Document ID: SS-RM-PROC-001
Document Title: Risk Management Process
Version: 1.1
Status: Approved
Date: 12 August 2025

1. Introduction

1.1 Purpose

The purpose of this document is to define the standard and repeatable process for identifying, assessing, treating, and monitoring risks across all Synthetic Systems activities. This process is designed to support the achievement of strategic objectives outlined in SS-CORP-PLAN-001 by proactively managing uncertainty and enabling risk-informed decision-making.

1.2 Scope

This process applies to all programs, projects, and functional areas within Synthetic Systems. It covers all categories of risk, including but not limited to technical, schedule, cost, security, safety, and operational risks. Compliance with this process is mandatory for all personnel involved in the planning and execution of company activities.

2. References

This process is a subordinate document and should be read in conjunction with the following parent and related documents:

- **SS-CORP-PLAN-001:** Corporate Plan 2025-2028
- **SS-ENG-PLAN-001:** Engineering Management Plan
- **SS-SEC-POL-001:** Defence Security Policy

3. Roles and Responsibilities

- **Head of Operations:** Is the owner of this process and is responsible for its maintenance, review, and the overall effectiveness of the risk management framework.
- **Project/Program Manager (PM):** Is responsible for the implementation of this risk management process at the project level. This includes maintaining the Project Risk Register, ensuring risks are regularly reviewed, and reporting on risk status to senior management.
- **Risk Owner:** An individual assigned responsibility for managing a specific risk, including the development and implementation of a risk treatment plan.
- **All Personnel:** Are responsible for identifying and reporting potential risks to their

line manager or the relevant Project Manager.
- **Defence Security Committee (DSC):** As established in SS-SEC-POL-001, the DSC is responsible for the oversight of strategic and security-related risks that could impact the company's overall security posture or strategic objectives.

4. Risk Management Process

Synthetic Systems employs a continuous four-stage risk management cycle.

4.1 Step 1: Identify

Risk identification is the process of finding, recognizing, and describing risks. This is a proactive and ongoing activity. Risks can be identified from various sources, including lessons learned, brainstorming sessions, audits, technical assessments, and stakeholder consultation. All identified risks must be clearly articulated and recorded in the relevant Risk Register.

4.2 Step 2: Assess

Once identified, each risk must be assessed to determine its potential impact. This assessment involves analyzing the likelihood of the risk occurring and the consequence if it does. The assessment provides the basis for prioritizing risks for treatment. The standard 5x5 Risk Assessment Matrix in Section 5 shall be used for all assessments to ensure consistency.

4.3 Step 3: Treat

For each assessed risk, a treatment strategy must be determined and documented. The PM, in consultation with the Risk Owner and relevant stakeholders, will decide on the most appropriate course of action. The primary risk treatment options are:

- **Avoid:** Decide not to start or continue with the activity that gives rise to the risk.
- **Mitigate:** Implement controls or take actions to reduce the likelihood or consequence of the risk.
- **Transfer:** Share a portion of the risk with another party (e.g., through insurance or contractual agreements).
- **Accept:** Formally acknowledge the risk and make a conscious decision to retain it without further action, typically when the cost of treatment outweighs the potential impact.

All treatment plans must be documented in the Risk Register, including specific actions, responsibilities, and timelines.

4.4 Step 4: Monitor and Review

Risk management is a dynamic process. Risks and their treatment plans must be continuously monitored and reviewed to ensure they remain effective. Project Managers are responsible for reviewing their Project Risk Register at least monthly. The risk environment should be formally re-evaluated at key project milestones and in response to any significant changes in the project or business environment.

5. Risk Assessment Matrix

All risks shall be rated using the following tables for Likelihood and Consequence to determine an overall Risk Level.

