The importance of your Statement of Applicability when implementing ISO 27001

Your Statement of Applicability (SoA) is the central document that defines how your organisation implements information security. It is the main link between your risk assessment, selected security controls and the implementation status of each control.

Its purpose is to provide a complete list of candidate security controls that could be chosen and implemented to protect your assets, and to demonstrate that you have considered whether or not it is appropriate that each security control should be selected and implemented. Security controls that you determine should be selected and implemented are called "applicable" controls while those which you determine are not relevant to your business and which will not be implemented are called "not applicable" controls.

ISO 27001 requires that organisations justify their decision for candidate controls that have not been selected for implementation ("not applicable" controls) and that they also provide a rationale for the security controls that they have selected for implementation. This information is conveniently recorded in the SoA.

Why do you need a SoA?

ISO 27001 requires that the organisation's Information Security Management System (ISMS) be designed on a risk basis. That is, security controls should be selected for implementation on the basis that they help to contain the likelihood or impact of a security risk to an acceptably low level.

Creating a SoA demonstrates that the organisation has considered a comprehensive set of candidate controls and that the applicability (or otherwise) of each has been duly considered in accordance with the requirements of ISO 27001. The SoA specifically justifies the inclusion or exclusion of candidate controls (whether sourced from ISO 27001 Annex A, from the ISM or from other sources) as appropriate for your environment and business delivery model. Controls may also be identified and added to the SoA that are required because of other reasons. For example, because of legal or regulatory requirements, specific contractual requirements, or for strategic or marketing purposes.

Good practice is to also describe how each applicable control is implemented. This could be by linking each applicable control to a document such as a policy or procedure, or by briefly describing the procedure. Providing clear links from the security controls that have been selected for implementation to organisational documents showing that the control is in place will be very important to inform your management review/self-assessment,

internal audits, and demonstrating this to your Certification Body if you are seeking independent certification of your ISMS.

The role of the SoA in your ISO certification

Your SoA requires thought about how controls will be implemented. Will implementation require the purchase of new equipment? Will it result in a change to business procedures? Are additional human resources required? Will the control be implemented across all physical sites or ICT systems, or will asset-specific implementations be required? These are important decisions with the potential to impact multiple areas across your business. Documenting the SoA helps organisations to do this assessment in a systematic way.

Written well, your SoA is a perfect overview of:

- your controls – what needs to be done to implement a suitable standard of information security across the business
- justification – why it has to be done, which risk or business requirement drives it
- how - with a description of how it is done.
- where – if a control needs to be implemented across multiple sites, the SoA can be modified to track implementation status at each location. If the control is applicable to multiple ICT systems, the SoA can be modified to record this as well.

By writing a strong SoA the number of other documents required could be decreased. For instance, control procedures require documentation. If the description is rather short, it can be included in the SoA. This could avoid the need to write a separate procedure document.

Your certification auditor will use your SoA when it comes time to be certified. They will walk around your organisation checking whether controls have in fact been implemented in the way described. It is a central document guiding their work. In the same way, your internal audits and your Management Review can both be well informed by a complete and accurate SoA.