

~~Date: ISO/IEC FDIS 27006-1:2023-08-09(E)~~

ISO/IEC JTC_1/SC 27

~~Date: 2023-08-09~~

~~ISO/IEC DIS 27006-1.2:2023(E)~~

~~ISO/IEC JTC 1/SC 27/WG 1~~

Secretariat: DIN

~~Date: 2023-10-18~~

Information security, cybersecurity and privacy protection — Requirements for bodies providing audit and certification of information security management systems — Part 1: General

~~Exigences pour les organismes procédant à l'audit et à la certification des systèmes de management de la sécurité de l'information — Partie 1 : Généralités~~

iTeh Standards
(<https://standards.iteh.ai>)
Document Preview

ISO/IEC FDIS 27006-1

<https://standards.iteh.ai/catalog/standards/sist/ee9551dd-1fbf-4c83-a38d-d9e3cb8cf644/iso-iec-fdis-27006-1>

Edited DIS - MUST BE USED FOR FINAL DRAFT

Style Definition: Heading 1: Indent: Left: 0 cm, First line: 0 cm, Tab stops: Not at 0.76 cm
Style Definition: Heading 2: Font: Bold, Tab stops: Not at 0.63 cm
Style Definition: Heading 3: Font: Bold
Style Definition: Heading 4: Font: Bold
Style Definition: Heading 5: Font: Bold
Style Definition: Heading 6: Font: Bold
Style Definition: ANNEX
Style Definition: AMEND Terms Heading: Font: Bold
Style Definition: AMEND Heading 1 Unnumbered: Font: Bold
Formatted: Left: 1.5 cm, Top: 1.4 cm, Footer distance from edge: 0.5 cm
Formatted: English (United Kingdom)
Formatted: English (United Kingdom)
Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

Formatted: Font: 11.5 pt

Formatted: Font: 11.5 pt

© ISO/IEC 2023

All rights reserved. Unless otherwise specified, or required in the context of its implementation, 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.

Formatted: Adjust space between Latin and Asian text, Adjust space between Asian text and numbers

Formatted: Default Paragraph Font

Formatted: Default Paragraph Font

ISO ~~copyright office~~ Copyright Office

CP 401 • Ch. de Blandonnet 8

CH-1214 Vernier, Geneva

Phone: +41 22 749 01 11

Email: copyright@iso.org

Email: copyright@iso.org

Website: www.iso.org

Published in Switzerland.

Formatted: Adjust space between Latin and Asian text, Adjust space between Asian text and numbers

Formatted: Adjust space between Latin and Asian text, Adjust space between Asian text and numbers

iTeh Standards

(<https://standards.iteh.ai>)
Document Preview

ISO/IEC FDIS 27006-1

<https://standards.iteh.ai/catalog/standards/sist/ee9551dd-1fbf-4c83-a38d-d9e3cb8cf644/iso-iec-fdis-27006-1>

Formatted: English (United Kingdom)

Formatted: Font: 9 pt

Formatted: Left, Space Before: 18 pt, Line spacing: Exactly 12 pt

Formatted: English (United Kingdom)

