Statement of Applicability (SoA) – Explanation

Overview

The Statement of Applicability (SoA) is a mandatory document required under ISO/IEC 27001:2022. It provides a summary of the information security controls selected by the organization and explains why each control is relevant or excluded.

Inputs to the SoA

The SoA is prepared using the following inputs:
- Business objectives and operational context
- Regulatory and legal compliance requirements
- Results of the information security risk assessment
- Contractual obligations with customers and partners

Control Justification

For each Annex A control, the organization documents:
- Whether the control is applicable
- The justification for inclusion or exclusion
- The reference to implemented policies or procedures

Relationship with Risk Treatment Plan

The SoA aligns directly with the Risk Treatment Plan (RTP). Controls selected in the SoA correspond to the treatment actions defined for identified risks.

Audit and Compliance Support

The SoA is used by internal and external auditors to verify:
- That appropriate controls have been selected
- That risk treatment decisions are justified
- That control implementation matches documented policies

Continuous Improvement

The SoA is a living document and is updated as part of the organization's continuous improvement process to ensure ongoing effectiveness of the ISMS.