ISO/IEC JTC 1/SC 27/WG 1 "Information security management systems"
Convenorship: **BSI**
Convenor: **Humphreys Edward Prof.**

Auditing Practices Note - SoA

Document type	Related content	Document date	Expected action
General / Other		2022-09-11	**INFO**

Description

The Auditing Practices Notes will be discussed at the WG 1 meeting on the 5th Oct.

SC 27/WG 1
Information Security Management Systems
Date: 10-09-2022

ISO/IEC 27001 Auditing Practices Group

Guidance on:

Statement of Applicability (SoA)

INTRODUCTION

This auditing practice note provides information on the proper way to use and interpret the requirements for a Statement of Applicability (SOA) as defined in ISO/IEC 27001. This information will be useful for both auditors and auditees of ISO/IEC 27001.

QUESTIONS ABOUT THE SOA

The following questions have been raised about the SOA and the text that follows provides some explanation as how best to interpret the requirements of the SOA to answer these questions.

1. Is the concept of applicability applied in the same way or shared as a common notion between ISO/IEC 27001:2013 and ISO 9001:2015?
2. Must the SOA use the same structure as ISO/IEC 27001 Annex A?
3. Is not the SOA just a conformance table, which explains how the organization implements the Annex A controls?
4. If the organization has implemented information security controls that are not in Annex A, must the organization include them in the SOA?
5. What if the organization is just a small business unit within a much larger enterprise and relies heavily on externally provided services?
6. Is it acceptable in common practice if regulators require or provide a standardized SOA?
7. Who has the ultimate decision on an SOA, the auditor, or the organization?

RELATIONSHIP BETWEEN SoA, ANNEX A AND ISO/IEC 27001 REQUIREMENTS

The term SOA has been used since the concept of an ISMS standard was first conceived. In BS 7799-2:1998 the earliest forerunner of ISO/IEC 27001, the controls were included in the main body of the standard as requirements. However, it was recognised that some controls did not apply to all organizations and the device of a SOA was introduced to specify which ones did apply. However, over time the SOA has been repurposed, but the name has remained the same.

Since ISO/IEC 27001:2013, the term SOA refers to the documented information that contains an organization’ s necessary information security controls; justification for why they are included in the SOA; whether they are implemented or not; and the justification for any Annex

A controls that are excluded, i.e., are determined as being unnecessary according to the organization's business context.

ISO/IEC 27001 (Clause 6.1.3. b)) requires organizations to determine the information security controls that they need to reduce their exposure to information security risk to an acceptable level. These are called *necessary controls*.

If, during this process of risk treatment, an organization inadvertently omits a necessary control, it will be unknowingly exposed to information security risk – it will think itself safe when it is not. To counter this, ISO/IEC 27001 Clause 6.1.3 c) requires organizations to compare their necessary controls with those in Annex A (see Auditing Practice Note WG1nXXX). Thus, Annex A is a *reference set of controls*, which is what the Annex is called. (Note: Annex A is renamed as *Information security controls reference* in the 2022 edition of ISO/IEC 27001.)

Such a comparison process can be performed by mapping the organization's necessary controls to the Annex A controls. If, at the conclusion of this process, there are any Annex A controls left over, then the organization must confirm that a control of that type is unnecessary. The justification must be included in the SOA.

Annex A contains a wide variety of controls, but this list of controls is, by design, neither complete nor recommended. It is simply an assortment of security measures which may (or may not) match the list of controls which an organisation decides to implement. The list of controls which an organisation decides are appropriate to it, and which it will implement, are its "necessary controls"; this list will vary by organisation. Indeed, organizations can design their own controls or select them from sources other than Annex A (e.g., standards such as ISO/IEC 27011, 27017, or industry sources such as NIST).

Thus, the presence of a control in Annex A does not make it necessary to an organisation. The determination of necessity is the responsibility of the organisation itself, via (for example) risk assessment, or via the need to comply with contractual or legal obligations. Annex A is intended to support the organisation's decision-making process, not replace it. It is an aide memoire, a selection of measures which can cause an organisation, by reason of being required to match its necessary controls to the controls in Annex A, to realise that it has missed something which is indeed necessary to the organisation for independently justifiable reasons.

To summarise: in an organisation's SOA, the justification for inclusion of a control must reflect the context and risk management arrangements of the organization, not simply because it is in Annex A. Exceptionally, an organization could provide other justifications, such as best practice when there is uncertainty as to the sources of risk.

It is possible that there will be necessary controls that are not in Annex A. These are referred to in ISO/IEC 27003 as *custom controls*. It is also possible that a custom control replaces the need for an Annex A control, as explained in ISO/IEC 27003. ISO/IEC 27007 refers to such a custom control that has a similar wording to the Annex A control that it replaces as a *variation*.