Formatted: Font: 9 pt

Formatted: Font: 9 pt

Formatted: Font: 9 pt

Formatted: Font: 11 pt

Formatted: Space Before: 18 pt, Line spacing: Exactly 12 pt

Formatted: Font: 11.5 pt

Formatted: Font: 11.5 pt

Contents

Page

Formatted: Font: Not Bold

Foreword 6

Introduction 8

1 Scope 1

2 Normative references 1

3 Terms and definitions 1

4 Principles 5

5 General requirements 5

5.1 Legal and contractual matters 5

5.2 Management of impartiality 5

5.2.1 General 5

5.2.2 Conflicts of interest 5

5.3 Liability and financing 5

6 Structural requirements 5

7 Resource requirements 6

7.1 Competence of personnel 6

7.1.1 General 6

7.1.2 Generic competence requirements 6

7.1.3 Determination of competence criteria 6

7.2 Personnel involved in the certification activities 9

7.2.1 General 9

7.2.2 Demonstration of auditor knowledge and experience 9

7.3 Use of individual external auditors and external technical experts 10

7.4 Personnel records 10

7.5 Outsourcing 10

8 Information requirements 10

8.1 Public information 10

8.2 Certification documents 10

8.2.1 General 10

8.2.2 ISMS Certification documents 10

8.2.3 Reference of other standards in the ISMS certification documents 10

8.3 Reference to certification and use of marks 11

8.4 Confidentiality 11

8.4.1 General 11

8.4.2 Access to organizational records 11

8.5 Information exchange between a certification body and its clients 11

9 Process requirements 11

9.1 Pre-certification activities 11

9.1.1 Application 11

9.1.2 Application review 12

9.1.3 Audit programme 12

9.1.4 Determining audit time 13

9.1.5 Multi-site sampling 13

9.1.6 Multiple management systems 15

Top Standards
https://standards.itohai.com/management/Preview

https://standards.itohai.com/standards/3cb8cf644/iso-iec-fdis-27006-1

Formatted: Font: 9 pt

Formatted: Left, Space Before: 18 pt, Line spacing: Exactly 12 pt

Formatted: Font: 9 pt

Formatted: Font: 11 pt, Not Bold

Formatted: Font: 9 pt

Formatted: Font: 9 pt

Formatted: Space Before: 18 pt, Line spacing: Exactly 12 pt

Formatted: Font: 11.5 pt

Formatted: Font: 11.5 pt

9.2	Planning audits	15
9.2.1	Determining audit objectives, scope and criteria	15
9.2.2	Audit team selection and assignments	15
9.2.3	Audit plan	16
9.3	Initial certification	16
9.3.1	General	16
9.3.2	Initial certification audit	16
9.4	Conducting audits	17
9.4.1	General	17
9.4.2	Specific elements of the ISMS audit	17
9.4.3	Audit report	18
9.5	Certification decision	18
9.5.1	General	18
9.5.2	Certification decision	18
9.6	Maintaining certification	19
9.6.1	General	19
9.6.2	Surveillance activities	19
9.6.3	Re-certification	20
9.6.4	Special audits	20
9.6.5	Suspending, withdrawing or reducing the scope of certification	20
9.7	Appeals	20
9.8	Complaints	20
9.8.1	General	20
9.8.2	Complaints	20
9.9	Client records	20
10	Management system requirements for certification bodies	20
10.1	Options	20
10.1.1	General	20
10.1.2	ISMS implementation	20
10.2	Option A: General management system requirements	21
10.3	Option B: Management system requirements in accordance with ISO 9001	21
Annex A (normative)	Knowledge and skills for ISMS auditing and certification	22
A.1	Overview	22
Annex B (informative)	Further competence considerations	23
B.1	General competence considerations	23
B.2	Specific knowledge and experience considerations	23
B.2.1	Typical knowledge related to ISMS	23
Annex C (normative)	Audit time	25
C.1	General	25
C.2	Concepts	26
C.2.1	Number of persons doing work under the organization's control	26
C.2.2	Auditor day	26
C.2.3	Temporary site	26
C.3	Procedure for determining audit time for initial audit	26
C.3.1	General	26
C.3.2	Remote methods for conducting audit	26

Formatted: English (United Kingdom)

Formatted: Left, Space Before: 18 pt, Line spacing: Exactly 12 pt

Formatted: English (United Kingdom)

Formatted: Font: 9 pt

Formatted: Font: 9 pt

Formatted: Font: 9 pt

Formatted: Font: 9 pt

Formatted: Font: 11 pt

Formatted: Space Before: 18 pt, Line spacing: Exactly 12 pt

Formatted: Font: 11.5 pt

Formatted: Font: 11.5 pt

C.3.3 Audit time calculation 27

C.3.4 Determination of initial number of persons 27

C.3.5 Factors for adjustment of audit time 28

C.3.6 Limitation of deviation of audit time 29

C.3.7 On-site audit time 29

C.4 Audit time for surveillance audits 30

C.5 Audit time for re-certification audit 30

C.6 Audit time of multi-site 30

C.7 Audit time for scope extensions 30

Annex D (informative) Methods for audit time calculations 32

D.1 General 32

D.2 Classification of factors for calculating audit time 32

D.3 Example for audit time calculation 34

Annex E (informative) Guidance for review of implemented ISO/IEC 27001:2022, Annex A controls 37

