periodic review of the risk management process.

Risk assessment methodologies were used to identify and evaluate the risks and also to make decisions on how to manage and mitigate risks. The methodologies used in “"Advanced AI Powered SaaS Platform for Image Processing"” project are described as below,

1) **Qualitative Risk Assessment**

- The risks were assessed based on qualitative measure and risks were categorized by their impact (low, medium, high), likelihood and probability.
- The tool used is “***Risk Register***” which is a document that records identified risks in each week and Sprint along with their assessment and mitigation.

2) **Quantitative Risk Assessment**

- Using numerical to evaluate risks and calculate the probability and the impact of the risks along with expected outcomes to provide a more precise assessment.
- The tool used is “***Expected Monetary Value (EMV) Analysis***”.

2.1 Identifying System Assets

To identify system risks and threats it's important to identify the system assets which are system architecture and the components. In this project the system assets are the critical components, resources and data that need for system's functionality. Here are the key assets of the application.

- AI Model - machine learning model used for image processing tasks.
- Could computing resources – used for processing large volumes of images.
- APIs and Integrations – facilitate interoperability and enables third party services.
- UI/UX – frontend components that used to interact with users including web interfaces.
- Database and storage - managing image data, model artifacts, user data, and logs.

2.3 Analyzing System Vulnerabilities

Vulnerabilities are weaknesses in the environment, system architecture, design, or implementation; and the management or administration of hardware, software, data, facility, or personnel resources. After analyzing system management, operational, and technical security controls for the system, system vulnerabilities are then identified. The analysis of the system's vulnerabilities, the threats associated with them, and the probable impact of that vulnerability exploitation resulted in a risk rating for each missing or partially implemented control. The risk level was determined on the following two factors:

1. **Likelihood of Occurrence** - The likelihood to which the threat can exploit a vulnerability given the system environment and other mitigating controls that are in place.
2. **Impact** – The impact of the threat exploiting the vulnerability in terms of loss of tangible assets or resources and impact on the organization's mission, reputation or interest.

To determine overall risk levels, the availability, integrity, and confidentiality of the system will be measures in future.

- **Loss of Availability**– Access to the system, specific system functionality or data is not available.

- **Loss of Integrity/ Modification** – Total loss of the asset either by complete destruction of the asset or irreparable damage, or unauthorized change, repairable damage to the asset, or change to asset functionality.
- **Loss of Confidentiality/Disclosure** – Release of sensitive data to unauthorized individuals.

The analysis of the systems vulnerabilities and risk determination will be further discussed in Section 4.0, Risk Calculation.

2.4 Information Sensitivity

The following table provides a general description of the information handled by the system and the need for protective measures.

Information Category	Explanation and Examples	Protection Requirements
AI Models	Machine learning and deep learning models used for image processing tasks like object detection, classification, segmentation.	• Encryption **during storage and transmission** • Access control **to limit who can view or modify models** • Regular backups **to prevent data loss**
User Data	Personal information, account details, and activity logs of users.	• Strong authentication **(e.g., multi-factor authentication)** • Data encryption **at rest and in transit** • Regular audits **for compliance**
Software Infrastructure	The software stack, web frameworks, APIs, databases, third-party services (Claudenary).	• Regular security assessments. • API security **through tokens and keys**
User Interface (UI) & User Experience (UX)	Front-end components like web interfaces, dashboards, and mobile apps.	• Secure coding practices **to prevent vulnerabilities**
Data Storage Systems	Databases and storage solutions for managing image data, models, user data.	• Access control **for sensitive data**

3.0 Risk Calculation

This section discusses vulnerabilities, the threats, and the probable impact of that vulnerability exploited. System vulnerabilities are identified as required security controls that are not fully implemented. These are classified as vulnerabilities because the lack of required controls result in vulnerability that a threat can be exploited successfully.

The risk level was determined based on the following two factors:

1. **Impact** of the threat exploiting the vulnerability in terms of loss of tangible assets or resources and impact on the organization's mission, reputation, or interest.
2. **Likelihood** to which the threat can exploit a vulnerability given the system environment, threat frequencies, and other mitigating controls in place.

The following sections discuss the areas of potential impact and how the values for the above two factors, magnitude of impact and likelihood of occurrence, and the level of risk were determined.

3.1 Impact

An impact analysis prioritizes the impact levels associated with the compromise of an organization's information assets based on a qualitative or quantitative assessment of the sensitivity and criticality of those assets.

Financial impact quantified according to,

- Cost of extended project duration due to delays.
- Cost of rework
- Labor costs
- Material cost

Impact Level/Value	Impact Description
Catastrophic (> 100,000 lkr)	Impact of the vulnerability may cause most severe consequences that a risk can have on the project and a significant financial loss.
Critical (50,000 - 100,000 lkr)	Impact of the vulnerability may result in the highly costly loss of major tangible assets or resources
Moderate (10,000 - 50,000 lkr)	Impact of the vulnerability may result in the costly loss of major tangible assets or resources
Low (< 10,000 lkr)	Impact of the vulnerability may result in loss of some tangible assets or resources.

3.2 Probability

The probability of a risk refers to the likelihood that a particular risk will occur within a given context, such as a project or organization. Assessing the probability of a risk is a crucial part of the risk assessment process, as it helps determine how likely it is that a risk event will happen, thereby allowing for appropriate planning and mitigation strategies.

The likelihood that a threat will exploit a vulnerability and cause damage for each of the four areas listed above was determined based on the following factors: Likelihood of occurrence was determined qualitatively to be high, moderate, or low using the following criteria.

