Document ID: SS-AUDIT-PLAN-001

Document Title: Audit Implementation Plan

Version: 1.0

Status: Approved

Date: 12 August 2025

Parent Document: SS-QM-PLAN-001: Quality Management Plan

Table of Contents

1. Introduction

1.1 Purpose

The purpose of this Audit Implementation Plan is to establish the framework and schedule for conducting regular internal and external audits within Synthetic Systems. This plan provides a structured mechanism to verify that our operations, processes, and systems comply with our own corporate standards, customer requirements, and relevant international standards. The execution of this plan is a critical component of the 'Check' phase of our Plan-Do-Check-Act cycle, as mandated by the **SS-QM-PLAN-001 Quality Management Plan**, ensuring continual improvement and the ongoing effectiveness of our management systems.

1.2 Scope

This plan applies to all departments, functions, and processes within the Synthetic Systems Quality Management System (QMS) and Information Security Management System (ISMS). This includes all activities from engineering and product development to corporate support functions and manufacturing. The procedures outlined herein are mandatory for all personnel involved in the planning, execution, and follow-up of audit activities, including auditors and auditees.

1.3 Acronyms and Definitions

- **Audit:** A systematic, independent, and documented process for obtaining objective evidence and evaluating it objectively to determine the extent to which audit criteria are fulfilled.
- **Auditee:** The department, function, or organisation being audited.
- **Auditor:** A person with the competence to conduct an audit.
- **CAPA:** Corrective and Preventive Action.
- **ISMS:** Information Security Management System.
- **ISO:** International Organization for Standardization.
- **NCR:** Non-Conformance Report.
- **OFI:** Opportunity for Improvement.
- **QMS:** Quality Management System.
- **Non-conformance:** A failure to meet a specified requirement.

2. References

- **SS-QM-PLAN-001:** Quality Management Plan
- **SS-SEC-POL-001:** Defence Security Policy
- **ISO 9001:2015:** Quality management systems — Requirements
- **ISO/IEC 27001:2022:** Information security, cybersecurity and privacy protection — Information security management systems — Requirements
- **ISO 19011:2018:** Guidelines for auditing management systems

3. Roles and Responsibilities

- **Head of Operations:** As the designated Quality Management Representative, the Head of Operations is the owner of this plan. They are responsible for ensuring sufficient resources are allocated for its execution, approving the annual audit schedule, and coordinating all external certification audits.
- **Lead Auditor:** A designated and suitably trained employee responsible for the planning, execution, and reporting of a specific internal audit. The Lead Auditor

must be independent of the area being audited.

- **Audit Team:** Personnel assigned to support the Lead Auditor in conducting an audit.
- **Auditees:** All managers are responsible for ensuring their teams are available and cooperative during scheduled audits. They are also responsible for implementing and verifying corrective actions resulting from audit findings.

4. Internal Audit Program

The internal audit program is designed to provide a comprehensive assessment of the QMS and ISMS over a twelve-month cycle. It serves as a proactive tool to identify system weaknesses, non-compliance, and opportunities for improvement before they impact product quality or security.

4.1 Annual Audit Schedule

The annual internal audit schedule is designed to review all key business functions. The schedule will be reviewed and re-issued annually by the Head of Operations. The indicative schedule is as follows:

Quarter	Focus Area	Key Documents & Processes Audited Against
Q1	**Engineering & Product Development**	SS-ENG-PLAN-001, Design & Development Processes, Configuration Management (SS-CM-PLAN-001), Risk Management (SS-RM-PROC-001)
Q2	**Corporate Functions & Support**	HR Processes (SS-HR-HNDBK-001), IT General Controls, Procurement, Document Control
Q3	**Operations & Manufacturing**	Manufacturing Procedures, Test & Evaluation (SS-TEST-PLAN-001), Product-Specific Test Procedures (e.g., SS-HYD-TEST-001), Supply Chain
Q4	**Security & Management**	Defence Security Policy

	Systems	(SS-SEC-POL-001), Classified Document Handling (SS-SEC-PROC-001), QMS & ISMS Management Review, CAPA Process