E.1 Purpose 37

E.2 How to use Table E.1 37

E.2.1 General 37

E.2.2 Column "system testing" 37

E.2.3 Column "Visual inspection" 38

E.2.4 Possible evidence of design and implementation of controls 38

Bibliography 55

Foreword v

Introduction vii

1 Scope 1

2 Normative references 1

3 Terms and definitions 1

4 Principles 5

5 General requirements 5

5.1 Legal and contractual matters 5

5.2 Management of impartiality 5

5.2.1 General 5

5.2.2 Conflicts of interest 5

5.3 Liability and financing 5

6 Structural requirements 5

7 Resource requirements 6

7.1 Competence of personnel 6

7.1.1 General 6

7.1.2 Generic competence requirements 6

7.1.3 Determination of competence criteria 6

7.2 Personnel involved in the certification activities 9

Formatted: Font: 9 pt

Formatted: Left, Space Before: 18 pt, Line spacing: Exactly 12 pt

Formatted: Font: 9 pt

Formatted: Font: 9 pt

Formatted: Font: 11 pt, Not Bold

Formatted: Font: 9 pt

Formatted: Space Before: 18 pt, Line spacing: Exactly 12 pt

Formatted: Font: 11.5 pt

Formatted: Font: 11.5 pt

7.2.1 General..... 9

7.2.2 Demonstration of auditor knowledge and experience..... 9

7.3 Use of individual external auditors and external technical experts 10

7.4 Personnel records..... 10

7.5 Outsourcing..... 10

8 Information requirements..... 10

8.1 Public information..... 10

8.2 Certification documents 10

8.2.1 General..... 10

8.2.2 ISMS Certification documents..... 10

8.2.3 Reference of other standards in the ISMS certification documents..... 10

8.3 Reference to certification and use of marks..... 11

8.4 Confidentiality..... 11

8.4.1 General..... 11

8.4.2 Access to organizational records..... 11

8.5 Information exchange between a certification body and its clients..... 11

9 Process requirements 11

9.1 Pre-certification activities 11

9.1.1 Application 11

9.1.2 Application review..... 12

9.1.3 Audit programme..... 12

9.1.4 Determining audit time..... 13

9.1.5 Multi-site sampling 13

9.1.6 Multiple management systems 15

9.2 Planning audits 15

9.2.1 Determining audit objectives, scope and criteria 15

9.2.2 Audit team selection and assignments..... 15

9.2.3 Audit plan..... 15

9.3 Initial certification..... 16

9.3.1 General..... 16

9.3.2 Initial certification audit 16

9.4 Conducting audits 17

9.4.1 General..... 17

9.4.2 Specific elements of the ISMS audit 17

9.4.3 Audit report..... 17

9.5 Certification decision..... 18

9.5.1 General..... 18

9.5.2 Certification decision..... 18

9.6 Maintaining certification..... 18

9.6.1 General..... 18

9.6.2 Surveillance activities 18

9.6.3 Re-certification 19

9.6.4 Special audits..... 19

9.6.5 Suspending, withdrawing or reducing the scope of certification 20

9.7 Appeals..... 20

9.8 Complaints..... 20

9.8.1 General..... 20

9.8.2 Complaints..... 20

9.9 Client records..... 20

10 Management system requirements for certification bodies..... 20

10.1 Options..... 20

10.1.1 General..... 20

10.1.2 ISMS implementation..... 20

Formatted: English (United Kingdom)

Formatted: Left, Space Before: 18 pt, Line spacing: Exactly 12 pt

Formatted: English (United Kingdom)

Formatted: Font: 9 pt

Formatted: Font: 9 pt

Formatted: Font: 9 pt

Formatted: Font: 11 pt

Formatted: Space Before: 18 pt, Line spacing: Exactly 12 pt

ISO/IEC ~~DIS~~ FDIS 27006-1:2023(E)

Formatted: Font: 11.5 pt

Formatted: Font: 11.5 pt

10.2 Option A: General management system requirements	20
10.3 Option B: Management system requirements in accordance with ISO 9001	20
Annex A (normative) Knowledge and skills for ISMS auditing and certification	21
Annex B (informative) Further competence considerations	22
Annex C (normative) Audit time	24
Annex D (informative) Methods for audit time calculations	31
Annex E (informative) Guidance for review of implemented ISO/IEC 27001:2022, Annex A controls	36
Bibliography	54

iTeh Standards
(<https://standards.iteh.ai>)
Document Preview

ISO/IEC FDIS 27006-1

<https://standards.iteh.ai/catalog/standards/sist/ee9551dd-1fbf-4c83-a38d-d9e3cb8cf644/iso-iec-fdis-27006-1>

