					[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 where applicable		
Standard/Regulation	**Clause/Article**	**Comment**
ISO/IEC 27001:2022	Clauses 6.1, 8.32, 10	
ISO/IEC 27005:2024		Full risk lifecycle methodology
ISO 31000:2018		Risk management principles and framework
NIST SP 800-30 Rev.1		SP 800-39
EU GDPR	Articles 24, 25, 32	
EU NIS2	Article 21(2)(a–d)	
EU DORA	Articles 5, 6	
COBIT 2019	APO12, MEA01	

					[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			

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 consistent application of risk-based principles that 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 The policy embeds information security risk management into organizational decision-making processes to meet 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, infrastructure, networks, and services.

2.3 It covers information security risks at the strategic, operational, project, and technical levels, and is mandatory for all employees, contractors, and service providers engaged in ISMS activities.

2.4 Risk management must 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 assignment of risk ownership and control linkages.

3.3 To maintain a centralized and 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 threat evolution or business change.

4. Roles and Responsibilities

4.1 **Executive 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 exceeding tolerance.

4.1.3 Allocates resources and 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 27005 standards.

[…..]

11. Reference Standards and Frameworks

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

ISO/IEC 27001:2022

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

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

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

ISO/IEC 27005:2024

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

ISO 31000:2018

This policy integrates ISO 31000 principles such as leadership commitment, integration with decision-making, and continuous improvement. It ensures that risk management is embedded into the organization's culture and operations.

NIST SP 800-30 Rev.1

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

NIST SP 800-39

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

EU GDPR

Article 24: Requires implementation of appropriate technical and organizational measures to ensure data protection risks are properly managed—addressed via this policy's structured risk process.

Article 25: "Data protection by design and by default" aligns with embedding risk treatment into systems and process designs.

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

EU NIS2 Directive

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

EU DORA

Article 5: Mandates a documented ICT risk management framework—fully covered by this policy's architecture, including SoA mapping and KRIs.

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

COBIT 2019

APO12 – Manage Risk: Directly maps to the organization's establishment of a structured risk management approach, assigning roles, tracking treatments, and ensuring Board-level accountability.

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 continuous improvement loops.