**ASSETRUST Risk**

**Management Plan**

A picture containing text

Description automatically generated

**ASSETRUST Software**

**Revision A**

**Project ID: #000-0001**

# Revisions

|  |  |  |  |
| --- | --- | --- | --- |
| **REVISION** | **DESCRIPTION OF CHANGE** | **REVISION DATE** | **AUTHRORIZED BY** |
| A | Initial Document | 04/02/2022 | Parsa Afrai  Marcos Vallejos  Mercy Jalango  Ian Davies  Luis Ruiz |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Contents

[Revisions 2](#_Toc101045850)

[Introduction 5](#_Toc101045851)

[Methodology 5](#_Toc101045852)

[Roles and Responsibilities 6](#_Toc101045853)

[Budget and Schedule 7](#_Toc101045854)

[Risk Categories 8](#_Toc101045855)

[Risk Probability and Impact 10](#_Toc101045856)

[Tracking 10](#_Toc101045857)

[Risk Documentation 11](#_Toc101045858)

[Document Retention 12](#_Toc101045859)

[Sponsor Acceptance 12](#_Toc101045860)

Graphical user interface, text, application

Description automatically generated

# Introduction

Planning for risks related to the project, as well as how to approach and address them alongside their consequences is an important part of proper project management. Assetrust’s Risk Management Plan serves as the documentation of activities related to risk, addressing important topics such as the methodology behind how risk management will be performed, roles and responsibilities as they relate to risk, the preparation of budget and schedule estimates for risk-related activities, the risk categories under consideration, the assessment of risk probabilities and impacts, and lastly the creation of any risk-related documentation. The risk management plan is an ever-evolving document that will undergo revisions and modifications as the environment surrounding the project and technology changes. As new threats and vulnerabilities lead to new risks being discovered, the risk register included with the documentation will be updated alongside the plan.

# Methodology

Risk Management will be performed on this project using the various plans set in place. While the project has its own plans, it is important to remember that the organization also has risk management policies in place at the corporate level. These higher-level risk management policies will be referenced to ensure that the project’s risk management strategy aligns with that of the organization. The most important plans regarding the response to risk related incidents are the contingency plans and the fallback plans. The contingency plans outline what actions to take in the event of a risk related incident. Preparation allows for an effective and swift response to incidents that may have potentially been harmful otherwise. The fallback plans are backup plans to the contingency plans, further building on the foundation of preparation. Tools such as the Risk Register and Top Ten Table will be used to keep track of the risks facing the project, and their severity. Utilizing a quantitative analysis, risks will be ranked within these tools based on impact and probability. Having this ranking system in place allows for effective risk mitigation strategies. On top of utilizing the plans and tools, the team will regularly participate in risk management activities to help identify risk. These activities include brainstorming sessions and interviews with both internal and external consultants.

# Roles and Responsibilities

Several roles and responsibilities must be assigned and specified in order to provide accountability. To begin with, there are responsibilities that should only be assigned to those with the authority to uphold them. When assigning the responsibility of ensuring the overall success of the Risk Management Plan, the Project Manager is the most appropriate role with the authority to complete the primary tasks necessary to accomplish this goal. These tasks include keeping track and managing all project issues related to risk management activities, ensuring all available information is accessible to the team, communicating issues and problems as they arise, and managing other to ensure they are fulfilling their responsibilities. Some of the individual responsibilities that can be given to the project team collectivity consist of activities such as identifying and assessing risks, identifying risk mitigation steps and reporting. Team members assigned to assessing risks must identify the probability and impact of each risk through the use of tools such as a threat matrix. Those assigned to identifying risk mitigation steps must describe steps that must be taken to reduce weaknesses as well as the overall impact of the risk. Last, the responsibility of reporting is comprised of sharing documentation with the manager who would then compile and create reports.

# Budget and Schedule

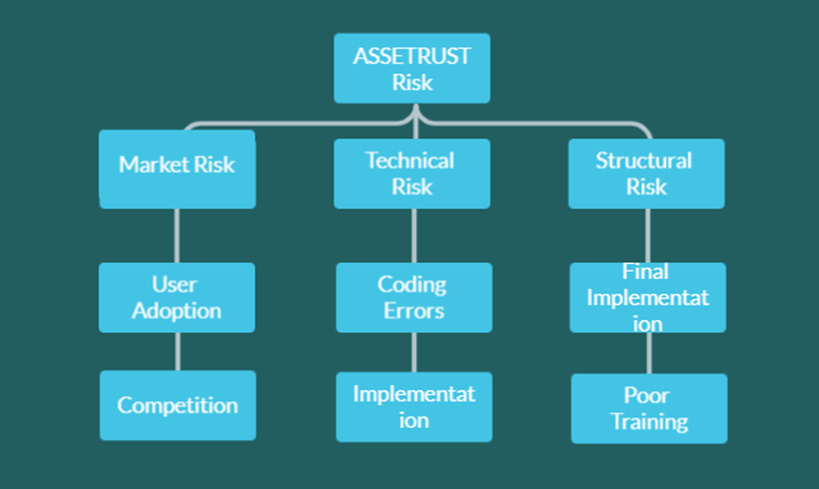
When assembling the budget for ASSETRUST’s software project, the project team identified critical sections which include labor costs, software costs including the licensing and development of the software, testing and marketing costs, reserves, and lastly annual maintenance and disaster recovery. The estimated costs for labor are $70,000, of which $30,000 is allocated to the project manager and $40,000 to the project team. A potential risk regarding labor costs could be team members working overtime because of the need to meet project deadlines. ASSETRUST would have to increase the budget to accommodate. The estimated costs for software licensing and development along with the necessary hardware are $15,000. The hardware would cost $7000, software licensing will cost $6,000 and $2000 for the development. A risk could include replacing or purchasing additional hardware due to faulty parts and damage. The testing costs are $3,500 while the marketing costs are $7,500, bringing the total to $11,000 for the wrap-up section. Additionally, the estimated costs for reserves are $15,000, of which $5,000 is separate for the management reserves and $10,000 for overall reserves. This amount will cover the risk of incidents occurring during the development phase. Lastly, the estimated costs for project maintenance, future upgrades, and disaster recovery will be $12,750. All these critical sections in the ASSETRUST budget carry the potential risk of going over the allocated amount for spending and resources for the project.

