					Insert Registered Legal Entity Name Here							
Document number: P33S					Document Title: **Audit and Compliance Monitoring Policy**							
Version: 1.0		Effective Date: 01.01.2025			Document Owner:							
X	Policy		Standard		Procedure		Form		Register		Other	

Revision history				
Revision number	**Revision Date**	**Changes**	**Reviewed by**	**Process owner**

Approvals			
Name	**Title**	**Date**	**Signature**

Aligned with standards and regulations

Standard/Regulation	Clause/Article	Comment
ISO/IEC 27001:2022	Clauses 9.2, 10	Internal audits, continual improvement, and remediation of nonconformities
ISO/IEC 27002:2022	Controls 5.35, 5.37	Scheduled internal reviews and independent reviews for outsourced processes
NIST SP 800-53 Rev.5	CA-2, CA-7, AU-6	Security assessments, continuous monitoring, and audit review, analysis, and reporting
EU GDPR	Articles 24 and 32	Auditing technical and organizational measures and evidencing control effectiveness
EU NIS2	Article 21(2)(f)	Proactive review and evidence-based compliance
EU DORA	Article 10	ICT risk management, monitoring, and reporting
COBIT 2019	MEA01, MEA03	Monitoring and conformance assessment, compliance, and readiness for third-party reviews

1. Purpose

1.1 This policy establishes the organization's approach to conducting internal audits, security control reviews, and compliance monitoring. It ensures that all controls, policies, systems, and service providers are subject to regular and structured review.

1.2 The purpose is to identify control failures, prevent non-compliance, and demonstrate due diligence under ISO/IEC 27001, GDPR, and related frameworks.

1.3 It enables SMEs to maintain operational control and audit readiness, even without a dedicated compliance function, by using simple, repeatable checklists and risk-prioritized audit findings.

2. Scope

2.1 This policy applies to:

2.1.1 All internal departments and external vendors with responsibilities related to IT systems, personal data, and business-critical services

2.1.2 All controls and systems within the scope of the Information Security Management System (ISMS)

2.1.3 All internal audits, security control reviews, and compliance checks, whether performed internally or by an external consultant, client, or regulator

2.2 This policy also applies to evidence collection and reporting for:

2.2.1 ISO/IEC 27001 certification audits and recertification audits

2.2.2 Data protection audits under GDPR or contractual terms

2.2.3 Client-driven security questionnaires or due diligence reviews

2.2.4 Any regulatory or independent reviews under NIS2 or DORA, where applicable

3. Objectives

3.1 Ensure that all key controls and policies are regularly reviewed for effectiveness and compliance.

3.2 Maintain audit trail records and corrective action records to demonstrate accountability and continual improvement.

3.3 Prepare for certification, recertification, and customer assurance programs (e.g., ISO 27001, supplier onboarding).

3.4 Identify gaps early to enable prompt remediation before issues escalate or result in breaches of obligations.

3.5 Enable the General Manager and IT Support Provider to coordinate reviews with minimal complexity while ensuring defensible audit results.

4. Roles and Responsibilities

4.1 General Manager (GM)

4.1.1 Oversees the audit programme

4.1.2 Approves internal review plans and audit findings

4.1.3 Assigns and tracks corrective actions

4.1.4 Authorizes the engagement of external auditors or consultants

4.2 IT Provider / Administrator

4.2.1 Provides evidence during internal and external audits (e.g., logs, configurations, access control records)

4.2.2 Assists with technical checks (e.g., backup status, patch compliance)

4.2.3 Maintains the audit evidence repository

[... Sections 4.3–8 are not included in this preview. Purchase the full document to access the complete policy content. ...]

9. Review and Update Requirements

9.1 Annual Policy and Audit Plan Review

9.1.1 The General Manager (GM) must review this policy and the audit schedule at least annually.

9.1.2 The review must evaluate:

9.1.2.1 The effectiveness of audits in identifying gaps

9.1.2.2 The completion rate of audits and corrective actions

9.1.2.3 Changes in applicable legal, regulatory, or certification requirements

9.2 Trigger-Based Updates

9.2.1 The policy must be reviewed and updated when:

9.2.2 A certification audit or surveillance audit results in a major nonconformity

9.2.3 Legal or regulatory frameworks change (e.g., new GDPR guidance, national implementation of NIS2)

9.2.4 Business changes affect systems, processes, or vendors included within the audit scope

9.2.5 A critical incident or data breach reveals previously undetected control gaps

9.3 Documentation of Updates

9.3.1 All revisions must be tracked in a policy version control log

9.3.2 Updates must be distributed to all team members involved in audits

9.3.3 A summary of changes must be included with the updated policy to ensure understanding

10. Related Policies and Linkages

10.1 This policy is supported by, and reinforces, several other SME policies:

10.1.1 P1S – Information Security Policy: Establishes the baseline for all control expectations and requires verification through audits.

10.1.2 P2S – Governance Roles and Responsibilities Policy: Establishes accountability for audit planning, execution, and ownership of corrective actions.

10.1.3 P6S – Risk Management Policy: Identifies control weaknesses uncovered in audits and ensures that audit findings are documented in the risk register.

10.1.4 P17S – Data Protection and Privacy Policy: Defines GDPR controls that must be audited, including data handling, breach response, and privacy notices.

10.1.5 P22S – Logging and Monitoring Policy: Provides the audit logs and forensic data used during compliance and control reviews.

10.1.6 P30S – Incident Response Policy: Requires periodic audit of incident records and post-event reviews to verify response effectiveness.

10.1.7 P31S – Evidence Collection and Forensics Policy: Provides procedures for collecting verifiable chain-of-custody evidence during audits.

10.2 Together, these policies create a closed-loop control environment that enables internal verification, external assurance, and standards-aligned governance.

11. Reference Standards and Frameworks

11.1 ISO/IEC 27001:

11.1.1 Clause 9.2 – Requires internal audits to evaluate the performance of the Information Security Management System (ISMS) and its alignment with requirements.

11.1.2 Clause 10.1 – Requires continual improvement based on audit results and remediation of nonconformities.

11.2 ISO/IEC 27002:

11.2.1 Control 5.35 – Requires scheduled internal reviews of controls and processes.

11.2.2 Control 5.37 – Emphasizes independent reviews, particularly for outsourced processes.

11.3 NIST SP 800-53 Rev.5:

11.3.1 CA-2 – Security Assessments: Requires audits of implemented controls to verify effectiveness.

11.3.2 CA-7 – Continuous Monitoring: Emphasizes proactive detection and review of control weaknesses.

11.3.3 AU-6 – Audit Review, Analysis, and Reporting: Requires regular analysis and resolution of audit logs and audit findings.

11.4 EU GDPR:

11.4.1 Articles 24 and 32 – Require the implementation and auditing of technical and organizational measures, including evidence of control effectiveness and improvement over time.

11.5 EU NIS2 Directive (2022/2555):

11.5.1 Articles 20–21 – Require proactive control review, evidence-based compliance, and auditability for essential and important entities.

11.6 COBIT 2019:

11.6.1 MEA01 – Monitor, Evaluate and Assess Performance and Conformance: Requires periodic assessment of process and control performance against standards and objectives.

11.6.2 MEA03 – Ensure Compliance with External Requirements: Focuses on internal monitoring and readiness for third-party audits and regulatory reviews.