			[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 where applicable		
Standard/Regulation	**Clause/Article**	**Comment**
ISO/IEC 27001:2022	Clauses 9.2, 10.1	
ISO/IEC 27002:2022	Controls 5.35, 5.37	
NIST SP 800-53 Rev.5	CA-2, CA-7, AU-6	
EU GDPR	Articles 24 and 32	
EU NIS2	Article 21(2)(f)	
EU DORA	Article 10	
COBIT 2019	MEA01, MEA03	

					[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

1. **Purpose**

1.1. This policy establishes the organization's approach to performing internal audits, security control checks, and regulatory 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 detect 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 certification readiness, even without a dedicated compliance department, by using simple, repeatable checklists and risk-prioritized findings.

2. **Scope**

2.1. This policy applies to:

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

2.1.2. All controls and systems under 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 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 all key controls and policies are regularly reviewed for effectiveness and compliance.

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

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

3.4. Identify gaps early, enabling prompt remediation before issues escalate or breach obligations.

3.5. Empower the General Manager and IT provider to coordinate reviews with minimal complexity while ensuring defensible outcomes.

4. **Roles and Responsibilities**

4.1. **General Manager (GM)**

4.1.1. Oversees the audit program

4.1.2. Approves internal review plans and findings

4.1.3. Assigns and tracks corrective actions

[…..]

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**: Sets the baseline for all control expectations and requires enforcement through audits.

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

10.1.3. **P6S – Risk Management Policy**: Identifies control weaknesses uncovered in audits and ensures that 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**: Supplies 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 the procedures for gathering 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

ISO/IEC 27001:2022

Clause 9.2 – Requires internal audits to evaluate the ISMS's performance and alignment with requirements.

Clause 10.1 – Mandates continual improvement based on audit results and nonconformity remediation.

ISO/IEC 27002:2022

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

Control 5.37 – Emphasizes independent reviews, especially for outsourced processes.

NIST SP 800-53 Rev.5

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

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

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

EU GDPR

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

EU NIS2 Directive (2022/2555)

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

COBIT 2019

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

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