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)

COPYRIGHT PROTECTED DOCUMENT

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.

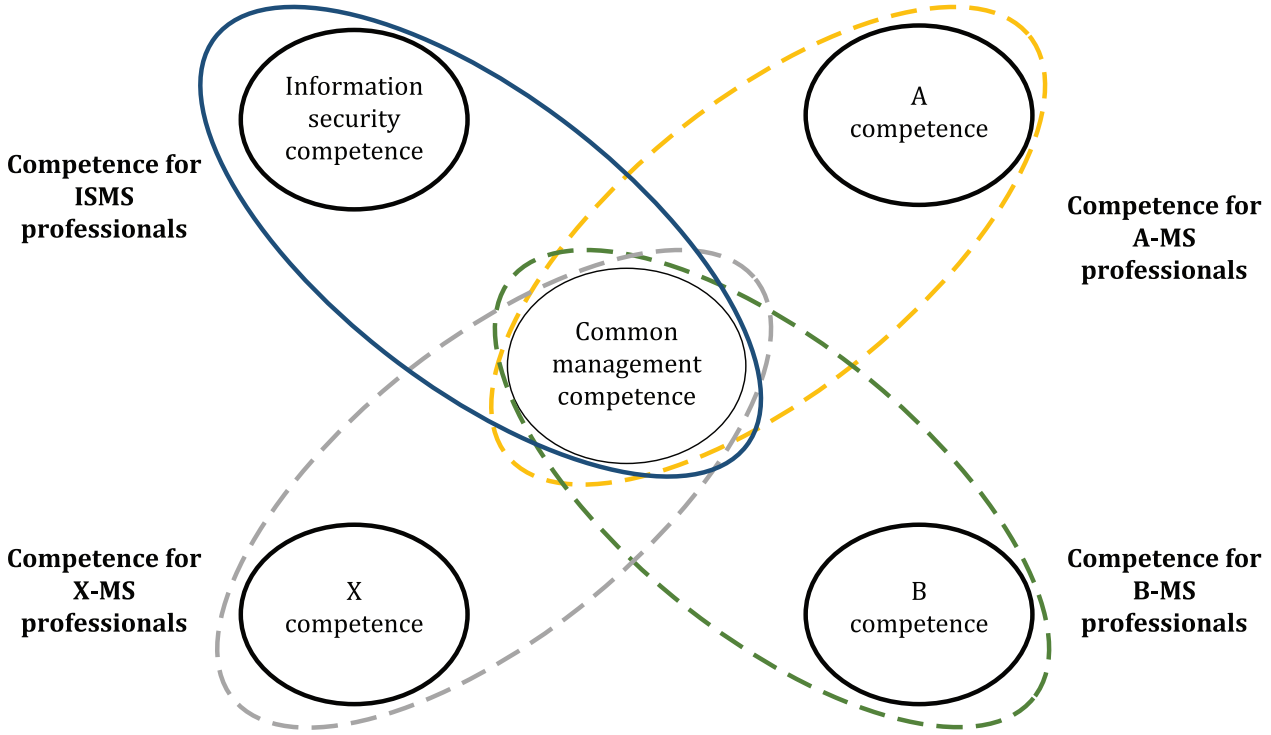

Figure 1 — Relationship of ISMS-specific competence with common and domain-specific competence

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

5.7 Competence: Human Resource, team and individual management

ISO/IEC 27001:2013 clause/subclause (if applicable)	7.2 Competence
Intended outcome	Taking proactive action and developing organizational processes to address the development needs of individuals, teams and the entire workforce
Knowledge required	— Appraisal systems and processes — Competence development methods — Competence needs analysis methodologies — Learning and development support methods (e.g. coaching, teaching, training) — The optimum staffing and skills required to implement and maintain the ISMS — Information security qualifications and certifications
Skills required	— Set organizational and individual objectives, goals and targets and link them — Understand and use strategies such as empowerment — Measure and influence the level of employee motivation — Use tools such as performance management, objective setting and appraisals — Coach and/or train and/or mentor individuals or teams — Work in cross-functional teams to achieve business and/or information security objectives — Build a team work culture — Support the specification, interview, recruitment, selection, training, supervision and development of staff with appropriate skills, experience and motivation — Measure the results of training, coaching and related actions and the acquisition of the skills

