				[Insert Registered Legal Entity Name Here]							
Document number: P33				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, 9.3, 10.1	
ISO/IEC 27002:2022	Controls 5.35–5.37	
NIST SP 800-53 Rev.5	CA-2, CA-5, CA-7	
EU GDPR	Articles 24, 32, 33	
EU NIS2	Article 21(2)(g), Article 27	
EU DORA	Articles 10(2)(e), 25	
COBIT 2019	MEA01, MEA03	

				[Insert Registered Legal Entity Name Here]							
Document number: P33				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. The purpose of this policy is to establish and govern the organization’s audit and compliance monitoring program to:
      1.1.1. Validate the effectiveness of security and privacy controls
      1.1.2. Ensure alignment with applicable standards, legal frameworks, and contractual obligations
      1.1.3. Detect nonconformities, inefficiencies, and compliance risks in a timely manner
      1.1.4. Support continual improvement and readiness for certifications, assessments, and regulatory reviews
   1.2. This policy supports the integrity and maturity of the Information Security Management System (ISMS) by embedding structured, risk-driven, and evidence-based auditing and monitoring practices.
2. **Scope**
   2.1. This policy applies to all:
      2.1.1. Internal business units, functions, and departments
      2.1.2. Physical facilities, cloud environments, SaaS platforms, and outsourced services
      2.1.3. Information systems, applications, infrastructure, and data assets governed by the ISMS
      2.1.4. Employees, contractors, and third-party service providers with audit or compliance obligations
   2.2. The policy covers:
      2.2.1. Internal audits
      2.2.2. External/certification audits
      2.2.3. Technical compliance monitoring
      2.2.4. Supplier and third-party audits
      2.2.5. Corrective and preventive actions (CAPA)
      2.2.6. Metrics, dashboards, and reporting processes
   2.3. It applies to all relevant frameworks the organization is subject to, including ISO/IEC 27001, GDPR, NIS2, DORA, and SOC 2, among others.
3. **Objectives**
   3.1. To verify the adequacy and effectiveness of implemented controls, policies, and procedures across the ISMS and related environments.
   3.2. To identify and remediate any deficiencies, nonconformities, or compliance gaps before they escalate into incidents or violations.
   3.3. To ensure sustained readiness for internal governance reviews, external audits, and independent certifications.
   3.4. To generate defensible evidence and audit trails in support of regulatory inquiries, legal processes, or customer assurance requests.
   3.5. To integrate audit results into the organization’s broader risk management, security metrics, and continual improvement activities.
4. **Roles and Responsibilities**
   4.1. **Internal Audit Lead / Compliance Manager**
      4.1.1. Plans, schedules, and executes internal audits based on risk priority.

4.1.2. Maintains the Audit Register, coordinates audit activities, and follows up on corrective actions.

4.2. **Chief Information Security Officer (CISO)**

4.2.1. Ensures audit scope covers all relevant ISMS elements and Annex A controls.

[….]

11. Reference Standards and Frameworks

This policy is aligned with global standards and legal requirements for auditing and continuous compliance validation.

ISO/IEC 27001:2022

Clause 9.2 – Internal Audit: Requires regular, risk-based audits of the ISMS to evaluate effectiveness and conformance.

Clause 9.3 – Management Review: Audit outcomes must feed into strategic review and improvement.

Clause 10.1 – Nonconformity and Corrective Action: Audit findings must be addressed through documented CAPA procedures.

ISO/IEC 27002:2022 – Controls 5.35–5.37

Annex A Controls 5.35–5.37: Cover independent review, compliance with legal/contractual requirements, and audit logging.

Provide implementation guidance for planning, executing, and improving audit and compliance programs.

NIST SP 800-53 Rev.5

CA-2 – Control Assessments: Requires routine review of implemented security controls.

CA-5 – Plan of Action and Milestones (POA&M): Aligns with tracking and remediating audit findings.

CA-7 – Continuous Monitoring: Supports proactive, automated compliance assessments.

EU GDPR (2016/679)

Articles 24 & 32: Mandate evidence of security control implementation and effectiveness through appropriate governance structures.

Article 33: Supports the need for verified audit trails in breach response and notification.

EU NIS2 Directive (2022/2555)

Article 21(2)(g): Requires auditing of policies and procedures as part of minimum cybersecurity risk management measures.

Article 27: National authorities may perform or require audits for essential and important entities.

EU DORA (2022/2554)

Article 10(2)(e): Entities must perform internal and external audits of ICT risk management practices.

Article 25 – Audit Requirements: Mandates periodic audits by internal or independent external auditors with regulatory visibility.

COBIT 2019

MEA01 – Monitor, Evaluate and Assess Performance and Conformance: Ensures control effectiveness is verified and reported to governance bodies.

MEA03 – Monitor, Evaluate and Assess Compliance: Requires alignment of organizational practices with legal, contractual, and standards-based requirements.