					Insert Registered Legal Entity Name Here							
Document number: P06					Document Title: **Risk Management 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 6.1, 8.32, 10	Core requirements for risk identification and management, integration with change management, and continual improvement
ISO/IEC 27005:2024	Full risk lifecycle methodology	End-to-end risk management process aligned with the standard
ISO 31000:2018	Risk management principles and framework	Risk management principles adopted within the framework
NIST SP 800-30 Rev.1	SP 800-30, SP 800-39	Guidance and structure for risk assessments and tiered risk governance
EU GDPR	Articles 24, 25, 32	Data protection risk processes and controls
EU NIS2	Article 21(2)(a–d)	Risk and security assessment obligations
EU DORA	Articles 5, 6	ICT risk management and operational resilience
COBIT 2019	APO12, MEA	Risk management structure and oversight

1. Purpose

1.1 This policy establishes a unified and formalized framework for identifying, analyzing, evaluating, treating, monitoring, and reviewing information security risks across the organization.

1.2 It ensures the consistent application of risk-based principles to protect the Confidentiality, Integrity, and Availability of information assets, in line with ISO/IEC 27001:2022 Clause 6.1 and ISO 31000:2018.

1.3 This policy embeds information security risk management into organizational decision-making processes to support internal strategic objectives and external regulatory requirements.

2. Scope

2.1 This policy applies to all organizational units, business processes, systems, personnel, and third-party engagements involved in the handling, development, storage, or management of information assets.

2.2 The scope extends to physical, digital, and cloud-hosted assets, including structured and unstructured data, applications, IT infrastructure, networks, and services.

2.3 It covers information security risks at the strategic, operational, project, and technical levels and is mandatory for all personnel, contractors, and service providers engaged in Information Security Management System (ISMS) activities.

2.4 Risk management shall be applied to the following scenarios:

2.4.1 New project or system implementation

2.4.1.1 Significant changes (e.g., architecture, ownership, processes)

2.4.1.2 Supplier onboarding and third-party agreements

2.4.1.3 Incident response and post-incident reviews

2.4.1.4 Periodic organizational risk reviews or audits

3. Objectives

3.1 To establish and operationalize a repeatable, organization-wide risk management process based on ISO/IEC 27005 and ISO 31000 methodologies.

3.2 To ensure that risks are identified, analyzed, evaluated, and treated using structured and traceable methods, including the assignment of risk ownership and control mappings.

3.3 To maintain a centralized, version-controlled Risk Register and Risk Treatment Plan reflecting current risk status, control coverage, and mitigation progress.

3.4 To align risk decisions with documented risk appetite and tolerance levels and enable informed governance decisions regarding risk acceptance, mitigation, transfer, or avoidance.

3.5 To continuously monitor risk trends and ensure the effectiveness of risk treatments while enabling proactive adjustments based on evolving threats or business change.

4. Roles and Responsibilities

4.1 Top Management / Board of Directors

4.1.1 Approves the risk management framework and defines acceptable risk appetite and tolerance thresholds.

4.1.2 Authorizes risk treatment strategies for residual risks that exceed tolerance.

4.1.3 Allocates resources and provides oversight for the effective operation of the risk management program.

4.2 ISMS Manager / Risk Officer

4.2.1 Owns this policy and maintains its alignment with ISO/IEC 27001 and ISO/IEC 27005.

4.2.2 Leads the enterprise risk assessment process and maintains the Risk Register and Risk Treatment Plan.

4.2.3 Ensures periodic reviews and escalation of key risks to Top Management or the ISMS Steering Committee.

[... 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 and its associated framework shall be reviewed annually, or:

9.1.1 Following a major risk event or security incident

9.1.2 Following significant organizational or technical change

9.1.3 In response to audit findings or new regulatory requirements

9.2 The ISMS Manager, Risk Officer, and Compliance Team are jointly responsible for:

9.2.1 Initiating the review cycle

9.2.2 Collecting input from business units

9.2.3 Revising procedures and thresholds as required

9.3 All revisions shall be:

9.3.1 Version-controlled and logged

9.3.2 Approved by Top Management

9.3.3 Communicated to stakeholders

9.3.4 Retained in the audit repository for a minimum of 5 years

10. Related Policies and Linkages

10.1 This policy is interdependent with the following information security policies:

10.1.1 P1 – Information Security Policy: Establishes the overall security governance model under which this risk policy operates.

