

---

---

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

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

IECNORM.COM : Click to view the full PDF of ISO/IEC 27021:2017



IECNORM.COM : Click to view the full PDF of ISO/IEC 27021:2017



**COPYRIGHT PROTECTED DOCUMENT**

© ISO/IEC 2017, Published in Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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
<b>Foreword</b> .....	<b>v</b>
<b>Introduction</b> .....	<b>vi</b>
<b>1 Scope</b> .....	<b>1</b>
<b>2 Normative references</b> .....	<b>1</b>
<b>3 Terms and definitions</b> .....	<b>1</b>
<b>4 Concept and structure</b> .....	<b>1</b>
4.1 General.....	1
4.2 Concept of ISMS competence.....	2
4.3 Structure of ISMS competence.....	2
4.4 Demonstration of competence.....	3
4.5 Structure of this document.....	3
<b>5 Business management competence for ISMS Professionals</b> .....	<b>3</b>
5.1 General.....	3
5.2 Competence: Leadership.....	3
5.3 Competence: Communication.....	4
5.4 Competence: Business Strategy and ISMS.....	4
5.5 Competence: Organization design, culture, behaviour and stakeholder management.....	5
5.6 Competence: Process design and organizational change management.....	5
5.7 Competence: Human Resource, team and individual management.....	6
5.8 Competence: Risk management.....	6
5.9 Competence: Resource management.....	7
5.10 Competence: Information systems architecture.....	7
5.11 Competence: Project and portfolio management.....	8
5.12 Competence: Supplier management.....	8
5.13 Competence: Problem management.....	8
<b>6 Information security competence for ISMS professionals</b> .....	<b>9</b>
6.1 ISMS Competence: Information Security.....	9
6.1.1 General.....	9
6.1.2 Competence: Information security governance.....	9
6.1.3 Competence: Context of the organization.....	9
6.2 ISMS Competence: Information Security Planning.....	10
6.2.1 General.....	10
6.2.2 Competence: Scope of ISMS.....	10
6.2.3 Competence: Information security risk assessment and treatment.....	11
6.3 ISMS Competence: Information Security Operation.....	11
6.3.1 General.....	11
6.3.2 Competence: Information security operations.....	12
6.4 ISMS Competence: Information Security Support.....	12
6.4.1 General.....	12
6.4.2 Competence: Information security awareness, education and training.....	13
6.4.3 Competence: Documentation.....	13
6.5 ISMS Competence: Information Security Performance evaluation.....	13
6.5.1 General.....	13
6.5.2 Competence: ISMS monitoring, measurement, analysis and evaluation.....	14
6.5.3 Competence: ISMS auditing.....	14
6.5.4 Competence: Management review.....	15
6.6 ISMS Competence: Information Security Improvement.....	15
6.6.1 General.....	15
6.6.2 Competence: Continual improvement.....	15
6.6.3 Competence: Technological trends and developments.....	16
<b>Annex A (informative) Including knowledge for ISMS professionals as part of a body of knowledge</b> .....	<b>17</b>

**Bibliography** ..... **21**

IECNORM.COM : Click to view the full PDF of ISO/IEC 27021:2017

## 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](http://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](http://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](http://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.