Formatted: Font: 9 pt

Formatted: Left, Space Before: 18 pt, Line spacing: Exactly 12 pt

Formatted: Font: 9 pt

Formatted: Font: 9 pt

Formatted: Font: 11 pt, Not Bold

Formatted: Font: 9 pt

Formatted: Space Before: 18 pt, Line spacing: Exactly 12 pt

Formatted: Font: 11.5 pt

Formatted: Font: 11.5 pt

Foreword

Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

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.

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 or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC ~~had~~ had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and <https://patents.iec.ch>. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

Formatted: Font: Not Italic, Font color: Auto

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

For an explanation of 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 www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*, in collaboration with the European Committee for Standardization (CEN) Technical Committee CEN-CLC/JTC-13 *Cybersecurity and data protection*, in accordance with the Agreement on technical cooperation between ISO and CEN (Vienna Agreement).

This first edition of ISO/IEC 27006-1 cancels and replaces ISO/IEC 27006:2015, which has been technically revised. It also incorporates the Amendment ISO/IEC 27006:2015/Amd 1:2020.

The main changes are as follows:

- this document has been converted into the first part of a multi-part series;
- the entire document has been updated for remote audits and organizations with few or no physical relevant sites;
- the concept of persons performing certain identical activities has been introduced in Annex C.3.4 and several updates were provided;

Formatted: std_publisher

Formatted: std_docNumber

Formatted: std_docPartNumber

Formatted: cite_sec

Formatted: English (United Kingdom)

Formatted: Font: 9 pt

Formatted: Left, Space Before: 18 pt, Line spacing: Exactly 12 pt

Formatted: English (United Kingdom)

Formatted: Font: 9 pt

Formatted: Font: 9 pt

Formatted: Font: 9 pt

Formatted: Font: 11 pt

Formatted: Space Before: 18 pt, Line spacing: Exactly 12 pt

ISO/IEC ~~DIS~~ FDIS 27006-1:2023(E)

Formatted: Font: 11.5 pt

Formatted: Font: 11.5 pt

- this document (in particular, Annex E) has been aligned with ISO/IEC 27001:2022 and ISO/IEC 27002:2022, including updating Annex E;
- redundancies with ISO/IEC 17021-1 have been removed;
- wording has been clarified and improved for better consistency, including more closely aligned with ISO/IEC 17021-1;
- structural changes to comply with the ISO/IEC directives have been made.

Formatted: Default Paragraph Font

Formatted: std_year

Formatted: Default Paragraph Font

A list of all parts in the ISO/IEC 27006 series can be found on the ISO and IEC websites.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

iTeh Standards
(<https://standards.itih.ai>)
Document Preview

ISO/IEC FDIS 27006-1

<https://standards.itih.ai/catalog/standards/sist/ee9551dd-1fbf-4c83-a38d-d9e3cb8cf644/iso-iec-fdis-27006-1>

Formatted: Font: 9 pt

Formatted: Font: 11 pt, Not Bold

Formatted: Left, Space Before: 18 pt, Line spacing: Exactly 12 pt

Formatted: Font: 9 pt

Formatted: Font: 9 pt

Formatted: Font: 9 pt

Formatted: Space Before: 18 pt, Line spacing: Exactly 12 pt

Formatted: Font: 11.5 pt

Formatted: Font: 11.5 pt

Introduction

ISO/IEC 17021-1 sets out requirements and guidance for bodies providing audit and certification of management systems. If such bodies intend to be compliant with ISO/IEC 17021-1 with the objective of auditing and certifying information security management systems (ISMS) in accordance with ISO/IEC 27001, some additional requirements and guidance to ISO/IEC 17021-1 are critical. These are provided by this document.