5.8 Competence: Risk management

ISO/IEC 27001:2013 clause/subclause (if applicable)	No applicable clauses or subclauses
Intended outcome	Understanding of the methodologies, frameworks and outputs of risk management
Knowledge required	— Fundamental principles of risk — Business risk management methodologies and frameworks, risk assessment treatment — The legal and regulatory environment the organization operates in
Skills required	— Understand the definition of risk and its components in real-world scenarios — Comprehend business risk management methodologies, assessment and treatment methodologies and processes — Explain the outputs of business or enterprise risk management

5.9 Competence: Resource management

ISO/IEC 27001:2013 clause/subclause (if applicable)	7.1 Resources
Intended outcome	Ensuring that appropriate resources are determined and provided in time for the establishment, implementation, maintenance and continual improvement of the ISMS
Knowledge required	— Financial reporting and measurement — Budget creation and management techniques — Cost management and reduction techniques — Time and materials management techniques — Management review and corrective action processes
Skills required	— Determine the resources needed for the establishment, implementation, maintenance and continual improvement of the ISMS — Budget business elements including cost of implementation and operation of the ISMS — Understand financial reporting, including cashflow and profit and loss — Create business and investment cases — State ROI (return on investment), ROSI (return on security investment) and other financial benefits — Apply cost control and budget management techniques — Provide appropriate resources in time in the right place

5.10 Competence: Information systems architecture

ISO/IEC 27001:2013 clause/subclause (if applicable)	No applicable clauses or subclauses
Intended outcome	Understanding the applicable information systems architecture used to create, store, process, transmit and dispose of the organization's information
Knowledge required	— Information systems architecture requirements — Hardware components, tools and hardware architectures — Operating systems and software platforms — Integration of, and dependency on, business processes with ICT applications — Information security aspects of information systems architecture
Skills required	— Understand the business objectives/drivers that impact the information systems architecture — Understand the interaction of security components and information system architecture components

5.11 Competence: Project and portfolio management

ISO/IEC 27001:2013 clause/subclause (if applicable)	No applicable clauses or subclauses
Intended outcome	Managing efficiently and effectively the different types of ISMS related projects and actions (such as corrective, preventative, improvement) in order to meet their intended outcomes on time, on budget and to quality
Knowledge required	— Project management methodologies and frameworks — Portfolio management methodologies and frameworks — Approaches to define project steps and tools to set up action plans
Skills required	— Manage projects, portfolio, activities and tasks — Manage, with the business, the portfolio of ISMS-related investment projects — Plan projects to implement strategies, establish procedures and implement them successfully and efficiently — Work in cross-disciplinary teams to achieve business and/or information security objectives

5.12 Competence: Supplier management

ISO/IEC 27001:2013 clause/subclause (if applicable)	No applicable clauses or subclauses
Intended outcome	Understanding the role of suppliers and the supply chain in the organization and the impact on information security
Knowledge required	— Use of suppliers and the supply chain
Skills required	— Assess suppliers and the supply chain(s) — Assess the impact on information security of suppliers and the supply chain(s) — Manage suppliers where required — Provide information security guidance when creating, assessing, selecting, managing and exiting supplier relationships

5.13 Competence: Problem management

ISO/IEC 27001:2013 clause/subclause (if applicable)	No applicable clauses or subclauses
Intended outcome	Identifying and resolving problems that might have consequences for the ISMS in a timely manner
Knowledge required	— Problem solving and analysis methodologies and frameworks
Skills required	— Understand internal and external issues — Analyse and synthesize information and data concerning the problems — Describe management problems analytically, apply analytical approaches, and elaborate problem solutions — Present and explain proposed solutions to relevant audiences

6 Information security competence for ISMS professionals

6.1 ISMS Competence: Information Security

6.1.1 General

To accomplish their roles in an organization successfully and efficiently ISMS professionals shall acquire and keep up-to-date with respect to the general information security techniques and processes that are common to information security management, engineering and operations such as key principles and objectives of information security.