IECNORM.COM : Click to view the full PDF of ISO/IEC 27021:2017

# 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](#).

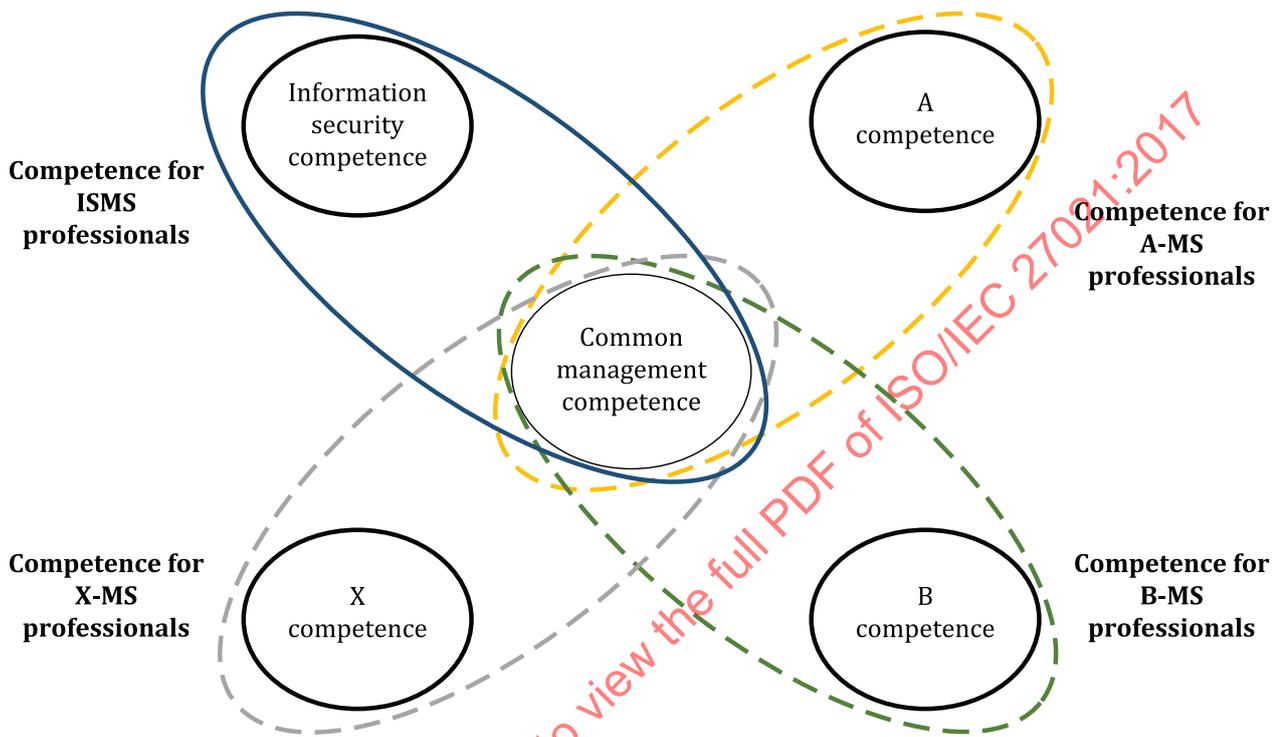


Figure 1 — Relationship of ISMS-specific competence with common and domain-specific competence

### 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

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

<b>ISO/IEC 27001:2013 clause/subclause (if applicable)</b>	5 Leadership
<b>Intended outcome</b>	Directing, motivating and encouraging staff across the organization to deliver information security
<b>Knowledge required</b>	<ul style="list-style-type: none"> <li>— Theories of leadership</li> <li>— Negotiation techniques</li> </ul>

<b>Skills required</b>	<ul style="list-style-type: none"> <li>— Set and give direction for information security across the organization</li> <li>— Provide guidance, set objectives and drive progress within the information security function, team and the business</li> <li>— Deliver commitments</li> <li>— Deploy responsibilities and authorities at the different levels of the organization</li> </ul>
------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

**5.3 Competence: Communication**

<b>ISO/IEC 27001:2013 clause/subclause (if applicable)</b>	7.4 Communication
<b>Intended outcome</b>	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
<b>Knowledge required</b>	<ul style="list-style-type: none"> <li>— Theories and methods of communication</li> <li>— Stakeholder analysis techniques</li> <li>— Communication techniques</li> </ul>
<b>Skills required</b>	<ul style="list-style-type: none"> <li>— Design the process and communication channels appropriate for the organization to establish the ISMS</li> <li>— Communicate using appropriate language and media to a range of audiences</li> <li>— Forge relationships with top management and business professionals</li> <li>— Determine the need for internal and external communications relevant the ISMS</li> </ul>

**5.4 Competence: Business Strategy and ISMS**

<b>ISO/IEC 27001:2013 clause/subclause (if applicable)</b>	4.1 Understanding the organization and its context
<b>Intended outcome</b>	Understanding how business strategy is formulated and how information security and ISMS strategy fits into the overall business strategy
<b>Knowledge required</b>	<ul style="list-style-type: none"> <li>— Business strategy and strategy formulation process</li> <li>— The legal and regulatory environment in which the organization operates</li> <li>— Definition of strategy, for example, by using a strategic alignment tree</li> <li>— Application of strategic objectives and ISMS global objectives to the different process of the ISMS</li> </ul>
<b>Skills required</b>	<ul style="list-style-type: none"> <li>— Understand business strategy and the strategy of the organization</li> <li>— Set information security objectives in the context of the business and its strategy</li> <li>— Demonstrate strategic direction with respect to the ISMS, ranging from planning to improvement that is organized toward common goals in information security</li> <li>— Allocate (or assist in the allocation of) resources to meet business and information security objectives</li> </ul>

