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

Auditing Practices Note - Annex A

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.

ISO/IEC 27001 Auditing Practices Group

Guidance on:

What is Annex A?

INTRODUCTION

This auditing practice note provides information on the proper way to use and interpret Annex A of ISO/IEC 27001. This information will be useful for both auditors and auditees of ISO/IEC 27001.

ISO/IEC 27001 applies a risk management approach to determine a set of controls, that must be compared with those in Annex A. This reduces the chances of having an incomplete risk treatment plan.

What is a normative Annex, according to ISO directives

Annex A of ISO/IEC 27001 is a normative annex which means it provides additional normative text to the main body of the document (ISO/IEC Directives Part 2). One particular use of a normative annex is to present information in regard to a particular application of the document, for example a process shall be carried out according to what is specified in the annex. Therefore, in the case of Annex A it states that the information security controls in Annex A **shall** be used in context with 6.1.3.

Purpose and proper use of Annex A

+ For comparison against the results of the risk assessment process to determine risk treatment options and controls
+ As the foundational control in the ISMS, because even if the risk assessment process is not mature, the organization will compare the results against a common base of controls to avoid omissions
+ As a quality check to ensure that the risk treatment plan is complete
+ To fulfil the requirement of producing a Statement of Applicability

Improper use of Annex A

− As a comprehensive list of controls. Requirements contained in sub-clause 6.1.2 and sub-clause 6.1.3 provide the flexibility to adopt any additional control set(s), allowing customization to any sector or business-specific need. This allows the organization to apply best practice when performing risk treatment
− As a requirement list; the shalls in Annex A apply only if the organization determines that the specific control is relevant

RELATIONSHIP BETWEEN ANNEX A AND ISO/IEC 27001 REQUIREMENTS

ISO/IEC 27001 6.1.3 c) states "…compare the controls determined in 6.1.3 b) above with those in Annex A and verify that no necessary controls have been omitted;"

Therefore, the requirement is to make a comparison between the results from the risk assessment and the controls in Annex A.

HELPING AN AUDITEE INTERPRET THE USE OF ANNEX A

As stated in ISO/IEC Directives part 1, Annex SL, a management system is "a set of interrelated or interacting elements of an organization to establish policies and objectives, as well as processes to achieve those objectives". In this sense, all organizations have a management system, whether or not they have implemented a formal management system standard.

An MSS defines the requirements for a management system that uses a framework of resources to achieve an organization's objectives. Organizations and interested parties, such as conformity assessment bodies and regulators, can decide whether or not they use (or require the use of) an ISMS and how to use it, based on their needs.

ISO/IEC 27001 subclause 6.1.2 c) requires the organization to apply an information security risk assessment process to identify risks associated with the loss of confidentiality, integrity and availability of information within the scope of the information security management system.

If information is affected, business objectives may be compromised. The ISMS should align information security objectives with business objectives, and apply a risk management process to assess, identify and evaluate those events that might have an effect on information, assets, and business enablers.

The organizational context, including risks to information security is always changing, therefore it is important that the ISMS remains appropriate, effective and suitable. This includes making sure that the risk management process remains fit for purpose.

During the early stages of the establishment of an ISMS, having a list of controls to be compared against those obtained from the risk assessment is a control in itself, because if the risk assessment process has overlooked a necessary control it may be identified during this comparison. However, Annex A is not an exhaustive set of controls, so additional control sources (e.g. ISO/IEC 27017, PCI-DSS, COBIT, NIST 800-53) can be applied to complement this.

When are exclusions from Annex A controls acceptable?
The following reasons may be considered as acceptable to not implement a control listed in Annex A (this is not a complete list):

- If there is no related risk;
- If the risk is acceptable when considering the related controls and the impact to interested parties;
- If there is(are) another control(s) that replaces the Annex A control.

DISCLAIMER

This paper has not been subject to an endorsement process by the International Organization for Standardization (ISO), or ISO/IEC Sub-Committee JTC 1/SC 27.

The information contained within it is available for educational and communication purposes. The ISO/IEC 27001 Auditing Practices Group does not take responsibility for any errors, omissions or other liabilities that may arise from the provision or subsequent use of such information.

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