6.1.2 Competence: Information security governance

ISO/IEC 27001:2013 clause/subclause (if applicable)	No applicable clauses or subclauses
Intended outcome	Provisioning of high-level direction to the ISMS
Knowledge required	— Business and/or corporate governance frameworks — Information security governance concepts and frameworks — Information security governance standards (e.g. ISO/IEC 27014) — ISMS-specific legal and regulatory issues — Enterprise governance and IT governance and related international standards
Skills required	— Design a governance framework that aligns with/supports the business governance framework — Identify reporting and control requirements — Create, implement and maintain an information security governance framework — Set out the principles of information security governance — Establish organization-wide information security — Adopt a risk-based approach — Set the direction of investment decisions — Ensure conformance with internal and external decisions — Foster a security-positive environment — Understand and determine the scope of legal, regulatory and guideline requirements that can impact the ISMS — Define roles and responsibilities within the framework

6.1.3 Competence: Context of the organization

ISO/IEC 27001:2013 clause/subclause (if applicable)	4.1 Understanding the organization and its context 4.2 Understanding the needs and expectations of interested parties
Intended outcome	Identifying the internal and external issues that could influence the ISMS
Knowledge required	— Methodologies and frameworks for analysing context of the organization — Organizational culture — Information flow diagram — The context of the organization in which the ISMS will be implemented — Legal/regulatory frameworks concerning the ISMS

Skills required	— Determine interested parties related to the ISMS and identify requirements of these interested parties — Determine the scope of the ISMS, boundaries and applicability of the ISMS and stakeholders — Communicate the purpose and benefits of the ISMS to interested parties — State the intended outcome(s) of the ISMS

6.2 ISMS Competence: Information Security Planning

6.2.1 General

To accomplish their roles in an organization successfully and efficiently ISMS professionals shall acquire and keep up-to-date with respect to planning an ISMS.

6.2.2 Competence: Scope of ISMS

ISO/IEC 27001:2013 clause/subclause (if applicable)	4.3 Determining the scope of the ISMS 6.2 Information security objectives and plans to achieve them
Intended outcome	Demonstrating strategic direction with respect to ISMS, ranging from planning to improvement that is organized toward a common goal in information security
Knowledge required	— Information security objectives and planning to achieve them — Information security governance frameworks — Information security policy frameworks
Skills required	— Craft, maintain and communicate information security strategy and policies in alignment with business strategy — Determine interested parties and their requirements — Lead strategic information security planning for the ISMS — Explain the business benefits of adopting the ISMS — Establish ISMS organization relevant to organization's strategy — Understand the issues relevant to organization's purpose and the ISMS — Understand and define the scope of the ISMS — Synthesize needs, expectations and requirements to determine the drivers for the ISMS — Define organizational roles, responsibilities with regard to the ISMS — Understand and generate key performance indicators, key risk indicators and other business measures for the information security strategy and the ISMS

6.2.3 Competence: Information security risk assessment and treatment

ISO/IEC 27001:2013 clause/subclause (if applicable)	6.1 Actions to address risks and opportunities 8.2 Information security risk assessment 8.3 Information security risk treatment
Intended outcome	Applying general risk management techniques (see 5.8 Competence: Risk management) to information security risks
Knowledge required	— Information security risk assessment/treatment methodologies and frameworks — Information security risk assessment — Information security risk treatment — Standards related to risk and information security risk (e.g. ISO 31000 and ISO/IEC 27005) — Controls and control objectives as stated in ISO/IEC 27001:2013, Annex A
Skills required	— Provide direction and guidance in assessing and evaluating information security risks and monitor compliance with information security standards and appropriate information security policies — Determine and address the business risks and opportunities, integrate and implement the actions into ISMS processes — Define and apply the information security risk assessment and treatment processes — Select, implement and improve controls to reduce information security risk — Compare the controls applied with those stated in ISO/IEC 27001:2013, Annex A and verify that no necessary controls have been omitted

6.3 ISMS Competence: Information Security Operation

6.3.1 General

To accomplish their roles in an organization successfully and efficiently ISMS professionals shall acquire and keep up-to-date with respect to operating and running an ISMS.

