					Insert Registered Legal Entity Name Here							
Document number: P06S					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, 6.1.3	
ISO/IEC 27002:2022	Controls 5.4, 5.25	
NIST SP 800-53 Rev. 5	RA-1 to RA-7, PM-9	
EU NIS2	Article 21(2)(a–d)	
EU DORA	Article 5	
COBIT 2019	APO12, MEA01	

1. Purpose

1.1 This policy defines how the organization identifies, assesses, and manages risks related to information security, operations, technology, and third-party services.

1.2 It ensures that risk management is an active component of planning, project execution, supplier selection, and incident response, in alignment with ISO 27001, ISO 31000, and applicable regulatory requirements.

1.3 This policy supports informed decision-making, the protection of information assets, and the resilience of critical business operations.

2. Scope

2.1 This policy applies to:

2.1.1 All departments, systems, and users within the organization

2.1.2 All information, services, and assets managed internally or through third parties

2.1.3 All risk-related activities, including project reviews, system upgrades, outsourcing, and regulatory compliance

2.2 It covers all types of risk, including:

2.2.1 Cybersecurity threats and system vulnerabilities

2.2.2 Operational disruptions and service outages

2.2.3 Legal, compliance, and reputational risks

2.2.4 Third-party and supply chain risks

2.3 All employees, contractors, and service providers must comply with this policy when identifying or reporting risks.

3. Objectives

3.1 Integrate simple and repeatable risk assessment procedures into routine business operations.

3.2 Identify and prioritize risks that could affect Confidentiality, Integrity, and Availability or regulatory compliance.

3.3 Assign ownership and define treatment actions for all significant risks.

3.4 Maintain an accurate and current Risk Register to support audit readiness and risk tracking.

3.5 Ensure management involvement in approving risk tolerance and major risk treatment plans.

4. Roles and Responsibilities

4.1 General Manager

4.1.1 Sets the organization's risk appetite and approves the risk management framework.

4.1.2 Approves major risk treatment decisions and the allocation of resources.

4.1.3 Reviews the highest risks quarterly with the Risk Coordinator.

4.2 Risk Coordinator (or ISMS Owner)

4.2.1 Facilitates risk assessments and maintains the Risk Register.

4.2.2 Ensures that risk scoring, ownership, and treatment actions are documented.

4.2.3 Organizes at least one formal risk review annually.

[... 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 Annual Policy Review

9.1.1 This policy must be reviewed at least annually by the General Manager and Risk Coordinator to ensure its continued relevance and completeness.

9.2 Update Triggers

9.2.1 An earlier review and update must take place if:

9.2.1.1 A major incident or audit finding reveals gaps in risk management

9.2.1.2 New business units, technologies, or partnerships are introduced

9.2.1.3 A regulatory or contractual requirement changes

9.3 Version Control

9.3.1 All updates to this policy must be version-controlled and include the following metadata:

9.3.1.1 Version number and effective date

9.3.1.2 Summary of changes

9.3.1.3 Approver (General Manager)

9.3.1.4 Archived prior versions for audit purposes

9.4 Communication and Awareness

9.4.1 Updated versions of this policy and major risk treatment plans must be communicated to affected personnel. Annual awareness training must include basic risk awareness principles.

10. Related Policies and Linkages

10.1 This policy operates in conjunction with the following policies to ensure comprehensive security governance:

10.1.1 P2S – Governance Roles and Responsibilities Policy: Defines accountability for risk ownership and decision-making.

10.1.2 P5S – Change Management Policy: Requires a risk assessment before implementing technical or process changes.

10.1.3 P17S – Data Protection and Privacy Policy: Addresses regulatory risk associated with the handling of personal data.

10.1.4 P30S – Incident Response Policy: Ensures that risk treatment continues during and after security incidents.

10.1.5 P33S – Business Continuity Policy: Identifies residual risks and recovery measures for critical services.

11. Reference Standards and Frameworks

11.1 ISO/IEC 27001:

11.1.1 Clause 6.1 – Establishes a formal risk management process and treatment planning requirements.

11.1.2 Clause 6.1.3 – Requires organizations to retain documented treatment plans and approvals.

11.2 ISO/IEC 27002:

11.2.1 Controls 5.4 and 5.25 – Provide implementation guidance for risk ownership, prioritization, and lifecycle management.

11.3 NIST SP 800-53 Rev. 5:

11.3.1 RA-1 to RA-7 – Define risk assessment, response strategies, documentation, and review mechanisms.

11.4 PM-9 – Requires consistent management oversight of organizational risks.

11.5 EU NIS2 Directive

11.5.1 Article 21(2)(a–d) – Imposes mandatory risk assessment, mitigation, and governance controls on essential and important entities.

11.6 EU DORA

11.6.1 Article 5 – Requires regulated entities to define and manage ICT risk management frameworks, including identification, classification, and response.

11.7 COBIT 2019

11.7.1 APO12 – Manage Risk: Integrates risk into strategic and operational planning.

11.7.2 MEA01 – Monitor, Evaluate, and Assess: Ensures the effectiveness and compliance of risk processes and related actions.