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

<b>ISO/IEC 27001:2013 clause/subclause (if applicable)</b>	4.2 Understanding the needs and expectations of interested parties
<b>Intended outcome</b>	Ensuring that the ISMS implementation matches the organizational structure and culture
<b>Knowledge required</b>	<ul style="list-style-type: none"> <li>— Organization design theory</li> <li>— Theory of organization culture</li> <li>— Organizational behaviour approaches, methodologies and frameworks</li> <li>— Conflict management</li> </ul>
<b>Skills required</b>	<ul style="list-style-type: none"> <li>— Understand organization design</li> <li>— Understand organization behaviour</li> <li>— Analyse and evaluate organization culture</li> <li>— Integrate the ISMS into organization design</li> <li>— Manage conflict stakeholders with different interests and negotiate in order to accomplish security objectives</li> </ul>

### 5.6 Competence: Process design and organizational change management

<b>ISO/IEC 27001:2013 clause/subclause (if applicable)</b>	No applicable clauses or subclauses
<b>Intended outcome</b>	Engineering of the performance of day-by-day information security related activities
<b>Knowledge required</b>	<ul style="list-style-type: none"> <li>— Operational planning and control</li> <li>— Process design methodologies and frameworks</li> <li>— Process documentation and record management</li> <li>— Organizational context</li> <li>— Change management methodologies and frameworks</li> </ul>
<b>Skills required</b>	<ul style="list-style-type: none"> <li>— Direct processes, and oversee the plans to achieve information security objectives</li> <li>— Manage organizational processes</li> <li>— Manage outsourced processes</li> <li>— Manage change management processes</li> <li>— Manage records</li> </ul>

**5.7 Competence: Human Resource, team and individual management**

<b>ISO/IEC 27001:2013 clause/subclause (if applicable)</b>	7.2 Competence
<b>Intended outcome</b>	Taking proactive action and developing organizational processes to address the development needs of individuals, teams and the entire workforce
<b>Knowledge required</b>	<ul style="list-style-type: none"> <li>— Appraisal systems and processes</li> <li>— Competence development methods</li> <li>— Competence needs analysis methodologies</li> <li>— Learning and development support methods (e.g. coaching, teaching, training)</li> <li>— The optimum staffing and skills required to implement and maintain the ISMS</li> <li>— Information security qualifications and certifications</li> </ul>
<b>Skills required</b>	<ul style="list-style-type: none"> <li>— Set organizational and individual objectives, goals and targets and link them</li> <li>— Understand and use strategies such as empowerment</li> <li>— Measure and influence the level of employee motivation</li> <li>— Use tools such as performance management, objective setting and appraisals</li> <li>— Coach and/or train and/or mentor individuals or teams</li> <li>— Work in cross-functional teams to achieve business and/or information security objectives</li> <li>— Build a team work culture</li> <li>— Support the specification, interview, recruitment, selection, training, supervision and development of staff with appropriate skills, experience and motivation</li> <li>— Measure the results of training, coaching and related actions and the acquisition of the skills</li> </ul>

**5.8 Competence: Risk management**

<b>ISO/IEC 27001:2013 clause/subclause (if applicable)</b>	No applicable clauses or subclauses
<b>Intended outcome</b>	Understanding of the methodologies, frameworks and outputs of risk management
<b>Knowledge required</b>	<ul style="list-style-type: none"> <li>— Fundamental principles of risk</li> <li>— Business risk management methodologies and frameworks, risk assessment treatment</li> <li>— The legal and regulatory environment the organization operates in</li> </ul>
<b>Skills required</b>	<ul style="list-style-type: none"> <li>— Understand the definition of risk and its components in real-world scenarios</li> <li>— Comprehend business risk management methodologies, assessment and treatment methodologies and processes</li> <li>— Explain the outputs of business or enterprise risk management</li> </ul>