Value	Probability Description
Very High	Threat-source is highly motivated and possesses the necessary capabilities to exploit the vulnerability.
High	The threat-source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exploited are ineffective.
Moderate	The threat-source is motivated and capable, but controls are in place that may impede successful exploitation of the vulnerability.

Low	The threat-source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exploited.
Very Low	Threat-source lacks the capability to exploit the vulnerability, and effective controls are in place that prevents the successful exploitation of the risk.

Probability has categorized as,

- Very High (80% - 100%)
- High (60% - 80%)
- Medium (40% - 60%)
- Low (20% - 40%)
- Very Low (0 - 20%)

Countermeasure Implementation Status	**Threat Frequency**		
	High	**Moderate**	**Low**
I (Implemented)	Likelihood = 0.1	Likelihood = 0.1	Likelihood = 0.1
P (Partially Implemented)	Likelihood = 0.5	Likelihood = 0.5	Likelihood = 0.1
NI (Not Implemented)	Likelihood = 1.0	Likelihood = 1.0	Likelihood = 0.5
NA (Not Applicable)	Likelihood = 0.1	Likelihood = 0.1	Likelihood = 0.1

3.3 Risk Exposure

A relative risk exposure was determined for each vulnerability. The purpose in defining this risk exposure is to determine both the overall level of risk for the system as well as the degree to which each vulnerability contributes to that risk.

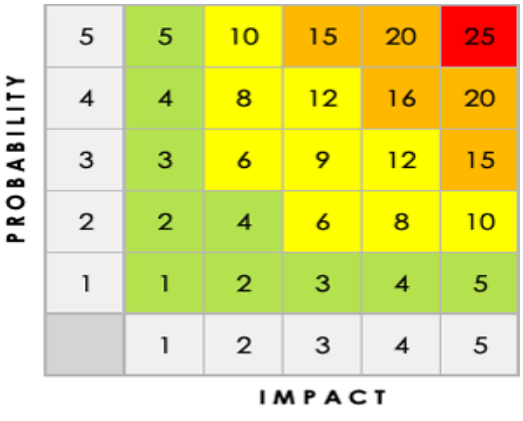
Since currently the team doesn't have subject matter experts for marketing and finance to perform expert judgment, I researched and analyzed *similar past projects* to find the probability and impact. Therefore these variables are estimated using *historical data*.

The risk exposure for each control was determined by the following formula:

Risk = Probability x Consequence

Id	Risk	EMV
1	Unclear project requirements.	16,000 * 0.80 = **12,800 LKR**
2	Difficulties understand new advanced technical concepts and new tools.	40,000 * 0.60 = **24,000 LKR**
3	Limited technical expertise on some technical areas such as cloud services and SaaS.	300,000 * 0.40 = **120,000 LKR**
4	Unavailability team members to the meetings.	32,000 * 0.00 = **0 LKR**
5	Market competition	(50000 + 100000) / 2 * 0.80 = **60,000 LKR**
6	UI designing Time Overruns (>60% tasks are in schedule)	3,034 * 0.20 = **606.80 LKR**

Table 5.1: Risk Register



IMPACT LEVEL	PROBABILITY LEVEL	PRIORITY LEVEL
Rate 1 (Low) to 5 (High)	Rate 1 (Low) to 5 (High)	Impact * Probability

RISK DESCRIPTION	IMPACT DESCRIPTION	IMPACT LEVEL	PROBABILITY LEVEL	PRIORITY LEVEL	MITIGATION NOTES	OWNER
Unclear project requirements.	The project requirements mentioned by the client are unclear and often changing,	4	4	16	Conduct a thorough requirement gathering meetings with the client and clearly define project scope, deliverables, goals.	Project Manager

	it leads to project delays and also scope creep.				Use techniques like user stories, prototypes and wireframes to illustrate the project functionalities and requirements.	
Difficulties understand new advanced technical concepts and new tools	When there is a difficulty or unawareness of advanced technical concepts and skills it creates implementation issues.	3	2	6	Provide training sessions before the implementation phase. Encourage members to be open and get assistance immediately when they need from mentors. Encourage the team in self-learning.	
Limited technical expertise on some technical areas such as cloud services and saas.	When there is a limited technical expertise in a particular area it limits the project and gets all benefits for that mentioned technology.	4	4	16	Conduct up-skilling the team members in cloud and saas technologies.	
Unavailability team members to the meetings	When the regular absences happen or the regular unavailability increases the miscommunication and also leads to wrong decision making.	3	4	12	Use scheduling tools to schedule meetings in advance. Project manager can advise the members or try to find the causes and find solutions. Maintain a clear agenda.	
Market competition	Market competition is a significant risk as the competitors in the same	4	4	16	Always stay aware of other competitors and regularly analyses new market trends and adapt to those strategies.	

	industry can come up with more advanced yet cost effective smart solutions. The user can be more attractive for such products and services over others.				Regularly engage with clients and users and implement a feedback mechanism to collect user feedback and preferences and do improvements according to them.	
UI designing Time Overruns	Significant project delays.	4	3	12	Break downed the UI design tasks into smaller, manageable components and allocated realistic timelines for each task and used project management tools to track progress. Held regular sprint reviews Increased communication among team members.	
Budget overruns	Direct increase in expenditure beyond the initial budget, affecting the project's profitability.	5	4	20	Conduct regular financial reviews. Ensured that the client was involved in the budgeting process and understood the financial constraints of the project.	