

# Writing Statement of Applicability (SOA)

Reading

40m

✓ Status

Incomplete

## Introduction

After drafting and completing the Risk Methodology document, the Risk Assessment matrix, and the Risk Treatment/Residual Risk matrices, it's time to understand what an SOA is, why it is important, and how to complete one.

## Reading

### ISO 27001 SOA: What Is It?

Certification to ISO 27001 calls for an SOA. Essentially, it's a declaration of which security rules from Annex A apply to your organization's ISMS and which don't.

An SOA must include the following items:

- Document the risk-reducing measures that a company has decided to take.
- Defend the rationale for your ISMS's selection of these particular control measures.
- Indicate whether all controls have been set up properly.
- Provide an explanation for the exclusion of any potential controls.

One of the most often asked questions is whether or not an SOA is considered secret due to the amount of information it contains; the answer is yes. It is only appropriate to provide them to your auditor, since they are meant to be used just for internal purposes.

### Reasons Why the ISO 27001 SOA is Crucial

ISO 27001 relies heavily on its introductory paper, the SOA. It specifies which of Annex A's proposed 114 controls will be implemented and how, and which will not, along with an explanation for your decision. The need of each control is explained, as is the degree to which it has been applied.



In simple words, an SOA document shows which of the 114 controls apply to your organization.

Putting away the need for ISO 27001 certification, the SOA is still a very helpful piece of paper. Additional significance lies in your SOA in several ways:

### **It helps in implementing your data security plan.**

To be compliant with ISO 27001, an ISMS must take into consideration and record the organization's legal, regulatory, and contractual responsibilities in regards to information security. This also necessitates an in-depth explanation of why you're qualified and how you plan to achieve that goal.

You may specify the measures you're using to keep these mission-critical promises in your SOA.

By connecting your Risk Assessment and Risk Treatment strategy, it may also help you concentrate on reaching an ISMS compliance. What dangers does your company face, how will you deal with them, and what will the end result be (SOA)?

### **It acts as a roadmap for both internal and external audits, including those required for certification.**

The SOA is the primary document used by the auditor to verify that your controls perform as specified during an ISO 27001 certification audit. It will serve as the nucleus for your regular internal security audits and facilitate your compliance with mandated ISMS upgrades.

If you document all of the safeguards you've set up, you'll have a better idea of how well your current method of risk mitigation is working and if another strategy might be preferable. The need to revisit this document on a yearly basis ensures that you're keeping up with any changes in the threat environment that may necessitate a shift in approach. Perhaps the possibility of a danger you'd previously accepted has grown, prompting you to introduce a new control.

If a client ever asks, they may verify they are looking at the appropriate reference by comparing the SOA document's version number and date to the information on your ISO 27001 certificate.

### **It gives you a living record to use in keeping track of and bettering your ISMS.**

Your auditor will find many uses for the information in your SOA during the certification audit. Its primary use is to help your company track and enhance its ISMS.

A good way to think about it is as a snapshot of your company's information security policies, complete with a running list of all controls, an explanation of why they're necessary, and a rundown of how they operate. By doing so, you may assist yourself and others (such as the board and investors) comprehend the rationale for your organization's approach to Risk Management.

## **How to Write an ISO 27001 SOA**

The time has come to put together your SOA, done in six easy steps, as described below:

### **1. Recognize and Assess Threats to Your ISMS**

List all of your information assets and the potential data security risks associated with each one as part of an ISO 27001 Risk Assessment.

Following this, you may assign a risk owner, develop a strategy to address any vulnerabilities, and rank and prioritize risks based on their probability and effect. This document serves as a template for conducting a risk analysis in accordance with ISO 27001.

### **2. Define Your Risk Management Strategy**

After compiling a list of potential threats, you must now choose how to address each one. A Risk Treatment plan is a document that specifies the risks that need to be addressed, who is responsible for them, how they will be addressed (either by avoiding them or accepting them), and when they will be addressed.

ISO 27001 specifies four methods for handling potential dangers:

- **Mitigate:** take precautions to lessen the possibility that it will really happen.
- **Avoid:** eliminate the potential for harm by putting an end to the underlying conditions that might bring about an adverse outcome.
- **Transfer:** outsource the danger to someone else (i.e., outsource security efforts to another company, purchase insurance, etc.)
- **Accept:** if the possible loss is less than the expense of preventing the risk, you should take it.

### **3. Settle on the Preventative Measures in Terms of Security**

After you've zeroed in on the threats you wish to eliminate, you may choose the controls that will have the most effect. Review the controls suggested in Annex A and ISO 27002 to figure out which ones will work best for your business.

Weak or shared passwords between workers, for instance, pose a threat to data security. Implementing a company-wide password management system, such as Password, is one feasible control.

4. Make a Tally of the Controls you Won't be Utilizing and the Reasons Why

Accepting a risk might be more cost-effective in the long run for a firm than attempting to mitigate it. You shouldn't, for instance, spend \$10,000 to avoid a cost of \$1,000, or maybe the risk is already manageable since the danger is so unlikely, and/or has such a low potential effect. A Toronto-based company probably doesn't require seismic server racks or other costly earthquake precautions.

In the ISO 27001 Risk Treatment strategy, be sure to document any hazards that you have decided to ignore. Your auditor will want to see that you have at least considered the potential consequences of completing the SOA and have decided to do so knowingly and voluntarily.