In addition to estimating the costs of the project, ASSETRUST has identified an estimated schedule for performing the critical tasks ranging from developing the actual software plan to the launch of the ASSETRUST product. Using a PERT chart, a chart to organize and schedule tasks and objectives for the project team to complete, the duration of the software project is 267 days (about 9 months). Developing the ASSETRUST software plan will take 20 days (about 3 weeks) to complete and 117 days (about 4 months) for software developers to create code for the product. There is a risk that the program developers may finish creating the code late due to employees calling off work, which would delay the code creation task to 137 days (about 4 and a half months). This risk generates another risk for the release of the Alpha version being 176 days (about 6 months) later and further the testing of the Alpha version to 199 days (about 6 and a half months). Lastly, the delayed release of the beta version will be 243 days (about 8 months), in which the beta version will proceed to the quality assurance test. A risk in this task could be the software not being compliant with the quality requirements as specified by the Quality Assurance lead. All the delays in tasks and the alteration of the quality of the product will lead to missing the deadline to launch the ASSETRUST software, which can hinder relationships with customers, partners, and stakeholders.

# Risk Categories

When defining the broad risk categories, there will be potential risk in all these categories for ASSETRUST. There is a market risk associated with the new software, as it will provide a new service. There is a risk that inexperienced users do not adopt the software as envisioned, or that a competitor comes out with a more viable solution. There is less of a financial risk, as the organization is capable of funding the project, and estimates show a viable ROI. If the project fails entirely, it will be very costly, but it will not put the company out of business. The technology risk associated with ASSETRUST is there, but through proper planning it has been determined that the project is technically feasible based on the assembled team. The technology used to implement ASSETRUST is not bleeding edge, it is more about the final functions of the software rather than the actual technology used to implement these functions. Because of this, the technology risk associated with the project is low. People risk within the company is also relatively low, as the team assembled to handle the project is fully qualified to complete the project successfully. There is a project champion and senior management has bought into the project in terms of support. The final risk category to be concerned with is the structure and process risks associated with implementing ASSETRUST. The use of the product could potentially change the day-to-day operations for certain employees significantly, meaning that training must be comprehensive. This also means that daily users of ASSETRUST must be satisfied with the result.

After analyzing the various risks associated with the creation of ASSETRUST, a basic risk breakdown structure has been created to highlight the main risk areas for the project.



# Risk Probability and Impact

The ASSETRUST Risk Register will be used to outline the probabilities and impacts of the various risks that the project potentially faces. The Risk Register also highlights the potential triggers, root causes, and potential responses for each risk. The risks are given assessments regarding potential and impact, allowing the risks to be ranked based on severity. Based on these rankings, it is clearly defined which risks have the potential to cause the most harm. The probability and impact matrix that visually shows the impact of various risks will be developed directly using the rankings from the Risk Register. All of these tools allow for the successful analysis of potential risk, allowing for the creation of an effective risk management plan.

# Tracking

The project will track risk management activities in several different ways. It is important that each member of the team is aware of all necessary documentation that must be completed. The Risk Register will be a live document that the team will reference and continue to complete as risks arise. The change request log will be used to keep track of changes to the project and when they occurred. An accurate change request log is critical to being able to stay aware of potential risks to the project. The issue log will be used to document any issues or incidents that arise. A lessons-learned register will be used to keep track of any growth opportunities that occur during the project. This could include areas that have room for improvement in the future as well as processes that worked well. This document will be available to the entire team to complete as needed. While this is most important to review at the conclusion of the project, the lessons-learned register should be filled in throughout the duration of the project. This will ensure that nothing is forgotten and the information within the register is accurate.

While the Project Manager is responsible for the success of the Risk Management Plan, the Quality Assurance Lead will be responsible for auditing the risk management processes and techniques throughout the duration of the project. The Quality Assurance Lead will also be responsible for maintaining the Top Ten Risk Item Tracking Table. This table will be used to outline the top 10 risks that the project faces. This table will be updated regularly for an accurate snapshot of the status of risks facing the project. The Top Ten Table will also allow for accurate tracking of the effectiveness of risk mitigation strategies. Mitigation strategies can be shown to be successful when a risk is removed from the table after implementation.

# Risk Documentation

Several different reports and plans make up the documentation used to keep track of all risk management activities related to the project. The contingency plan defines what actions will be taken if an incident occurs. The fallback plan takes this one step further by defining what will be done if attempts to reduce risk fail. Contingency reserves and management reserves have been budgeted for in order to proactively prepare for the consequences of incidents. Utilizing the defined actions in the risk management plans creates a structured process for the project’s response to risk. The project will also utilize change management logs to help reduce the amount of risk when changes occur.

# **Document Retention**

The Quality Management Plan and each revised version will be maintained for a minimum of three (3) years. All Corrective Action and Prevention Reports and audit findings will also be maintained for a minimum of three (3) years unless otherwise specified.

# Sponsor Acceptance

Approved by the Project Sponsor:

Date:

<Project Sponsor>

<Project Sponsor Title>