For the ISMS certification activity, the version of the SOA must be referenced in the certification documents (see ISO/IEC 27006:2015, 8.2.1). However, a change to the SOA which does not

change the coverage of the controls in the scope of certification does not require an update of the certification document.

Thus:

- The ISO/IEC 27001 requirement is to compare the organization's necessary controls with a common reference set of controls to discover if any necessary control has been inadvertently omitted;
- Annex A is that common reference set;
- The SOA is a means to document all the organization's necessary controls in one place; explain why they are necessary; whether they are already implemented or not and explain why any of the reference controls are unnecessary;
- ISO/IEC 27006 requires that the version of the SOA shall be referenced in the ISMS certification document.

HELPING AN AUDITEE INTERPRET THE USE OF SoA

The concept of *applicability* is used in both ISO/IEC 27001 and ISO 9001. ISO 9001 addresses the applicability of the requirements in the main body of the standard, which organizations can exclude provided that the exclusion does not affect quality. For ISO/IEC 27001, all the requirements in Clauses 4 – 10 are applicable and cannot be excluded. The controls in Annex A, as explained above, are not requirements and therefore the term SOA, in the context of ISO/IEC 27001 is not the same as it is in ISO 9001.

ISO/IEC 27001 specifies what the SOA must contain. It does not specify how it should be structured. Nevertheless, organizations could use the structure of Annex A, for example in the form of a table with additional columns for implementation status and justifications. Alternatively, it could place all its necessary controls the top of the SOA and place the justifications for any unnecessary Annex A control at the bottom. If the same justification applies to several unnecessary Annex A controls, the controls can be grouped, and the explanation given once.

In either case the organization is permitted to include whatever additional information that it deems necessary. For example, ISO/IEC 27002:2022 introduces the concept of control attributes and explains how organizations can define its own. If it does, the SOA would be an appropriate place to record them.

The necessary controls in the SOA do not have to have the same names as those in Annex A and they do not have to use the same control text. Moreover, they can be expressed as statements of fact ("we do X…") as opposed to instructions of intent (*The organization shall*). Nevertheless, it is important to be able to demonstrate conformity to Clause 6.1.3 c), and that can be done by showing the mapping between the necessary controls and the Annex A reference controls.

It is also important to implement exactly what the organization uses as control text for its necessary controls. In this respect, the use of custom controls and variations is a powerful device. If all the necessary controls are expressed in this way, the organization can be very precise in terms what it does (either directly in the organization's necessary control text or by

reference to the detail), significantly reducing the possibility of being found nonconformant. If the organization adopts the Annex A control text as its necessary control specifications but does not do what the Annex A control specifies, then there is plenty of scope to be found nonconformant.

The SOA must contain the necessary controls. Therefore, if the organization uses a control that is not in Annex A, then for conformity with ISO/IEC 27001, 6.1.3 d) it must be included in the SOA.

ISO/IEC 27001 applies to all types of organizations. If the organization is part of a larger entity, the term *organization* in ISO/IEC 27001 refers only to the part of the larger entity that is within the ISMS. In this situation, the organization could rely on the external parties to implement the processes and activities of its ISMS, which include the external suppliers outside the larger entity and internal suppliers in the larger entity. For example, the power company is an external supplier, and the HR department of the larger entity is also an external supplier, albeit internal to the larger organization. There is a new requirement in ISO/IEC 27001:2022 that requires externally provided processes, products and services that are relevant to the ISMS to be controlled. If the risk of power failure, for example, is an acceptable risk, it will not affect the intended results of the ISMS. Therefore, it is not relevant to the ISMS and does not need to be controlled. If, on the other hand, it is an unacceptable risk, risk treatment should result in the use of a control (like A.7.11 – Supporting utilities). Even if the necessary control is performed by an external organization it must still be included in the SOA.

Interested parties, such as regulators, are perfectly entitled to place requirements on the organization. These should be dealt with via ISO/IEC 27001:2022 Clause 4.2 and should find their way into the risk assessment and risk treatment processes, and hence the SOA that way. The regulator is perfectly entitled to seek evidence of compliance with its requirements, but whether the SOA is the most suitable way to do that would depend on the case in question. Demonstrating compliance with regulatory requirements is not the same as producing an SOA.

The organization has the final authority and responsibility for how to implement its ISMS, including the SOA. The SOA is for the benefit of the organization. Nevertheless, auditors are looking for evidence of conformity against Clause 6.1.3 d), and auditors can rule the SOA nonconformant if it does not meet those requirements.

For further information on the ISO/IEC 27001 Auditing Practices Group, please refer to the paper: *Introduction to the ISO/IEC 27001 Auditing Practices Group*

Feedback from users will be used by the *ISO/IEC 27001 Auditing Practices Group* to determine whether additional guidance documents should be developed, or if these current ones should be revised.

Comments on the Auditing Practices Notes can be sent to the following email address: sc27.wg1@gmail.com