# ISO 27001 Statement of Applicability (SoA) Template

## Introduction:

This document provides the ISO 27001 Statement of Applicability (SoA) template, listing controls selected from ISO 27001. The SoA includes their applicability, justification for inclusion or exclusion, implementation status, and references. This document supports [COMPANY NAME]'s commitment to managing information security risks and achieving ISMS objectives.

## 1. Purpose of the SoA

The SoA serves to:  
1. Document the controls selected from ISO 27001.  
2. Justify the inclusion or exclusion of each control based on risk assessments and business requirements.  
3. Demonstrate compliance with regulatory, legal, and contractual requirements.  
4. Provide traceability for auditors and stakeholders.  
5. Support ongoing risk management efforts.

## 2. Statement of Applicability Table Example

The table below outlines the applicability, justification, implementation status, and other relevant details for each selected control.

| Control ID | Control Description | Applicable (Yes/No) | Justification | Implementation Status | Control Owner | Linked Risk(s) | Action Plan (if needed) |
| --- | --- | --- | --- | --- | --- | --- | --- |
| A.5.1 | Information Security Policies | Yes | Ensures a consistent approach to information security. | Implemented | Compliance Officer | Lack of unified policy framework | N/A |
| A.6.1 | Organization of Information Security | Yes | Align roles with security needs. | Implemented | CISO | Undefined roles and responsibilities | N/A |
| A.12.3 | Backup | Yes | Ensure data recovery in case of incidents. | Partially Implemented | IT Manager | Loss of critical data | Complete full backup automation. |
| A.18.1 | Compliance with Legal Requirements | Yes | Fulfill statutory obligations. | Implemented | Legal Team | Failure to meet legal obligations | N/A |

---

## 3. Roles and Responsibilities

Information Security Manager (ISM):  
- Maintain and update the SoA.  
- Ensure the implementation of selected controls.

Top Management:  
- Approve the SoA.  
- Provide resources for control implementation.

Compliance Officer:  
- Ensure selected controls meet regulatory requirements.

IT Operations Team:  
- Implement and monitor technical controls.

## 4. Narrative Context

The SoA ensures [COMPANY NAME] aligns its ISMS with ISO 27001 controls. For example, the inclusion of A.12.3 (Backup) enables data recovery in case of critical incidents, demonstrating a proactive approach to mitigating data loss risks.

## 5. Revision and Maintenance

The SoA will be reviewed [Insert frequency, e.g., annually or as needed] to reflect changes in risks, business operations, or regulatory requirements.

## Approval:

| Name | Title | Date |
| --- | --- | --- |
|  |  |  |
|  |  |  |