### 5.9 Competence: Resource management

<b>ISO/IEC 27001:2013 clause/subclause (if applicable)</b>	7.1 Resources
<b>Intended outcome</b>	Ensuring that appropriate resources are determined and provided in time for the establishment, implementation, maintenance and continual improvement of the ISMS
<b>Knowledge required</b>	<ul style="list-style-type: none"> <li>— Financial reporting and measurement</li> <li>— Budget creation and management techniques</li> <li>— Cost management and reduction techniques</li> <li>— Time and materials management techniques</li> <li>— Management review and corrective action processes</li> </ul>
<b>Skills required</b>	<ul style="list-style-type: none"> <li>— Determine the resources needed for the establishment, implementation, maintenance and continual improvement of the ISMS</li> <li>— Budget business elements including cost of implementation and operation of the ISMS</li> <li>— Understand financial reporting, including cashflow and profit and loss</li> <li>— Create business and investment cases</li> <li>— State ROI (return on investment), ROSI (return on security investment) and other financial benefits</li> <li>— Apply cost control and budget management techniques</li> <li>— Provide appropriate resources in time in the right place</li> </ul>

### 5.10 Competence: Information systems architecture

<b>ISO/IEC 27001:2013 clause/subclause (if applicable)</b>	No applicable clauses or subclauses
<b>Intended outcome</b>	Understanding the applicable information systems architecture used to create, store, process, transmit and dispose of the organization's information
<b>Knowledge required</b>	<ul style="list-style-type: none"> <li>— Information systems architecture requirements</li> <li>— Hardware components, tools and hardware architectures</li> <li>— Operating systems and software platforms</li> <li>— Integration of, and dependency on, business processes with ICT applications</li> <li>— Information security aspects of information systems architecture</li> </ul>
<b>Skills required</b>	<ul style="list-style-type: none"> <li>— Understand the business objectives/drivers that impact the information systems architecture</li> <li>— Understand the interaction of security components and information system architecture components</li> </ul>

**5.11 Competence: Project and portfolio management**

<b>ISO/IEC 27001:2013 clause/subclause (if applicable)</b>	No applicable clauses or subclauses
<b>Intended outcome</b>	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
<b>Knowledge required</b>	<ul style="list-style-type: none"> <li>— Project management methodologies and frameworks</li> <li>— Portfolio management methodologies and frameworks</li> <li>— Approaches to define project steps and tools to set up action plans</li> </ul>
<b>Skills required</b>	<ul style="list-style-type: none"> <li>— Manage projects, portfolio, activities and tasks</li> <li>— Manage, with the business, the portfolio of ISMS-related investment projects</li> <li>— Plan projects to implement strategies, establish procedures and implement them successfully and efficiently</li> <li>— Work in cross-disciplinary teams to achieve business and/or information security objectives</li> </ul>

**5.12 Competence: Supplier management**

<b>ISO/IEC 27001:2013 clause/subclause (if applicable)</b>	No applicable clauses or subclauses
<b>Intended outcome</b>	Understanding the role of suppliers and the supply chain in the organization and the impact on information security
<b>Knowledge required</b>	<ul style="list-style-type: none"> <li>— Use of suppliers and the supply chain</li> </ul>
<b>Skills required</b>	<ul style="list-style-type: none"> <li>— Assess suppliers and the supply chain(s)</li> <li>— Assess the impact on information security of suppliers and the supply chain(s)</li> <li>— Manage suppliers where required</li> <li>— Provide information security guidance when creating, assessing, selecting, managing and exiting supplier relationships</li> </ul>

**5.13 Competence: Problem management**

<b>ISO/IEC 27001:2013 clause/subclause (if applicable)</b>	No applicable clauses or subclauses
<b>Intended outcome</b>	Identifying and resolving problems that might have consequences for the ISMS in a timely manner
<b>Knowledge required</b>	<ul style="list-style-type: none"> <li>— Problem solving and analysis methodologies and frameworks</li> </ul>
<b>Skills required</b>	<ul style="list-style-type: none"> <li>— Understand internal and external issues</li> <li>— Analyse and synthesize information and data concerning the problems</li> <li>— Describe management problems analytically, apply analytical approaches, and elaborate problem solutions</li> <li>— Present and explain proposed solutions to relevant audiences</li> </ul>