6.3.2 Competence: Information security operations

ISO/IEC 27001:2013 clause/subclause (if applicable)	8 Operation
Intended outcome	Performing information security-related processes efficiently and effectively
Knowledge required	— Asset management methodologies and frameworks — Access control methodologies and frameworks — Information security engineering methodologies and frameworks — Methodologies and frameworks for physical and environmental protection — Communications security methodologies and frameworks — System acquisition, development and maintenance methodologies and frameworks — Information security incident management methodologies and frameworks — Disaster Recovery methodologies and frameworks — Business continuity methodologies and frameworks — Compliance methodologies and frameworks — Change and configuration management methodologies and frameworks — Information security risk assessment and treatment — Information technologies — Software life cycle frameworks and methodologies — Fundamentals of operation and implementation of widely deployed information security controls — Controls and control objectives as stated in ISO/IEC 27001:2013, Annex A
Skills required	— Manage information security in outsourced processes — Perform information security risk assessment processes — Implement information security risk treatment plan — Measure information security-related processes/operations — Measure information security in other business processes/operations in organization

6.4 ISMS Competence: Information Security Support

6.4.1 General

To accomplish their roles in an organization successfully and efficiently ISMS professionals shall acquire and keep up-to-date with respect to supporting an ISMS.

6.4.2 Competence: Information security awareness, education and training

ISO/IEC 27001:2013 clause/subclause (if applicable)	7.3 Awareness
Intended outcomes	Diffusing an information security culture among the personnel operating within the ISMS
Knowledge required	— Information security awareness, education and training approaches and techniques — Learning approaches and styles — Pedagogical approaches and education delivery methods — Training needs analysis methodologies
Skills required	— Create education and awareness programmes and advise operating units at all levels on the information security policy, their contribution to the effectiveness of the ISMS, best practices — Maintain awareness of the security status of sensitive information systems — Identify awareness, training and education requirements — Generate information security awareness, education and training messages and disseminate to a range of audiences — Evaluate and suggest enforcement mechanisms to support information security culture

6.4.3 Competence: Documentation

ISO/IEC 27001:2013 clause/subclause (if applicable)	6.2 Information security objectives and plans to achieve them 7.5 Documented information
Intended outcome	Controlling the lifecycle of the information security management documentation
Knowledge required	— Documentation required by the ISMS — Tools for production, editing and distribution of documented information — Documentation versioning tools and techniques — Documentation management systems
Skills required	— Determine and provide information that should be documented for the ISMS — Create and change documentation inventory for the ISMS — Manage document changes and version control — Manage templates for shared publications — Organize and control documentation management workflows — Document and catalogue essential processes and procedures

6.5 ISMS Competence: Information Security Performance evaluation

6.5.1 General

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

6.5.2 Competence: ISMS monitoring, measurement, analysis and evaluation

ISO/IEC 27001:2013 clause/subclause (if applicable)	9.1 Monitoring, measurement, analysis and evaluation
Intended outcomes	Evaluating the information security performance and the effectiveness of the ISMS in order to support organizational decisions for continual improvement of the ISMS
Knowledge required	— Characteristics of monitoring and measurement — Aggregation and presentation of quantitative and qualitative data — Trend analysis in information security management and business environment
Skills required	— Monitor, measure and evaluate whether the processes are implemented in accordance with information security policies — Set evaluation criteria and processes for: — ISMS implementation — deployment of management, organizational structure and ISMS resources — quantification of information security incidents — compliance to laws and regulations — Evaluate the ISMS effectiveness — Evaluate for the following items if the ISMS had been precisely implemented: the implementation of management, the organizational structure and ISMS resources were appropriate; information security incidents were reduced; violation of laws and regulations did not happen — Review all system-related information security plans throughout the organization's network, acting as a liaison to Information Systems — Review requested exceptions to information security policies — Analyse the causes and draw lessons from non-achievement of information security objectives

6.5.3 Competence: ISMS auditing

ISO/IEC 27001:2013 clause/subclause (if applicable)	9.2 Internal audit
Intended outcome	Evaluating the ISMS compliance level with external and internal relevant regulation on a periodic basis
Knowledge required	— Information security audit methodologies and frameworks — Internal and external audit processes and procedures — Role and function of audit, both internal and external — Information security assessment, testing and sampling techniques

Skills required	— Manage the internal ISMS audits — Set or influence the scope of information security audit — Analyse the results of one or more information security audits — Propose initiatives, activities, projects and programmes, with associated resource requirements, to address audit findings, recommendations and points — Report against compliance obligations — Scope, lead, manage and participate in information security audits — Write, lead and implement information security testing plans and processes and audit reports — Trend analysis as applied to information security management, ISMS audit results and business environment — Trace indications of information security incidents back to the appropriate elements of the ISMS

