Statement of Applicability (SoA) – Explanation

1. Overview

The Statement of Applicability (SoA) is a mandatory document under ISO/IEC 27001:2022. It identifies which Annex A controls are applicable to the organization's Information Security Management System (ISMS) and provides justification for their inclusion or exclusion.

2. Purpose of the SoA

The primary purpose of the SoA is to demonstrate how identified information security risks are addressed through appropriate controls. It ensures transparency in control selection and supports audit and certification activities.

3. Basis for Control Selection

Controls are selected based on:
- Results of the risk assessment and risk register
- Business and operational requirements
- Legal, regulatory, and contractual obligations
- Expectations of interested parties such as customers and regulators

4. Control Applicability

Each Annex A control is evaluated and marked as:
- Applicable (Y) – The control is relevant and implemented or planned
- Not Applicable (N) – The control is not relevant, with documented justification

5. Implementation Status

The SoA also indicates the current status of each control:
- Implemented – Control is fully deployed and operational
- Partial – Control is implemented but requires improvement
- Planned – Control is scheduled for future implementation

6. Relationship with Risk Treatment Plan

The SoA is directly linked to the Risk Treatment Plan (RTP). Controls selected in the SoA correspond to treatment actions defined for identified risks, ensuring alignment between risk management and control implementation.

7. Role in Audits and Certification

The SoA is used by internal and external auditors to verify that:
• Appropriate controls have been selected
• Justifications are valid and documented
• Implemented controls match policies and procedures

8. Review and Maintenance

The SoA is a living document and is reviewed periodically or when significant changes occur, such as:
• Introduction of new systems or services
• Changes in regulatory requirements
• Identification of new risks

9. Conclusion

The Statement of Applicability provides a clear link between organizational risks and selected controls, supporting effective ISMS operation and continuous improvement.