## 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

<b>ISO/IEC 27001:2013 clause/subclause (if applicable)</b>	No applicable clauses or subclauses
<b>Intended outcome</b>	Provisioning of high-level direction to the ISMS
<b>Knowledge required</b>	<ul style="list-style-type: none"> <li>— Business and/or corporate governance frameworks</li> <li>— Information security governance concepts and frameworks</li> <li>— Information security governance standards (e.g. ISO/IEC 27014)</li> <li>— ISMS-specific legal and regulatory issues</li> <li>— Enterprise governance and IT governance and related international standards</li> </ul>
<b>Skills required</b>	<ul style="list-style-type: none"> <li>— Design a governance framework that aligns with/supports the business governance framework</li> <li>— Identify reporting and control requirements</li> <li>— Create, implement and maintain an information security governance framework</li> <li>— Set out the principles of information security governance               <ul style="list-style-type: none"> <li>— Establish organization-wide information security</li> <li>— Adopt a risk-based approach</li> <li>— Set the direction of investment decisions</li> <li>— Ensure conformance with internal and external decisions</li> <li>— Foster a security-positive environment</li> </ul> </li> <li>— Understand and determine the scope of legal, regulatory and guideline requirements that can impact the ISMS</li> <li>— Define roles and responsibilities within the framework</li> </ul>

#### 6.1.3 Competence: Context of the organization

<b>ISO/IEC 27001:2013 clause/subclause (if applicable)</b>	4.1 Understanding the organization and its context 4.2 Understanding the needs and expectations of interested parties
<b>Intended outcome</b>	Identifying the internal and external issues that could influence the ISMS
<b>Knowledge required</b>	<ul style="list-style-type: none"> <li>— Methodologies and frameworks for analysing context of the organization</li> <li>— Organizational culture</li> <li>— Information flow diagram</li> <li>— The context of the organization in which the ISMS will be implemented</li> <li>— Legal/regulatory frameworks concerning the ISMS</li> </ul>

<b>Skills required</b>	<ul style="list-style-type: none"> <li>— Determine interested parties related to the ISMS and identify requirements of these interested parties</li> <li>— Determine the scope of the ISMS, boundaries and applicability of the ISMS and stakeholders</li> <li>— Communicate the purpose and benefits of the ISMS to interested parties</li> <li>— State the intended outcome(s) of the ISMS</li> </ul>
------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

## 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

<b>ISO/IEC 27001:2013 clause/subclause (if applicable)</b>	<p>4.3 Determining the scope of the ISMS</p> <p>6.2 Information security objectives and plans to achieve them</p>
<b>Intended outcome</b>	Demonstrating strategic direction with respect to ISMS, ranging from planning to improvement that is organized toward a common goal in information security
<b>Knowledge required</b>	<ul style="list-style-type: none"> <li>— Information security objectives and planning to achieve them</li> <li>— Information security governance frameworks</li> <li>— Information security policy frameworks</li> </ul>
<b>Skills required</b>	<ul style="list-style-type: none"> <li>— Craft, maintain and communicate information security strategy and policies in alignment with business strategy</li> <li>— Determine interested parties and their requirements</li> <li>— Lead strategic information security planning for the ISMS</li> <li>— Explain the business benefits of adopting the ISMS</li> <li>— Establish ISMS organization relevant to organization’s strategy</li> <li>— Understand the issues relevant to organization’s purpose and the ISMS</li> <li>— Understand and define the scope of the ISMS</li> <li>— Synthesize needs, expectations and requirements to determine the drivers for the ISMS</li> <li>— Define organizational roles, responsibilities with regard to the ISMS</li> <li>— Understand and generate key performance indicators, key risk indicators and other business measures for the information security strategy and the ISMS</li> </ul>

### 6.2.3 Competence: Information security risk assessment and treatment

<b>ISO/IEC 27001:2013 clause/subclause (if applicable)</b>	6.1 Actions to address risks and opportunities 8.2 Information security risk assessment 8.3 Information security risk treatment
<b>Intended outcome</b>	Applying general risk management techniques (see 5.8 Competence: Risk management) to information security risks
<b>Knowledge required</b>	<ul style="list-style-type: none"> <li>— Information security risk assessment/treatment methodologies and frameworks</li> <li>— Information security risk assessment</li> <li>— Information security risk treatment</li> <li>— Standards related to risk and information security risk (e.g. ISO 31000 and ISO/IEC 27005)</li> <li>— Controls and control objectives as stated in ISO/IEC 27001:2013, Annex A</li> </ul>
<b>Skills required</b>	<ul style="list-style-type: none"> <li>— Provide direction and guidance in assessing and evaluating information security risks and monitor compliance with information security standards and appropriate information security policies</li> <li>— Determine and address the business risks and opportunities, integrate and implement the actions into ISMS processes</li> <li>— Define and apply the information security risk assessment and treatment processes</li> <li>— Select, implement and improve controls to reduce information security risk</li> <li>— Compare the controls applied with those stated in ISO/IEC 27001:2013, Annex A and verify that no necessary controls have been omitted</li> </ul>

