INTERNATIONAL STANDARD

ISO/IEC 27021

First edition
2017-10

Information technology — Security techniques — Competence requirements for information security management systems professionals

Technologies de l'information — Tecniques de sécurité — Exigences de compétence pour les professionnels de la gestion des systèmes de management de la sécurité

Reference number
ISO/IEC 27021:2017(E)

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

Introduction

This document is intended for use by:

a) individuals who would like to demonstrate their competence as information security management system (ISMS) professionals, or who wish to understand and accomplish the competence required for working in this area, as well as wishing to broaden their knowledge,

b) organizations seeking potential ISMS professional candidates to define the competence required for positions in ISMS related roles,

c) bodies to develop certification for ISMS professionals which need a body of knowledge (BOK) for examination sources, and

d) organizations for education and training, such as universities and vocational institutions, to align their syllabuses and courses to the competence requirements for ISMS professionals.

This document should be read and used in conjunction with ISO/IEC 27001.

Information technology — Security techniques — Competence requirements for information security management systems professionals

1 Scope

This document specifies the requirements of competence for ISMS professionals leading or involved in establishing, implementing, maintaining and continually improving one or more information security management system processes that conforms to ISO/IEC 27001.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000 and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at http://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

3.1
competence
ability to apply knowledge and skills to achieve intended results

[SOURCE: ISO/IEC 17024:2012, 3.6]

3.2
information security management system professional
ISMS professional
person who establishes, implements, maintains and continually improves one or more information security management system processes

4 Concept and structure

4.1 General

ISMS professionals are people whose role is to manage the establishment, implementation, maintenance and continual improvement of one or more ISMS processes. They shall have and maintain knowledge and skills required in this document to fulfil their role successfully.

4.2 Concept of ISMS competence

Within an organization, several management systems may be implemented, operated and maintained. Each management system will be the responsibility of one or more professionals. One such system is the ISMS. This document describes the business management and domain-specific competence required of ISMS professionals responsible for an organization's ISMS. Figure 1 illustrates how "common management" and "domain-specific" competence (namely A, B, and X competence) are related with information security competence. Business management competence are given in Clause 5. Information security competence for ISMS professionals are given in Clause 6.

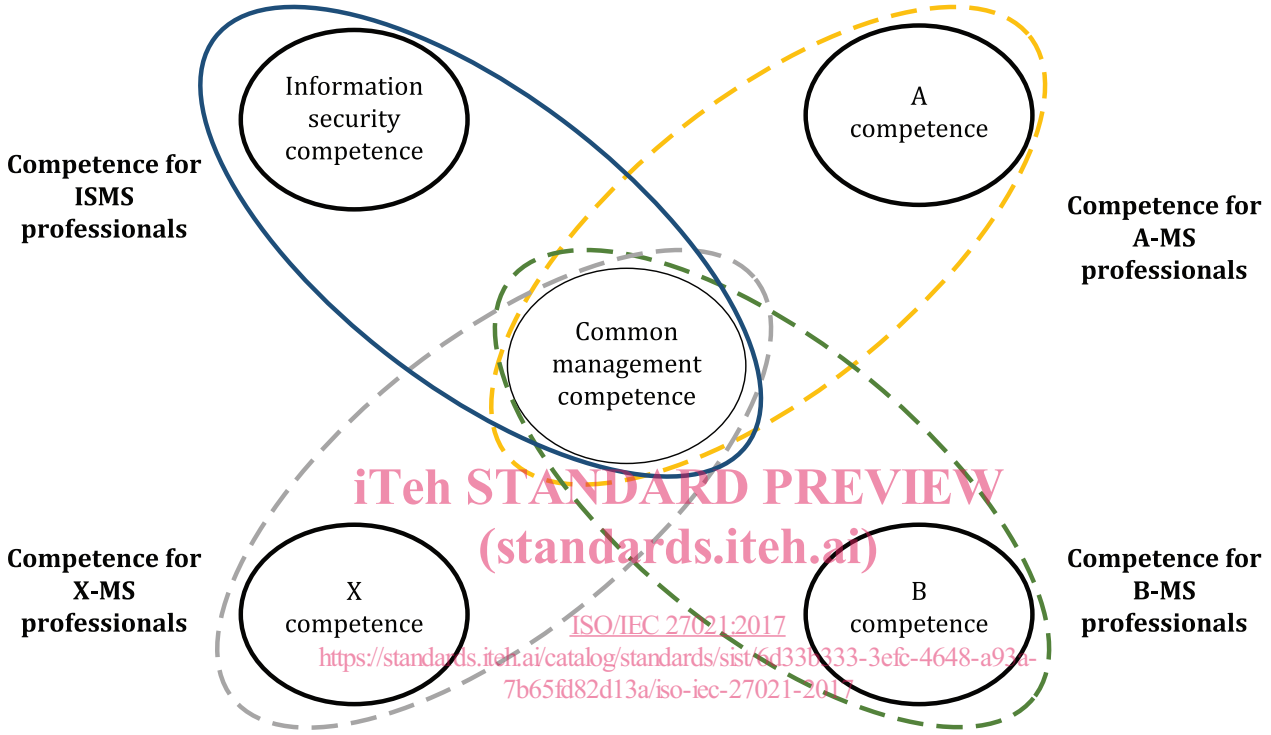

Figure 1 — Relationship of ISMS-specific competence with common and domain-specific competence

4.3 Structure of ISMS competence

For each of ISO/IEC 27001:2013, Clauses 5 to 10, one category and several competence are defined. Each competence is given a unique name and a unique number, a reference to associated clauses/subclauses of ISO/IEC 27001 if applicable, the intended outcome of the competence and a list of the knowledge topics and skills that make up the competence. Each competence is presented using a common template, shown in Table 1.