6.5.4 Competence: Management review

ISO/IEC 27001:2013 clause/subclause (if applicable)	9.3 Management review 10.1 Nonconformity and corrective action
Intended outcome	Ensuring the continual improvement, adequacy and effectiveness of the ISMS
Knowledge required	— Risk management and techniques — Financial reporting and measurement — Budget management techniques — Cost management and reduction techniques
Skills required	— Determine an appropriate interval to ensure the ISMS effectiveness — Review the ISMS objectives, budgets, business metrics and confirm appropriate actions — Communicate the output of management review to the interested parties as appropriate — Influence the output of management review over information security performance and effectiveness — Preside over a management review meeting successfully

6.6 ISMS Competence: Information Security Improvement

6.6.1 General

To accomplish their roles in an organization successfully and efficiently ISMS professionals shall acquire and keep up-to-date with respect to improving an ISMS.

6.6.2 Competence: Continual improvement

ISO/IEC 27001:2013 clause/subclause (if applicable)	10.2 Continual improvement
Intended outcome	Enabling of a process guiding the continual improvement of all key aspects of the ISMS in a timely manner
Knowledge required	— Continual improvement methodologies and frameworks

Skills required	— Judge whether the current ISMS should be maintained — Implement corrective actions effectively — Determine how the application of a continual improvement process will support the objectives of the ISMS — Suggest corrective actions — Balance the benefits of corrective actions against cost and business disruption — Address new legal and regulatory requirements and obligations — Propose mechanisms to improve the suitability, adequacy and effectiveness of the ISMS

6.6.3 Competence: Technological trends and developments

ISO/IEC 27001:2013 clause/subclause (if applicable)	No applicable clauses or subclauses
Intended outcome	Aligning the current ISMS with the most recent technological innovations with specific attention to information security risks they might mitigate or introduce
Knowledge required	— Emerging technologies and their application
Skills required	— Create a picture of the future technologies, threats and risks and modify the current ISMS to ensure its continued suitability, adequacy and effectiveness — Analyse business impacts of emerging technologies such as Artificial Intelligence

Annex A
(informative)

Including knowledge for ISMS professionals as part of a body of knowledge

This Annex provides elements that can be used in a body of knowledge (BOK) for an organization. An organization may require more knowledge than is stated in this Annex and may create a BOK which is specific to that organization.

A BOK should contain the complete set of concepts, terms and activities that make up an ISMS professional domain, as defined by the relevant learned society or professional association. Table A.1 is illustrative and presents concepts that may be used to create a BOK.

Table A.1 — Examples of ISMS competence for BOK

Category	Competence	Example Knowledge Terms
5 **Business management**	**5.2 Leadership**	commitment, continual improvement, ISMS requirement, inspiration, motivation, influence, negotiation, organizational authority, organizational responsibility, organizational role, purpose of the organization, strategic direction, top management
	5.3 Communication	internal and external issue, presentation, communication management, communication plan, communications security, culture of stakeholders, documentation management, intended audience, internal and external communication, public relations officer, stakeholder management, stakeholder mapping, top management
	5.4 Business strategy and ISMS	business metrics (balanced score card (BSC), key goal indicators (KGI), key performance indicators (KPI), business strategy, legal and regulatory environment
	5.5 Organization design, culture, behaviour and stakeholder management	behaviour analysis/evaluation, motivation control, empowerment, organization, organization design, organizational culture, stakeholder analysis
	5.6 Process design and organizational change management	antivirus software, baseline, configuration management, control, control objective, correction, identification management, information security risk assessment, information security risk treatment, information technology infrastructure library (ITIL), insider threat, objective, process, process maturity model, risk, security data analysis, security information and event management (SIEM), security measures, system log, system monitoring, threat analysis, threat monitoring, vulnerability analysis
	5.7 Human Resource, team and individual management	learning curve, motivation control, empowerment, background verification check, certification, competence, computer based training (CBT), conformity, disciplinary process, end user security training and education, human resource employment, human resource training and education, information security awareness, Information security training program, labour pirating, management responsibility, qualification, role-based training, screening, web based training (WBT)

