					Insert Registered Legal Entity Name Here							
Document number: P02					Document Title: **Governance Roles and Responsibilities 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	Clause 5.3; Annex A Control 5	
ISO/IEC 27002:2022	Control 5	
NIST SP 800-53 Rev.5	PL-1 through PL-4, PM-1 through PM-13	
EU GDPR	Articles 5(1)(f), 24, 37	
EU NIS2	Article 21(2)(a)	
EU DORA	Article 5	
COBIT 2019	EDM01, EDM02, APO01, APO12, MEA	

1. Purpose

1.1 This policy defines the governance model, organizational roles, and responsibilities required to operate an effective Information Security Management System (ISMS).

1.2 It establishes clear lines of accountability, decision-making authority, and interdependencies and escalation paths to ensure that information security is embedded at all levels of the organization and aligned with strategic business objectives.

1.3 This policy implements the requirements of ISO/IEC 27001:2022 Clause 5.3 and Annex A Control 5.2, ensuring that responsibilities for security-related activities are clearly assigned, documented, communicated, and periodically reviewed.

1.4 This policy also provides a foundation for integrated governance with other disciplines such as risk management, compliance, IT operations, and legal.

2. Scope

2.1 This policy applies to all individuals and entities involved in the governance, operation, and oversight of information security within the ISMS scope. This includes:

2.1.1 Top Management, senior management, and Board members

2.1.2 The ISMS Manager, CISOs, and Control Owners

2.1.3 Process Owners and Asset Owners

2.1.4 Contractors and Third-Party Service Providers with delegated security responsibilities

2.2 It covers both internal and externally sourced functions (e.g., outsourced SOC, cloud platform administrators) where governance roles are formally assigned or contractually defined.

2.3 This policy also applies to organizational units, departments, and project teams that manage or influence security-relevant assets, systems, or services.

3. Objectives

3.1 To ensure that information security roles and responsibilities are formally defined, assigned, communicated, and documented.

3.2 To maintain a governance model that enforces segregation of duties, eliminates conflicts of interest, and enables escalation of unresolved security issues.

3.3 To ensure accountability and authority for security decisions are assigned in alignment with business impact and organizational structure.

3.4 To establish a framework for managing delegations, role changes, and the review of assigned responsibilities.

3.5 To provide assurance to stakeholders, including regulators, auditors, and clients, that information security is governed effectively and in compliance with applicable standards.

4. Roles and Responsibilities

4.1 Executive Management (Top Management)

4.1.1 Provides strategic oversight, allocates resources, and ensures alignment between ISMS objectives and business goals.

4.1.2 Approves major ISMS documentation, including the Information Security Policy, risk treatment plans, and audit remediation decisions.

4.1.3 Participates in ISMS management reviews and escalates decisions requiring Board-level approval.

4.1.4 Champions a culture of security and promotes organizational adherence to security governance principles.

4.2 Information Security Steering Committee (ISSC)

4.2.1 Acts as the cross-functional coordination body for ISMS oversight.

4.2.2 Reviews risk posture, control performance, audit findings, and strategic security initiatives.

4.2.3 Facilitates coordination among departments (e.g., IT, Legal, HR, Risk, Compliance, Operations).

4.2.4 Approves escalation thresholds, budget allocations, and policy changes requiring executive input.

[... 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 Review Schedule

9.1.1 This policy shall be reviewed at least annually or upon the occurrence of:

9.1.1.1 Changes to the organizational structure or executive team

9.1.1.2 Expansion or redefinition of the ISMS scope

9.1.1.3 Regulatory changes affecting role assignment or oversight

9.1.1.4 Significant audit findings or incidents involving governance failure

9.2 Review and Approval Process

9.2.1 The ISMS Manager shall initiate and lead the review process, including the collection of stakeholder input and audit feedback.

