ISO/IEC JTC 1/SC 27/WG 1 **N 3083**

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

WG 1 CATF Advisory Note 1 - Why Is ISO/IEC 27001 Sufficient for the disciplines of Information Security and Cybersecurity?

Document type	Related content	Document date	Expected action
Project / Other		2021-11-28	INFO

Description

This is an Advisory Note from the WG 1 Conformity Assessment Task Force (CATF).

SC 27/WG 1
Information Security Management Systems

WG 1 Conformity Assessment Task Force

Advisory Note One

Why Is ISO/IEC 27001 Sufficient for the disciplines of Information Security and Cybersecurity?

EXECUTIVE SUMMARY

Is ISO/IEC 27001 SUFFICIENT for the disciplines of information security and cybersecurity?

YES, ISO/IEC 27001 is sufficient for all discipline-specific requirements of information security and cybersecurity due to several facts:

- ISO/IEC 27001 is a Type A Management System Standard (MSS)[1] and by its structure, definitions, concepts and content, is applicable to all types and size of organization requiring all types of information security and cybersecurity protection. ISO/IEC 27001 is sufficient to provide information security and cybersecurity protection to organizations in all business[2] markets and sectors;
- By adopting the harmonized structure (HS) contained in the ISO Directives Part 1[3] (Annex SL Appendix 2), ISO/IEC 27001 is intentionally designed to be the only MSS within the discipline of *information security and cybersecurity*;
- According to the ISO Directives Part 1 (Appendix 1), MSSs shall not overlap with each other and therefore, by publishing ISO/IEC 27001, this prevents the proliferation of management system standards (MSS) for *information security and cybersecurity*, and hence, it avoids duplication, conflict or contradiction of requirements.

This advisory note expands in detail, supporting what makes ISO/IEC 27001 sufficient, resulting in the fact that there is NEITHER A JUSTIFICATION FOR AN ADDITIONAL MSS FOR THE DISCIPLINE OF INFORMATION SECURITY AND CYBERSECURITY NOR A NEED FOR AN EXTENSION TO THE SCOPE OF ISO/IEC 27001.

[1] In the context of this advisory note, whenever the abbreviation MSS is used, this has to be understood as a Type A Management System Standard only.

[2] The term *business* in this advisory note is understood according to Annex SL Appendix 2, Edition 2021, page 12, sub-clause 5.1, left column:
NOTE Reference to business in this document can be interpreted broadly to mean those activities that are core to the purposes of the organization’ s existence.

[3] ISO/IEC Directives Part 1 and Consolidated ISO Supplement – 2021 (12th Edition)

SUFFICIENCY OF ISO/IEC 27001

PURPOSE OF A MANAGEMENT SYSTEM STANDARD (MSS)

A MSS provides requirements. Such a standard is not a conformance assessment standard. It may be used, purely on a voluntary basis, to conform with MSS requirements using a conformance assessment standard (e.g. ISO/IEC 17021-1). Therefore, ISO/IEC 27001 IS NOT A CONFORMANCE ASSESSMENT STANDARD[4] - IT IS A MSS FOR INFORMATION SECURITY AND CYBERSECURITY.

CHARACTERISTICS OF A MANAGEMENT SYSTEM STANDARD

Some important MSS characteristics include:

- A MSS specifies WHAT requirements are mandated for an organization to claim it has established, implemented, maintained and continually improve a management system;
- A MSS does NOT specify HOW its requirements can be fulfilled by an organization;
- An organization may cover only a part of a legal entity, the whole legal entity can span over several legal entities;
- such an organization has only ONE management system,
- such a management system can CONFORM to several different MSSs,
- A MSS is risk-aware or risk-based, depending on the discipline, resulting in the fact that any determined control shall be based on risk assessment and risk treatment;
- A MSS specifies a requirement for the continual improvement of the EFFECTIVENESS of a management system, not of the discipline-specific PERFORMANCE;
- The structure of a MSS, the order of the clause numbers and the order of the requirements DO NOT imply any SEQUENCE and could, in principle, be rearranged[5] without changing the requirements and their meaning.

DETERMINING RELEVANT REQUIREMENTS

An ISMS according to ISO/IEC 27001 is flexible enough to meet the needs and expectations of an organization. This means that ISO/IEC 27001 IS A UNIVERSAL STANDARD: all specific needs can and should be integrated in the design of the management system as well be an integral part of all actions conducted in the management system. The following are a few examples to illustrate this:

- All requirements applicable to the organization are to be determined in the ISMS. An organization might be affected by different kind of sector specific, customer or legal requirements, these should be integrated in the part of the ISMS where understanding the organization and its context and Understanding the needs and expectations of interested parties is explained;
- These will impact on the fulfilment of the MSS requirements such as;
  - the content of the policy,
  - the internal structure, operations and processes of the organization,
  - the roles, their responsibilities, and awareness,

[4] Note: In addition, ISO, and hence SC 27, does not involve itself in conformity assessment activities. ISO is involved in standards, ISO/IEC 17021 is a conformity assessment standard but ISO/IEC 27001 is not, and neither ISO/IEC 17021 nor ISO/IEC 27001 deals with conformity assessment activities this is done outside of ISO.

[5] TC/SC/PCs shall not rearrange clauses or requirements based on the HS for harmonization purposes.

- the provision of resources,
- the internal and external communication,
- the performance evaluation,
- the improvement of the management system,
- the design of the risk management process(es) and the applied risk assessment methodologies.

Therefore, the requirements clause 4 of ISO/IEC 27001, provides the ability for an ISMS to address any and all sector- or business-specific needs.

RISK MANAGEMENT

The ISO/IEC 27001 approach to assessing and treating risk is aligned with the principles and generic guidelines provided in ISO 31000. The objective of risk management is to ensure that exposure to information security risks is acceptable to the organization. Based on clause 6.1.3 c), organizations are mandated to compare the controls the organization has determined to those in the reference set of controls contained in ISO/IEC 27001 Annex A. This process is intended to provide confidence that no necessary control has been inadvertently omitted.

This comparison shall be summarized in a Statement of Applicability. ISO/IEC 27001 provides the flexibility to use any other control set(s) or source. ISO/IEC 27001 just requires the mapping against Annex A as described above.

The requirement for identifying risks is … *identify risks associated with the loss of confidentiality, integrity and availability for information within the scope of the ISMS*. This is a very powerful statement. It covers both properties of information and the use of information, as evidenced by the wide range of controls in the Annex A reference set. Moreover, it also covers all information that an organization wishes to be within scope of its ISMS, for example, a service provider, that should include information that customers store in its servers. The term *asset*, used in many of the Annex A reference controls, is defined as *anything that has value to the organization*. Therefore, service providers should regard such customer information as an asset and afford its protection, much as a bank protects the money deposited with it by its customers.

Therefore, the risk management approach adopted by ISO/IEC 27001 is sufficient to provide protection for all information within scope. However, different sources for controls can be used to complement those in Annex A to widen the comparison stated in 6.1.3 c), this includes documents containing controls for specific disciplines or sector, such as ISO/IEC 27011 or ISO/IEC 27017. For conformity assessment purposes, ISO/IEC 27006-1 includes the possibility to express this in a certification document mentioning the implementation of controls from other national or international standards.

The requirements contained in sub-clause 6.1.2 and sub-clause 6.1.3 provide the flexibility to address any sector- or business-specific need or best practise to use any additional control set(s) when performing the risk treatment and to fulfil the requirement of producing a Statement of Applicability.