Table A.1 *(continued)*

	5.8 Risk management	attack, business impact analysis, business risk, communication and consultation, consequence, continual improvement, control, event, information security event, level of risk, likelihood, monitoring, residual risk, review, risk, risk acceptance, risk analysis, risk assessment, risk attitude, risk appetite, risk tolerance, risk communication and consultation, risk criteria, risk evaluation, risk identification, risk management, risk management framework, risk management process, risk owner, risk profile, risk source, risk treatment, stakeholder, threat, vulnerability
	5.9 Resource management	business metrics (BSC, KGI, KPI), review, budget management, budgeting ISMS, cost, costs and benefits of implementing ISMS, expense, finance principles, financial management, financial report, net present value (NPV), internal rate of return (IRR), investment, investment appraisal, return on investment (ROI), key effectiveness indicator, management discipline, return on security investment (ROSI), security KPIs
	5.10 Information systems architecture	configuration management, data, information need, information security requirement (analysis and specification), availability, change management, cloud service, database system, documentation, information processing facilities, information security architecture, information security incident, information system, information system failure, information system architecture, maintainability, maintenance contract, maintenance cost, network architecture, outsourced development, patch management, redevelopment/renovation, reliability, requirement, security specification, security vulnerability analysis, secure coding, secure coding principles, secure development environment, secure development policy, secure system design, secure system engineering principles, software assurance, stability, system acceptance testing, system development life cycle (SDLC), system development project management, system engineering, system security testing, usability
	5.11 Project and portfolio management	control, stakeholder, activity, approval and prioritization, baseline, change request, configuration management, corrective action, critical path, group dynamics, ISMS project, lag, learning curve, project life cycle, project manager, risk register, tender, work breakdown structure (WBS),
	5.12 Supplier management	information security requirement (analysis and specification), stakeholder, business impact analysis, risk analysis, contract management, cost-benefit analysis, disposal, information security forensics, information security policy, interested party, laws and regulations, outsource, prequalification, regulatory compliance, request for proposal (RFP), risk mitigation, risk-based decision, service level agreement (SLA), solicitation, statement of objectives (SOO), statement of work (SOW), total cost of ownership (TCO)
	5.13 Problem management	analysis and synthesis, analytical model, analytical thinking, assessment, cognitive science, critical success factor (CSF), critical thinking, data, decision criteria, derived measure, evaluation, indicator, information need, information security requirement (analysis and specification), internal and external issue, measurement, presentation, problem solving approach, problem solving methodologies, scale, validation
6 ISMS Competence		
6.1 Information Security	**6.1.2 Information security governance**	stakeholder, information security forensics, interested party, executive management, governance, governance of information security, governing body, information security governance framework, information security risk, internal context, organizational goals and objectives, program resource
	6.1.3 Context of the organization	commitment, continual improvement, ISMS requirement, leadership, negotiation, organizational authority, organizational responsibility, organizational role, purpose of the organization, strategic direction, top management

