The Benefits of the Statement of Applicability in ISMS Projects

Jayakumar Sundaram, CISA, ISO 27001 LA
Is vice president of information systems and security at CRP Risk Management Ltd. (now SecUR Credentials Pvt Ltd), Mumbai, India. He has 25 years of information systems experience, working for 12 years on IT project developments, application management and delivery, and, for the past 13 years, on Capability Maturity Model Integration (CMMI), information security management system (ISMS) value implementations, with an information security audit perspective.

The statement of applicability (SoA) is the main link between risk assessment and risk treatment in an enterprise or in an organization within an enterprise and, therefore, is a requirement for information security management system (ISMS) implementations. The SoA is a continuously updated and controlled document that provides an overview of information security implementation.

ISO 27001:2013 includes a documented statement (the SoA) with 35 control objectives and 114 comprehensive controls to implement in an organizational ISMS.[1] The SoA should provide a reason for including or excluding any of the SoA controls in the ISMS. Some organizations may not require all controls listed under the SoA. For example, an organization that does not allow staff to work remotely does not need to implement telecommuting-related controls. Likewise, implementing only the ISO 27001:2013 controls may not sufficiently secure enterprise systems. For example, an enterprise that subscribes to cloud services might require additional controls.

SoA preparation at the enterprise level requires significant coordination, time, effort and upper-management commitment. The resulting SoA should be a short chart of controls. The SoA must be reviewed and approved by top management or an appropriate authority of the organization. Enterprises are often very anxious about audits, and top management can put great pressure on information security roles to eliminate nonconformity in an audit. The scenario at most enterprises is often quite dramatic when an audit is nearing and during the audit. Full attention and focus on the SoA during its preparation should result in few or no surprises. If the SoA is created correctly, nothing major can fall through the cracks regarding conformance to information security requirements. Any nonconformance/noncompliance found by the auditors could be considered as extra resources that would help organizations toward continual improvements.

The process for producing the SoA and implementing the ISMS is very simple to understand:

- The International Organization for Standardization (ISO) says that all activities must follow a method.
- That method or process must be documented.
- Processes must have controls, such as audits and reviews.
- The enterprise must have a security goal, which is stated in the information security policy.
- The enterprise must continuously verify and continuously improve the processes and controls.

To implement the ISMS, the enterprise requires written policies, procedures and work instructions—adhering to these policies and methods fills most information security gaps. Enterprises' top management should be prepared to answer the following questions:

- Why is the ISMS being implemented?
- How is the ISMS being implemented?

The purpose of information security is to ensure the protection of confidentiality, integrity and availability (CIA). An ISMS is a systematic risk approach to

establish, implement, operate, monitor, review, maintain and improve information security. An ISMS can be implemented as the result of risk analysis to eliminate or reduce risk to an acceptable level. The basics of information security are the preservation of CIA:

- **Confidentiality**—Ensuring that the information is accessible only to those authorized to access it
- **Integrity**—Ensuring that the information is accurate and complete and that the information is not modified without authorization
- **Availability**—Ensuring that the information is accessible to authorized users when required

The SoA serves as a checklist to implement ISMS in the organization so that no necessary controls are omitted. The SoA controls identify all relevant regulatory and legal requirements, and must address contractual obligations and controls that are related to the business needs.[2] The SoA should be unique to the enterprise and must be relevant to its business.

The advantages of the SoA are that it explains the controls succinctly and is acceptable to the auditor who assesses the enterprise. ISO seldom dictates writing 100-page policy documents for each control.

The first step to an SoA is an information security risk assessment with a mapped risk acceptance criteria. The risk assessment process is associated with the loss of confidentiality, integrity and availability of information, which must include:

- People
- Software
- Hardware
- Data and databases
- Information
- History of attacks
- Previous audits
- Current and planned controls to decrease risk
- External vulnerability, assessment and penetration test (VA/PT) exercise
- Subject matter experts
- Procedures or work instructions to which staff must adhere

> **“One size does not fit all. The enterprise must avoid the risk of using borrowed/downloaded sample documents as its own.”**

Each risk must be identified, analyzed to determine levels of risk, evaluated for the significance of the risk, recorded and reviewed. One size does not fit all. The enterprise must avoid the risk of using borrowed/downloaded sample documents as its own. Performing real-life risk treatment processes begins when the SoA document is completed. For each risk that is identified in the risk assessment, the risk treatment identifies whether the enterprise accepts, avoids, reduces, shares the source of, changes the likelihood of or changes the consequence of the risk. Data classification, media handling, backup, insurance, asset management, continuous monitoring and reporting are strategies to mitigate the risk. The information security risk treatment plan

is often documented in the risk register, which must include all likely threats and impacts. Evaluation of risk, remedial risk strategies and follow-up can only be related with a comprehensive SoA.

The SoA is the central document that information security auditors use to walk through the ISMS process controls. Every control that the SoA explains must be understood by all management and all staff. The SoA explains succinctly the information security controls that are relevant to any enterprise business. The time that an enterprise spends preparing the SoA, systematically keeping it up to date, including SoA in their internal audit scope and conducting management reviews will always be beneficial.

Endnotes

1 International Organization for Standardization (ISO), *Information Technology—Security Techniques—Information Security Management Systems—Requirements*, ISO 27001:2013, 2013
2 *Ibid.*