5. Finalize Your Application's SOA

Describe whether or not you implemented each control specified in Annex A and explain your reasoning. You'll detail the date the control was put into place and indicate whether it satisfies a statutory, contractual, operational, or compliance mandate.

Most individuals utilize a spreadsheet to keep track of the SOA's extensive list of Annex A controls and the data that go along with them. Thus, any written work that can be conveniently divided into chapters will do.

	A	B	C	D	E	F	G
1	Statement of Applicability (SOA) for Acme Inc. ISMS : As at September 17, 2021						
2	Annex A reference	Control title	Control description	Applicability	Implemented	Notes	Justification for Inclusion or Non-inclusion
3	A.5	Security Policy					
4	A5.1	Information security policy					
5	A.5.1.1	Policies for information security	A set of policies for information security shall be defined, approved by management, published and communicated to employees and relevant external parties				
6	A.5.1.2	Review of the policies for information security	The policies for information security shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness				
7	A.6	Organization of information security					
8	A.6.1	Internal Organization	To manage information security within the organization.				
9	A.6.1.1	Information security roles and responsibilities	All information security responsibilities shall be defined and allocated.				
10	A.6.1.2	Segregation of duties	Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.				
11	A.6.1.3	Contact with authorities	Appropriate contacts with relevant authorities shall be maintained.				
12	A.6.1.4	Contact with special interest groups	Appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained.				
13	A.6.1.5	Information security in project management	Information security shall be addressed in project management, regardless of the type of the project.				
14	A6.2	Mobile devices and teleworking					
15	A.6.2.1	Mobile device policy	A policy and supporting security measures shall be adopted to manage the risks introduced by using mobile devices.				
16	A.6.2.2	Teleworking	A policy and supporting security measures shall be implemented to protect information accessed, processed or stored at teleworking sites.				
17	A.7	Human resource security					
18	A.7.1	Prior to employment					
19	A.7.1.1	Screening	Background verification checks on all candidates for employment shall be carried out in accordance with relevant laws, regulations and ethics and shall be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.				
20	A.7.1.2	Terms and Conditions of employment	The contractual agreements with employees and contractors shall state their and the organization's responsibilities for information security.				
21	A.7.2	During employment					
22	A.7.2.1	Management responsibilities	Management shall require all employees and contractors to apply information security in accordance with the established policies and procedures of the organization.				
23	A.7.2.2	Information security awareness, education and training	All employees of the organization and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.				
24	A.7.2.3	Disciplinary process	There shall be a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach.				
25	A.7.2	Termination and change of employment					

Figure 1: Sample Statement of Applicability


6. Make Sure that Your SOA is always up to date

Your SOA should be seen as a dynamic document. In order to maintain compliance with ISO 27001 requirements, it is necessary to regularly review and update your security measures.

The controls you employ and how you've modified them to enhance your ISMS should be reflected in your SOA, which should be updated on a regular basis.

ISO 27001 and SOA

What Annex(es) of ISO/IEC 27001 apply to a certain organization is detailed in an SOA. A security control may or may not be relevant to your company's ISMS. A justification must be provided if a given control is inapplicable.



Here are some commonly asked questions related to ISO 27001 and SOA to deepen your understanding of SOA.



Is it necessary to have an SOA in order to comply with ISO 27001?

*Toggle the answer below to see the response.*

If you want to get your hands on an ISO 27001 certification, you'll need to submit an SOA.

Toggle Answer



To what end does one formulate an ISO 27001 SOA?

*Toggle the answer below to see the response.*

SOAs often take the form of an Excel spreadsheet since they detail the Annex A controls established by your company. Please detail the implementation and last assessment dates for each control listed in Annex A, as well as whether or not it has been applied and the rationale for doing so.

Since SOAs are ever-evolving documents that should reflect the state of your ISMS at any given time, a revision history is also a good idea.

Toggle Answer



What is the reason for an SOA in ISO 27001?

*Toggle the answer below to see the response.*

You must provide an explanation (or justification) for why an Annex A control is not relevant to your ISMS if you choose not to apply it.

Toggle Answer

## Key Takeaways

In this reading, you learned how to:

- Outline the controls selected by an organization to meet the requirements of the ISO 27001 standard.
- Demonstrate that an organization has identified the security risks it faces and has taken steps to effectively manage them.
- Provide an audit trail of the control selection process to verify that the organization is compliant with the standard.

## Conclusion

In this reading, you learned what an SOA is and how to write one. Next, in the lecture, your instructor will guide you through completing an SOA.

✓ Mark Completed



Previous

RMF Stage 6 - Monitoring Security Controls

How well did this activity help you to understand the content?

Let us know how we're doing



W05D1

Mon Jul 22

> Lectures (1)

✓ Work (8)

7 hrs

- </> [Risk Management Methodology Document](#)
- [RMF Stage 4 – Assessing Controls \(Part One\)](#)
- [RMF Stage 4 – Assessing Controls \(Part Two\)](#)
- ? [GRC Quiz 2](#)
- [RMF Stage 5 - Authorizing Information Systems](#)
- </> [Conducting Residual Risk Assessment](#)
- [RMF Stage 6 - Monitoring Security Controls](#)
- [Writing Statement of Applicability \(SOA\)](#)

W05D1 Schedule »