9.2.2 Proposed updates shall be reviewed by the ISSC and formally approved by Executive Management.

9.2.3 Each version shall be tracked in the ISMS Document Register and shall include the following metadata:

9.2.3.1 Policy ID and title

9.2.3.2 Version number and change summary

9.2.3.3 Effective date and next review date

9.2.3.4 Policy owner and approver

9.2.3.5 Document classification level

9.2.3.6 Retention and archival history

10. Related Policies and Linkages

10.1 This policy shall be read in conjunction with the following policies:

10.1.1 P1 – Information Security Policy: Establishes the overall security program and outlines leadership responsibilities for policy endorsement and strategic oversight.

10.1.2 P5 – Change Management Policy: Ensures that changes to governance structures, roles, or responsibilities are subject to documented approval and risk review.

10.1.3 P6 – Risk Management Policy: Identifies and addresses governance risks arising from role conflicts, unassigned duties, or lack of escalation.

10.1.4 P7 – Onboarding and Termination Policy: Enforces control assignment and revocation processes during personnel lifecycle changes.

10.1.5 P33 – Audit and Compliance Monitoring Policy: Supports independent review of governance effectiveness and enforces corrective actions for non-compliance.

10.2 These policies collectively support a unified and enforceable ISMS governance framework.

11. Reference Standards and Frameworks

11.1 This policy aligns with globally recognized standards and frameworks for information security governance and role accountability. It ensures traceability to regulatory and certification requirements and supports a defensible ISMS structure.

11.2 ISO/IEC 27001

11.2.1 Clause 5.3 – Organizational Roles, Responsibilities and Authorities: This policy fulfills the requirement that roles relevant to information security be clearly assigned, communicated, and documented.

11.2.2 Clause 9.3 – Management Review: This policy enforces executive oversight of ISMS roles and governance through quarterly and annual reviews.

11.2.3 Annex A Control 5.2 – Information Security Roles and Responsibilities: Defines roles across technical, operational, and strategic levels to ensure segregation of duties, risk ownership, and traceable accountability.

11.3 ISO/IEC 27002:2022 – Control 5

11.3.1 Provides implementation guidance for assigning information security responsibilities across an organization. This policy adopts that guidance by defining role types, delegation rules, escalation procedures, and review mechanisms.

11.4 NIST SP 800-53 Rev.5

11.4.1 PL-1 through PL-4: Require formal planning documentation, including policies that define governance and assign security responsibilities.

11.4.2 PM-1 (Information Security Program Plan) and PM-2 (Senior Information Security Officer): Reflected in this policy through the assignment of the CISO/ISMS Manager and formal governance roles.

11.4.3 PM-5 through PM-13: This policy addresses requirements for role documentation, enterprise-wide risk roles, configuration management oversight, and integration with mission and business functions.

11.5 EU GDPR (2016/679)

11.5.1 Article 5(1)(f): Requires personal data to be protected against unauthorized or unlawful processing. This policy ensures that individuals responsible for data protection are clearly designated and monitored.

11.5.2 Article 24: Requires appropriate organizational measures, including governance structures.

11.5.3 Article 37: Requires designation of a Data Protection Officer (DPO), which shall be reflected in the organization's governance framework and Roles and Responsibilities Register.

11.6 EU NIS2 Directive (2022/2555)

11.6.1 Article 21(2)(a): Requires entities to implement policies on risk analysis and information system security, including role-specific responsibilities. This policy defines such roles and their governance mechanisms.

11.7 EU DORA (2022/2554)

11.7.1 Article 5 – Governance and Internal Control Framework: Requires formal assignment of ICT risk management responsibilities, decision-making roles, and reporting channels. This policy provides the basis for governance of security-related roles in ICT environments.

11.8 COBIT 2019

11.8.1 EDM01 – Ensured Governance Framework Setting: This policy ensures that the ISMS has a clearly defined governance structure aligned with enterprise needs.

11.8.2 EDM02 – Ensured Benefits Delivery: Aligns role-based security activities with strategic and operational objectives, ensuring accountability and measurable outcomes.

11.8.3 APO01 – Managed I&T Management Framework and APO12 – Managed Risk: This policy supports the structured management of information security roles within a broader IT governance and risk framework.

11.8.4 MEA01 – Monitor, Evaluate and Assess Performance: Embeds review mechanisms for verifying that governance roles are effective, current, and enforced.