Statement of Applicability (SoA)

Purpose

The Statement of Applicability (SoA) defines the set of security controls selected from ISO/IEC 27001:2022 Annex A that are applicable to the organization’s Information Security Management System (ISMS).

Basis for Control Selection

The selection of controls is based on:

- Business and operational requirements
- Regulatory and contractual obligations
- Results of the information security risk assessment
- Expectations of interested parties

Control Applicability

Each control from Annex A is evaluated and marked as either:

- Applicable – Control is required and implemented
- Not Applicable – Control is excluded with documented justification

Implementation Approach

Applicable controls are implemented through:

- Information security policies
- Technical safeguards (e.g., access control, encryption)
- Operational procedures and monitoring mechanisms

Governance and Maintenance

The SoA is reviewed periodically and updated whenever:

- New risks are identified
- Significant business or technology changes occur
- Regulatory or contractual requirements change

Role in Certification

The SoA serves as a key reference document for:

- ISO/IEC 27001 certification audits
- Internal audits and management reviews
- Demonstrating alignment between risk treatment and control implementation