Table 1 — Template for competence description

ISO/IEC 27001 :2013 clause/subclause (if applicable)	N.N Title of clause/subclause
Intended outcome	Description of intended outcome – the result of applying the competence
Knowledge required	— Outlines of the topics, concepts and principles ISMS professionals know, are aware of, or are familiar with in this competence
Skills required	— The skills ISMS professionals are able to perform

4.4 Demonstration of competence

For each competence, ISMS professionals shall be able to demonstrate the following:

a) knowledge of the competence demonstrated by the possession of educational and/or professional qualifications; and

b) skill, or ability to carry out the managerial or technical tasks.

4.5 Structure of this document

This document shows the competence required for ISMS professionals structured into two categories. These categories are arranged based on common areas of business management and information security management and include 12 competence each. This is followed by a breakdown of ISMS-specific competence in a process order (Planning, Operation, Support, Performance evaluation, and Improvement). The structure of the clauses/subclauses is as follows:

— 5 Business management competence for ISMS Professionals

— 6 Information security competence

— 6.1 ISMS competence: Information Security

— 6.2 ISMS competence: Information Security Planning

— 6.3 ISMS competence: Information Security Operation

— 6.4 ISMS competence: Information Security Support

— 6.5 ISMS competence: Information Security Performance evaluation

— 6.6 ISMS competence: Information Security Improvement.

Annex A provides elements of knowledge for ISMS professionals that can be used in a body of knowledge (BOK) for an organization. When an organization creates a BOK which covers the knowledge for ISMS professionals, Annex A can be referenced as a source of elements that are included in the BOK.

5 Business management competence for ISMS Professionals

5.1 General

To accomplish their roles in an organization successfully and efficiently ISMS professionals shall acquire and keep up-to-date with respect to the fundamental areas of business management.

5.2 Competence: Leadership

ISO/IEC 27001:2013 clause/subclause (if applicable)	5 Leadership
Intended outcome	Directing, motivating and encouraging staff across the organization to deliver information security
Knowledge required	— Theories of leadership — Negotiation techniques

Skills required	— Set and give direction for information security across the organization — Provide guidance, set objectives and drive progress within the information security function, team and the business — Deliver commitments — Deploy responsibilities and authorities at the different levels of the organization

5.3 Competence: Communication

ISO/IEC 27001:2013 clause/subclause (if applicable)	7.4 Communication
Intended outcome	Sharing the correct information in a concise manner with the relevant parties and enabling the most productive interaction with the organization's management with regards to information security
Knowledge required	— Theories and methods of communication — Stakeholder analysis techniques — Communication techniques
Skills required	— Design the process and communication channels appropriate for the organization to establish the ISMS — Communicate using appropriate language and media to a range of audiences — Forge relationships with top management and business professionals — Determine the need for internal and external communications relevant the ISMS

5.4 Competence: Business Strategy and ISMS

ISO/IEC 27001:2013 clause/subclause (if applicable)	4.1 Understanding the organization and its context
Intended outcome	Understanding how business strategy is formulated and how information security and ISMS strategy fits into the overall business strategy
Knowledge required	— Business strategy and strategy formulation process — The legal and regulatory environment in which the organization operates — Definition of strategy, for example, by using a strategic alignment tree — Application of strategic objectives and ISMS global objectives to the different process of the ISMS
Skills required	— Understand business strategy and the strategy of the organization — Set information security objectives in the context of the business and its strategy — Demonstrate strategic direction with respect to the ISMS, ranging from planning to improvement that is organized toward common goals in information security — Allocate (or assist in the allocation of) resources to meet business and information security objectives

5.5 Competence: Organization design, culture, behaviour and stakeholder management

ISO/IEC 27001:2013 clause/subclause (if applicable)	4.2 Understanding the needs and expectations of interested parties
Intended outcome	Ensuring that the ISMS implementation matches the organizational structure and culture
Knowledge required	— Organization design theory — Theory of organization culture — Organizational behaviour approaches, methodologies and frameworks — Conflict management
Skills required	— Understand organization design — Understand organization behaviour — Analyse and evaluate organization culture — Integrate the ISMS into organization design — Manage conflict stakeholders with different interests and negotiate in order to accomplish security objectives

5.6 Competence: Process design and organizational change management

ISO/IEC 27001:2013 clause/subclause (if applicable)	No applicable clauses or subclauses
Intended outcome	Engineering of the performance of day-by-day information security related activities
Knowledge required	— Operational planning and control — Process design methodologies and frameworks — Process documentation and record management — Organizational context — Change management methodologies and frameworks
Skills required	— Direct processes, and oversee the plans to achieve information security objectives — Manage organizational processes — Manage outsourced processes — Manage change management processes — Manage records