

Audio transcripts and lesson notes

Hi, this is your instructor Anup Narayanan and in this chapter we shall look at “Preparing the Statement of Applicability”. We shall use the short form of “SOA” for “Statement of applicability” in this chapter.

Let us remind ourselves about where we are. We are in the PLAN phase.

In the PLAN phase, we are at “Step 8 – Preparing the “Statement of Applicability”

Let us define the “Statement of Applicability”. The SOA is a document that lists the controls that you have chosen for treating the information security risks in your environment. The SOA also provides a brief explanation of how the control is implemented by giving reference to policies, procedures and physical evidences of implementation.

You can also list controls that you have chosen apart from the ISO 27001 controls.

The SOA is structured as shown in the screen. There is also an entire SOA sample available in the iSQ World ISO 27001 e-Learning portal. The SOA has the following columns.

Column 1 is ISO 27001 Control Objective – This column shows the control objective that you have selected, for example control objective 5.1 - Information Security Policy.

Column 2 is ISO 27001 Control – This column shows the ISO 27001 controls that you have selected. In this case “A.5.1.1 Information Security Policy document” and “A.5.1.2 Review of Information Security Policy”.

Column 3 shows whether you have implemented the control or not

Column 4 provides a justification for implementing or not implementing the control. In this case control “A.5.1.1 Information security policy” is implemented and justified by stating that it defines the ISMS framework. The control “A.5.1.2” is implemented and justified by stating that it is required “to ensure that the security requirements of the business is continuously evaluated and updated”.

Column 5 shows the evidence for implementation. In this case the justification for control “A.5.1.1” is the ISMS manual of the company and for control “A.5.1.2 is the version control in the ISMS manual”.

There are few important things that you must remember about the SOA. The SOA is a public document. This means that the SOA is available to the public on demand. Typically, the SOA may be demanded by the customers or interested parties. This is because by reading the SOA the reader is able to clearly understand the information security controls that you have implemented along with the justification for the same.

Thank you and I hope you have understood about the SOA. There is a sample SOA available in the ISO 27001 e-learning portal. Please do go through it.