## 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

<b>ISO/IEC 27001:2013 clause/subclause (if applicable)</b>	8 Operation
<b>Intended outcome</b>	Performing information security-related processes efficiently and effectively
<b>Knowledge required</b>	<ul style="list-style-type: none"> <li>— Asset management methodologies and frameworks</li> <li>— Access control methodologies and frameworks</li> <li>— Information security engineering methodologies and frameworks</li> <li>— Methodologies and frameworks for physical and environmental protection</li> <li>— Communications security methodologies and frameworks</li> <li>— System acquisition, development and maintenance methodologies and frameworks</li> <li>— Information security incident management methodologies and frameworks</li> <li>— Disaster Recovery methodologies and frameworks</li> <li>— Business continuity methodologies and frameworks</li> <li>— Compliance methodologies and frameworks</li> <li>— Change and configuration management methodologies and frameworks</li> <li>— Information security risk assessment and treatment</li> <li>— Information technologies</li> <li>— Software life cycle frameworks and methodologies</li> <li>— Fundamentals of operation and implementation of widely deployed information security controls</li> <li>— Controls and control objectives as stated in ISO/IEC 27001:2013, Annex A</li> </ul>
<b>Skills required</b>	<ul style="list-style-type: none"> <li>— Manage information security in outsourced processes</li> <li>— Perform information security risk assessment processes</li> <li>— Implement information security risk treatment plan</li> <li>— Measure information security-related processes/operations</li> <li>— Measure information security in other business processes/operations in organization</li> </ul>

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

<b>ISO/IEC 27001:2013 clause/subclause (if applicable)</b>	7.3 Awareness
<b>Intended outcomes</b>	Diffusing an information security culture among the personnel operating within the ISMS
<b>Knowledge required</b>	<ul style="list-style-type: none"> <li>— Information security awareness, education and training approaches and techniques</li> <li>— Learning approaches and styles</li> <li>— Pedagogical approaches and education delivery methods</li> <li>— Training needs analysis methodologies</li> </ul>
<b>Skills required</b>	<ul style="list-style-type: none"> <li>— 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</li> <li>— Maintain awareness of the security status of sensitive information systems</li> <li>— Identify awareness, training and education requirements</li> <li>— Generate information security awareness, education and training messages and disseminate to a range of audiences</li> <li>— Evaluate and suggest enforcement mechanisms to support information security culture</li> </ul>

#### 6.4.3 Competence: Documentation

<b>ISO/IEC 27001:2013 clause/subclause (if applicable)</b>	6.2 Information security objectives and plans to achieve them 7.5 Documented information
<b>Intended outcome</b>	Controlling the lifecycle of the information security management documentation
<b>Knowledge required</b>	<ul style="list-style-type: none"> <li>— Documentation required by the ISMS</li> <li>— Tools for production, editing and distribution of documented information</li> <li>— Documentation versioning tools and techniques</li> <li>— Documentation management systems</li> </ul>
<b>Skills required</b>	<ul style="list-style-type: none"> <li>— Determine and provide information that should be documented for the ISMS</li> <li>— Create and change documentation inventory for the ISMS</li> <li>— Manage document changes and version control</li> <li>— Manage templates for shared publications</li> <li>— Organize and control documentation management workflows</li> <li>— Document and catalogue essential processes and procedures</li> </ul>

