					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

Standard/Regulation	Clause/Article	Comment
ISO/IEC 27001:2022	Clauses 9.2, 9.3, 10	
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), 27	
EU DORA	Articles 10(2)(e), 25	
COBIT 2019	MEA01, MEA03	

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-based, 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, IT 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 This policy covers:

2.2.1 Internal audits

2.2.2 External and 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, monitoring dashboards, and reporting processes

2.3 This policy applies to all relevant frameworks to which the organization is subject, 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 deficiencies, nonconformities, or compliance gaps before they escalate into incidents or violations.

3.3 To ensure sustained audit readiness for internal governance reviews, external audits, and independent certifications.

3.4 To generate defensible evidence and an audit trail in support of regulatory inquiries, legal proceedings, 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 priorities.

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

4.2.2 Oversees CAPA verification and integrates audit results into the security program.

[... 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 This policy shall be reviewed at least annually by the Compliance Manager and CISO, or sooner in response to:

9.1.1 Changes in regulatory, contractual, or certification frameworks

9.1.2 Significant audit findings or recurring control failures

9.1.3 Organizational restructuring or changes to GRC systems

9.1.4 External auditor recommendations or regulator feedback

9.2 The review process shall assess:

9.2.1 Audit planning methodology and frequency

9.2.2 Changes in the ISMS scope or IT infrastructure

9.2.3 Updates to the control catalog or legal register

9.2.4 Consistency and quality of audit evidence and CAPA processes

9.3 All policy changes shall be:

9.3.1 Documented in a version-controlled repository

9.3.2 Approved by Top Management

9.3.3 Communicated to all affected personnel and integrated into updated procedures and awareness programs

9.4 Post-review validation shall confirm that updated requirements are reflected in the Audit Register, compliance tools, and internal monitoring dashboards.

10. Related Policies and Linkages

10.1 This policy aligns with the following related organizational policies:

10.1.1 P1 – Information Security Policy: Defines the ISMS and establishes accountability for compliance and continual improvement

10.1.2 P5 – Change Management Policy: Ensures audit visibility into IT infrastructure and configuration changes affecting control environments

10.1.3 P6 – Risk Management Policy: Integrates audit results into enterprise risk evaluation and treatment activities

10.1.4 P14 – Data Retention and Disposal Policy: Governs retention of audit evidence, logs, and compliance records

10.1.5 P18 – Cryptographic Controls Policy: Supports secure storage and transfer of sensitive audit data

10.1.6 P26 – Third-Party and Supplier Security Policy: Covers audit rights, assurance documentation, and vendor compliance oversight

10.1.7 P30 – Incident Response Policy: Aligns audits of incident handling processes with ISMS assurance objectives

10.1.8 P32 – Business Continuity and Disaster Recovery Policy: Requires verification of continuity testing and disaster recovery plan (DRP) compliance during audit cycles

11. Reference Standards and Frameworks

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

11.2 ISO/IEC 27001:

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

11.2.2 Clause 9.3 – Management Review: Audit results shall inform strategic review and improvement.

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

11.3 ISO/IEC 27002:2022 – Controls 5.35–5.37:

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

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

11.4 NIST SP 800-53 Rev.5:

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

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

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

11.5 EU GDPR (2016/679):

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

11.5.2 Article 33: Supports the need for a verified audit trail in breach response and notification.

11.6 EU NIS2 Directive (2022/2555):

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

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

11.7 EU DORA (2022/2554):

11.7.1 Article 10(2)(e): Requires entities to perform internal and external audits of ICT risk management practices.

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

11.8 COBIT 2019:

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

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