Table A.1 *(continued)*

6.2 Information Security Planning	**6.2.2 Scope of ISMS**	(Information) asset, base measure, business benefits of ISMS, control, control objective, correction, costs and benefits of implementing ISMS, critical success factor (CSF), effectiveness, executive management, external context, information security, information security controls, information security measures, information security policy, information security role and responsibility, ISMS project, key effectiveness indicator, law enforcement authority, management system, mobile device policy, new platform, non-repudiation, object, objective, organization, policy, preventive action, reliability, return on security Investment (ROSI), review of Information security policies, risk, risk acceptance criteria, risk management, risk management process, segregation of duties, special interest groups, teleworking, top management
	6.2.3 Information security risk assessment and treatment	acceptable risk, annual loss expectancy, annual rate of occurrence, attack, availability, backup strategy, baseline, baseline modelling, benchmarking, business continuity, business impact analysis, business metrics (BSC, KGI, KPI), business recovery plan, change management, confidentiality, delegation of authority, digital identity, disaster recovery, event, human resource development, information processing facilities, information security clearance, information security continuity, information security event, information security incident, information security risk assessment, information security risk management, information security risk treatment, information system contingency plan, insider threat, interoperable communications, job rotation, leadership, level of risk, likelihood, management capability, minimum business continuity objective (MBCO), mission assurance, monitoring, nondisclosure agreement, occupant emergency plan, order of succession, position sensitivity, preparedness/readiness, preventive action, recovery point objective (RPO), recovery time objective (RTO), residual risk, risk acceptance, risk acceptance criteria, risk analysis, risk assessment, risk criteria, risk evaluation, risk identification, risk level, risk management process, risk mitigation, risk owner, risk source, risk treatment, security breach, security implementation standard, security incident response, segregation of duties, social engineering, special background investigation (SBI), stakeholder, interested party, information security risk, laws and regulations, availability, information processing facilities, requirement, internal and external issue, organization, attack, confidentiality, information security risk assessment, information security risk management, information security risk treatment, integrity, objective, planning (ISMS process)
6.3 Information Security Operation	**6.3.2 Information security operations**	(information) asset, access control, accreditation, antivirus software, asset management, authentication, availability, backup, baseline sec, cause determination, change management, communications security, computer security incident response team (CSIRT), confidentiality, configuration management, cryptography, disaster recovery, documentation, environmental security, identification management, Incident handling, incident response team, information security architecture, information security engineering, information security forensics, information security incident, information security incident management information security system evaluation, information technology infrastructure library (ITIL), insider threat, integrated development environment, maintainability, maintenance cost, patch management, penetration testing, physical security, preventive maintenance, review method, risk communication and consultation, risk mitigation, security data analysis, security evaluation testing, security measures, security requirements analysis, security specification, security testing and evaluation, security vulnerability analysis, secure coding principles, secure programming techniques, secure system design, software assurance, stability, system acquisition, system development life cycle (SDLC), system development project management, system engineering, system hardening, system log, system monitoring, technical security controls, testing tools, threat analysis, usability

Table A.1 *(continued)*

6.4 Information Security Support	**6.4.2 Information security awareness, education and training**	baseline, computer based training (CBT), curriculum, documentation, end user security training and education, human resource training and education, information security awareness, information security training program, learning curve, learning management system (LMS), learning objectives, needs assessment, role-based training, test(ing), web based training (WBT)
	6.4.3 Documentation	archival, change management, classification, destruction, disposal, documentation criteria, documentation management, documentation methodologies, documentation technologies, documented Information, metadata, ontology, records management, versioning
6.5 Information security Performance evaluation	**6.5.2 ISMS monitoring, measurement, analysis and evaluation**	accountability, analysis and synthesis, assessment, auditing, code of ethics, contract management, control, derived measure, evaluation, governance, guidelines, information security forensics, information security performance, information security policy, laws and regulations, measure, measurement, measurement function, measurement method, measurement result, monitoring nonconformity, performance, privacy principles/fair information practices, procedure, review, review object, review objective standards (international/domestic/industry standards, guidelines, etc.), trusted information communication entity, unit of measurement, validation, verification
	6.5.3 ISMS auditing	audit, audit client, audit conclusion, audit criteria, audit evidence, audit findings, audit method, audit objective, audit plan, audit program, audit scope, audit team, auditee, auditor, authentication, conformity, costs and benefits of implementing ISMS, guide, internal and external audit, ISMS process, ISMS scope and boundary, nonconformity, observer, principles of auditing, risk, scope for audit; audit evidence, technical expert
	6.5.4 Management review	budget management, business metrics (BSC, KGI, KPI), communication management, cost management, financial, management, objective, risk management
6.6 Information Security Improvement	**6.6.2 Continual improvement**	approval and prioritization, cause determination, continual improvement, corrective action, Information security continuity, nonconformity
	6.6.3 Technological trends and developments	critical infrastructure, digital government, information sharing community, new platform, scenario writing, security implementation standard, social vision, technology forecasting methodologies

Bibliography

[1] ISO/IEC 27001:2013, *Information technology — Security techniques — Information security management systems — Requirements*

[2] ISO/IEC 27002, *Information technology — Security techniques — Code of practice for information security controls*

[3] ISO/IEC 27005, *Information technology — Security techniques — Information security risk management*

[4] ISO/IEC 27014, *Information technology — Security techniques — Governance of information security*

ICS 03.100.70; 35.030

Price based on 21 pages