10.1.2 P2 – Governance Roles and Responsibilities Policy: Defines accountable owners and governance tiers referenced in the risk escalation matrix.

10.1.3 P5 – Change Management Policy: Triggers risk reassessment for IT infrastructure and organizational changes.

10.1.4 P13 – Data Classification and Labeling Policy: Supports impact assessment during risk identification.

10.1.5 P33 – Audit and Compliance Monitoring Policy: Validates adherence to this policy, including completeness of the Risk Register and evidence of treatment actions.

11. Reference Standards and Frameworks

11.1 This policy is explicitly aligned with the following standards and frameworks to ensure that it meets international best practices and regulatory expectations for information security risk management:

11.2 ISO/IEC 27001:

11.2.1 Clause 6.1: Establishes requirements for identifying risks and opportunities, including the full lifecycle of information security risk assessment and treatment. This policy operationalizes Clause 6.1.2 and Clause 6.1.3 through a structured framework that mandates documented risk identification, analysis, evaluation, treatment, and residual risk acceptance protocols.

11.2.2 Clause 8.32: Integration of risk-based thinking into change management processes ensures that all significant organizational changes trigger formal risk reassessments.

11.2.3 Clause 10: Continual improvement is embedded through regular policy reviews, risk trend analysis, and SoA updates driven by risk insights.

11.3 ISO/IEC 27005:

11.3.1 Provides specialized and detailed guidance on information security risk management. This policy implements the full ISO/IEC 27005 risk process model: Context Establishment, Risk Identification, Risk Analysis, Risk Evaluation, Risk Treatment, Risk Acceptance, Risk Communication, Risk Monitoring, and Review.

11.4 ISO 31000:

11.4.1 This policy incorporates ISO 31000 principles such as leadership commitment, integration with decision-making, and continual improvement. It ensures that risk management is embedded in the organization’s culture and operations.

11.5 NIST SP 800-30 Rev.1:

11.5.1 Aligns with NIST guidance for conducting risk assessments, including threat identification, vulnerability analysis, likelihood estimation, and impact determination. This policy’s structure reflects NIST’s defined risk assessment steps and adapts them to both technical and business processes.

11.6 NIST SP 800-39:

11.6.1 Supports enterprise-level risk governance, emphasizing tiered risk management at the organizational, mission/business process, and information system levels. This policy ensures that risk ownership is clearly defined at all levels and includes organization-wide treatment strategies.

11.7 EU GDPR:

11.7.1 Article 24: Requires the implementation of appropriate technical and organizational measures to ensure that data protection risks are properly managed, as addressed through this policy’s structured risk process.

11.7.2 Article 25: “Data protection by design and by default” aligns with embedding risk treatment into system and process design.

11.7.3 Article 32: Mandates a risk-based approach to security measures, fulfilled through impact-based risk evaluations and control selection.

11.8 EU NIS2 Directive:

11.8.1 Article 21(2)(a–d): Requires entities to conduct risk assessments, implement policies on risk analysis, and ensure proportionate security measures. This policy addresses these obligations through continual application of the risk lifecycle and documented governance.

11.9 EU DORA:

11.9.1 Article 5: Mandates a documented ICT risk management framework, fully covered by this policy’s structure, including SoA mapping and KRIs.

11.9.2 Article 6: Requires the integration of risk management into operational resilience strategies, addressed through escalation matrices and critical asset tracking.

11.10 COBIT 2019:

11.10.1 APO12 – Manage Risk: Directly maps to the organization’s establishment of a structured risk management approach, assignment of roles, tracking of treatment actions, and Board-level accountability.

11.10.2 MEA01 – Monitor, Evaluate and Assess Performance and Conformance: Reflected in this policy’s focus on trend analysis, monitoring of KRIs, and integration of audit feedback into continual improvement activities.