### 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

<b>ISO/IEC 27001:2013 clause/subclause (if applicable)</b>	9.1 Monitoring, measurement, analysis and evaluation
<b>Intended outcomes</b>	Evaluating the information security performance and the effectiveness of the ISMS in order to support organizational decisions for continual improvement of the ISMS
<b>Knowledge required</b>	<ul style="list-style-type: none"> <li>— Characteristics of monitoring and measurement</li> <li>— Aggregation and presentation of quantitative and qualitative data</li> <li>— Trend analysis in information security management and business environment</li> </ul>
<b>Skills required</b>	<ul style="list-style-type: none"> <li>— Monitor, measure and evaluate whether the processes are implemented in accordance with information security policies</li> <li>— Set evaluation criteria and processes for:                             <ul style="list-style-type: none"> <li>— ISMS implementation</li> <li>— deployment of management, organizational structure and ISMS resources</li> <li>— quantification of information security incidents</li> <li>— compliance to laws and regulations</li> </ul> </li> <li>— Evaluate the ISMS effectiveness</li> <li>— 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</li> <li>— Review all system-related information security plans throughout the organization's network, acting as a liaison to Information Systems</li> <li>— Review requested exceptions to information security policies</li> <li>— Analyse the causes and draw lessons from non-achievement of information security objectives</li> </ul>

6.5.3 Competence: ISMS auditing

<b>ISO/IEC 27001:2013 clause/subclause (if applicable)</b>	9.2 Internal audit
<b>Intended outcome</b>	Evaluating the ISMS compliance level with external and internal relevant regulation on a periodic basis
<b>Knowledge required</b>	<ul style="list-style-type: none"> <li>— Information security audit methodologies and frameworks</li> <li>— Internal and external audit processes and procedures</li> <li>— Role and function of audit, both internal and external</li> <li>— Information security assessment, testing and sampling techniques</li> </ul>

<b>Skills required</b>	<ul style="list-style-type: none"> <li>— Manage the internal ISMS audits</li> <li>— Set or influence the scope of information security audit</li> <li>— Analyse the results of one or more information security audits</li> <li>— Propose initiatives, activities, projects and programmes, with associated resource requirements, to address audit findings, recommendations and points</li> <li>— Report against compliance obligations</li> <li>— Scope, lead, manage and participate in information security audits</li> <li>— Write, lead and implement information security testing plans and processes and audit reports</li> <li>— Trend analysis as applied to information security management, ISMS audit results and business environment</li> <li>— Trace indications of information security incidents back to the appropriate elements of the ISMS</li> </ul>
------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

**6.5.4 Competence: Management review**

<b>ISO/IEC 27001:2013 clause/subclause (if applicable)</b>	9.3 Management review 10.1 Nonconformity and corrective action
<b>Intended outcome</b>	Ensuring the continual improvement, adequacy and effectiveness of the ISMS
<b>Knowledge required</b>	<ul style="list-style-type: none"> <li>— Risk management and techniques</li> <li>— Financial reporting and measurement</li> <li>— Budget management techniques</li> <li>— Cost management and reduction techniques</li> </ul>
<b>Skills required</b>	<ul style="list-style-type: none"> <li>— Determine an appropriate interval to ensure the ISMS effectiveness</li> <li>— Review the ISMS objectives, budgets, business metrics and confirm appropriate actions</li> <li>— Communicate the output of management review to the interested parties as appropriate</li> <li>— Influence the output of management review over information security performance and effectiveness</li> <li>— Preside over a management review meeting successfully</li> </ul>

**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**

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

<b>Skills required</b>	<ul style="list-style-type: none"> <li>— Judge whether the current ISMS should be maintained</li> <li>— Implement corrective actions effectively</li> <li>— Determine how the application of a continual improvement process will support the objectives of the ISMS</li> <li>— Suggest corrective actions</li> <li>— Balance the benefits of corrective actions against cost and business disruption</li> <li>— Address new legal and regulatory requirements and obligations</li> <li>— Propose mechanisms to improve the suitability, adequacy and effectiveness of the ISMS</li> </ul>
------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

**6.6.3 Competence: Technological trends and developments**

<b>ISO/IEC 27001:2013 clause/subclause (if applicable)</b>	No applicable clauses or subclauses
<b>Intended outcome</b>	Aligning the current ISMS with the most recent technological innovations with specific attention to information security risks they might mitigate or introduce
<b>Knowledge required</b>	<ul style="list-style-type: none"> <li>— Emerging technologies and their application</li> </ul>
<b>Skills required</b>	<ul style="list-style-type: none"> <li>— Create a picture of the future technologies, threats and risks and modify the current ISMS to ensure its continued suitability, adequacy and effectiveness</li> <li>— Analyse business impacts of emerging technologies such as Artificial Intelligence</li> </ul>

IECNORM.COM : Click to view the full PDF of ISO/IEC 27021:2017