4.2 Internal Audit Process

All internal audits shall be conducted in accordance with the guidelines of ISO 19011:2018 and will follow a consistent, four-stage process:

1. **Planning:** The Lead Auditor will develop an audit plan detailing the scope, objectives, criteria, and schedule for the audit. The plan will be communicated to the auditee at least two weeks prior to the audit commencement date.
2. **Execution:** The audit team will conduct the audit through interviews, examination of records, and observation of activities. Objective evidence will be collected to verify compliance against the audit criteria. A daily wash-up meeting will be held with the auditee to discuss emerging findings.
3. **Reporting:** Within ten working days of the audit's conclusion, the Lead Auditor will issue a formal Audit Report. The report will summarise the audit activities and detail all findings, including non-conformances and opportunities for improvement. The report will be distributed to the auditee's manager, the Head of Operations, and the CEO.
4. **Follow-up & Closure:** The Lead Auditor is responsible for tracking the progress of corrective actions raised in response to audit findings. An audit is formally closed only when all resulting corrective actions have been implemented and their effectiveness has been verified.

5. Management of Audit Findings

The effective management of audit findings is crucial for driving continual improvement. All findings must be formally documented, tracked, and resolved in a timely manner.

5.1 Classification of Findings

Audit findings will be classified into one of three categories:

- **Major Non-conformance:** A significant failure to meet a requirement of the management system standard, a legal requirement, or a key corporate procedure. This could include a total breakdown of a process or a finding that could lead to the delivery of a non-conforming product or a significant security breach.
- **Minor Non-conformance:** A single observed lapse or failure to meet a

requirement that does not represent a systemic failure or pose a significant risk to the business.

- **Opportunity for Improvement (OFI):** A situation where no non-conformance exists, but a process or system could be made more efficient, effective, or robust.

5.2 Non-Conformance and Corrective Action

The handling of non-conformances is a critical output of the audit process and must be managed with rigour.

- **Reporting: All Major and Minor Non-conformances identified during an audit must be formally documented and raised on a Non-Conformance Report (NCR).** This process provides the formal mechanism for tracking and dispositioning the finding.
- **Process Adherence:** The initiation, review, and disposition of the NCR shall be conducted in strict accordance with the **Non-Conformance Reporting (NCR) process defined in Section 6.2 of SS-QM-PLAN-001: Quality Management Plan.**
- **Corrective Action:** All NCRs resulting from audit findings will trigger the Corrective and Preventive Action (CAPA) process, as detailed in Section 6.3 of SS-QM-PLAN-001. The auditee is responsible for conducting a root cause analysis and implementing an effective corrective action plan to prevent recurrence. The effectiveness of the implemented action must be verified before the NCR and the parent audit can be closed.

6. External Audit Program

Synthetic Systems is subject to regular external audits by accredited certification bodies to maintain its corporate certifications. These audits provide independent assurance to our customers and stakeholders that our management systems meet international standards. The Head of Operations is responsible for the central coordination of all external audits.

6.1 ISO 9001:2015 Quality Management

Synthetic Systems will undergo an annual external surveillance audit to maintain its certification to the ISO 9001:2015 standard. This audit will assess the ongoing compliance and effectiveness of our QMS. The scope of this audit typically covers all aspects of the business that impact product and service quality.

6.2 ISO/IEC 27001:2022 Information Security

In line with the strategic objective defined in SS-CORP-PLAN-001, Synthetic Systems will undergo an annual external surveillance audit to maintain its certification to the

ISO/IEC 27001:2022 standard. This audit assesses the effectiveness of our ISMS in protecting the confidentiality, integrity, and availability of information. The audit will be conducted with reference to the **SS-SEC-POL-001 Defence Security Policy** and its subordinate procedures.

7. Document Control

This document is a controlled document under the Synthetic Systems QMS. The official version is maintained electronically by the Head of Operations. Any printed copies are considered uncontrolled. This plan will be reviewed at least annually and updated as necessary to reflect changes in our processes, objectives, or regulatory requirements.