5.1 Likelihood Levels

Level	Descriptor	Description
5	Almost Certain	Is expected to occur in most circumstances
4	Likely	Will probably occur in most circumstances
3	Possible	Might occur at some time
2	Unlikely	Could occur at some time
1	Rare	May occur only in exceptional circumstances

5.2 Consequence Levels

Level	Descriptor	Cost	Schedule	Technical/Quality	Security
5	Catastrophic	>$1M	>6 months delay	System non-functional; goal unachievable	Sustained loss of classified data; breach of national security
4	Major	$250k - $1M	3-6 months delay	Major degradation; primary objective at	Loss of sensitive data; significant

				risk	breach of policy
3	Moderate	$50k - $250k	1-3 months delay	Minor degradation; some objectives impacted	Minor loss of sensitive data; localized policy breach
2	Minor	$10k - $50k	2-4 weeks delay	Nuisance issue; performance targets still met	Minor information spillage (unclassified)
1	Insignificant	<$10k	<2 weeks delay	Negligible impact on performance	Negligible security impact

5.3 Risk Level Matrix

The overall risk level is determined by mapping the Likelihood and Consequence ratings on the matrix below.

Likelihood	**1. Insignificant**	**2. Minor**	**3. Moderate**	**4. Major**	**5. Catastrophic**
5. Almost Certain	Medium	High	High	Extreme	Extreme
4. Likely	Medium	Medium	High	High	Extreme
3. Possible	Low	Medium	Medium	High	High
2. Unlikely	Low	Low	Medium	Medium	High
1. Rare	Low	Low	Low	Medium	Medium

- **Extreme:** Immediate action required. Must be managed by senior leadership.
- **High:** Senior management attention needed. A detailed treatment plan is required.
- **Medium:** Management responsibility must be specified. Treatment plan required.
- **Low:** Manage by routine procedures. May be accepted without specific

treatment.

6. Risk Review and Acceptance

This section defines the minimum requirements for the review and acceptance of risks based on their assessed residual risk level. The residual risk is the risk level that remains after treatment measures have been implemented.

6.1 Acceptance Authority

The authority to formally accept a residual risk on behalf of the company is dependent on its severity. The following table outlines the minimum level of authority required to accept a risk at each level. Acceptance must be formally documented in the Risk Register.

Residual Risk Level	Minimum Acceptance Authority
Extreme	Chief Executive Officer (CEO)
High	Head of Operations / Defence Security Committee (DSC)
Medium	Project/Program Manager (PM)
Low	Risk Owner / Project/Program Manager (PM)

For **Extreme** and **High** level security risks, acceptance must be formally endorsed by the Defence Security Committee (DSC) before being presented to the final acceptance authority.

6.2 Review Frequency

Risks must be monitored and reviewed in accordance with their level to ensure treatment plans are effective and the risk assessment remains current. The Project Manager is responsible for ensuring these reviews occur.

- **Extreme/High Risks:** Must be formally reviewed at each quarterly Defence Security Committee (DSC) meeting, or more frequently as directed by the Head of Operations.
- **Medium Risks:** Must be reviewed at least monthly as part of standard project management reviews.
- **Low Risks:** To be reviewed as part of periodic (e.g., quarterly) project reviews or as required.

7. Risk Register

7.1 Purpose

The Risk Register is the formal repository for all identified risks and is the primary tool for managing and tracking them.

7.2 Procedure

Each project or program shall establish and maintain a Risk Register from its inception. The register shall be a controlled document, managed by the PM. The register must, at a minimum, contain the following fields for each identified risk:

- **Risk ID:** A unique identifier.
- **Date Identified:** The date the risk was first recorded.
- **Risk Description:** A clear and concise statement of the risk, including the cause and potential impact.
- **Risk Category:** (e.g., Technical, Schedule, Cost, Security).
- **Likelihood:** The likelihood rating (1-5) from the matrix.
- **Consequence:** The consequence rating (1-5) from the matrix.
- **Risk Level:** The overall risk level (Low, Medium, High, Extreme) from the matrix.
- **Risk Owner:** The single point of accountability for the risk.
- **Treatment Plan:** A description of the actions to be taken to treat the risk.
- **Status:** The current status of the risk (e.g., Open, Closed, In-Progress).
- **Last Reviewed:** The date the risk was last reviewed.

The Risk Register will be a key input into all project gate reviews and management progress reports.

8. Document Control

This is a controlled document. The official version is maintained by the Head of Operations. Any printed copies are considered uncontrolled. This document shall be reviewed biennially or as required by changes to parent policies or corporate strategy.