Formatted: std_publisher

Formatted: std_docNumber

Formatted: Default Paragraph Font

Formatted: std_year

~~The text in this document follows the structure of ISO/IEC 17021-1:2015.~~

~~In this document, the following verbal forms are used:~~

~~— “shall” indicates a requirement;~~

~~— “should” indicates a recommendation;~~

~~— “may” indicates a permission;~~

~~— “can” indicates a possibility or a capability.~~

This document specifies requirements for bodies providing audit and certification of an ISMS. It gives generic requirements for such bodies which are referred to as certification bodies. Observance of these requirements is intended to ensure that certification bodies operate ISMS certification in a competent, consistent and impartial manner, thereby facilitating the recognition of such bodies and the acceptance of their certifications on a national and international basis.

~~Throughout this document, the terms “management system” and “system” are used interchangeably. The management system as used in this document should not be confused with other types of systems, such as IT systems.~~

~~The text in this document follows the structure of ISO/IEC 17021-1:2015.~~

Formatted: Default Paragraph Font

Formatted: std_year

~~In this document, the following verbal forms are used:~~

~~— “shall” indicates a requirement;~~

~~— “should” indicates a recommendation;~~

~~— “may” indicates a permission;~~

~~— “can” indicates a possibility or a capability.~~

ISO/IEC FDIS 27006-1

<https://standards.iteh.ai/catalog/standards/sist/ee9551dd-1fbf-4c83-a38d-d9e3cb8cf644/iso-iec-fdis-27006-1>

Formatted: English (United Kingdom)

Formatted: Font: 9 pt

Formatted: Left, Space Before: 18 pt, Line spacing: Exactly 12 pt

Formatted: English (United Kingdom)

Formatted: Font: 9 pt

Formatted: Font: 9 pt

Formatted: Font: 9 pt

Formatted: Font: 11 pt

Formatted: Space Before: 18 pt, Line spacing: Exactly 12 pt

Formatted: Font: 11.5 pt
Formatted: Font: 11.5 pt
Formatted: Font: 11.5 pt

Formatted: Section start: New page

Information security, cybersecurity and privacy protection — Requirements for bodies providing audit and certification of information security management systems — Part 1: General

1 Scope

This document specifies requirements and provides guidance for bodies providing audit and certification of an information security management system (ISMS), in addition to the requirements contained within ISO/IEC 17021-1.

The requirements contained in this document are demonstrated in terms of competence and reliability by bodies providing ISMS certification. The guidance contained in this document provides additional interpretation of these requirements for bodies providing ISMS certification.

NOTE This document can be used as a criteria document for accreditation, peer assessment or other audit processes.

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 17021-1:2015, *Conformity assessment — Requirements for bodies providing audit and certification of management systems — Part 1: Requirements*

ISO/IEC 27001:2022, *Information security, cybersecurity and privacy protection — Information security management systems — Requirements*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 17021-1 and the following apply.

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

- ISO Online browsing platform: available at <https://www.iso.org/obp>
- IEC Electropedia: available at <https://www.electropedia.org/>

3.1 certification document

document indicating that a client's information security management system (ISMS) conforms to specified ISMS standards and any supplementary documentation required under the management system

Note 1 to entry:— This definition does not limit the number of documents collectively known as certification documents.

Formatted: Font: Times New Roman
Formatted: Font: Times New Roman, English (United States)
Formatted: Note, Tab stops: 0.7 cm, Left + 1.4 cm, Left + 2.1 cm, Left + 2.8 cm, Left + 3.5 cm, Left + 4.2 cm, Left + 4.9 cm, Left + 5.6 cm, Left + 6.3 cm, Left + 7 cm, Left
Formatted: Font: 9 pt
Formatted: Font: 9 pt
Formatted: Font: 11 pt, Not Bold
Formatted: Font: Not Bold
Formatted: Left, Space Before: 18 pt, Line spacing: Exactly 12 pt
Formatted: Font: 9 pt
Formatted: Font: 9 pt
Formatted: Space Before: 18 pt, Line spacing: Exactly 12 pt
Formatted: Font: Not Bold
Formatted: Justified

ISO/IEC ~~DIS~~ FDIS 27006-1:2023(E)

Formatted: Font: 11.5 pt

Formatted: Font: 11.5 pt

3.2

control

measure that maintains and/or modifies *risk* (3.10)

Note 1 to entry:—_Controls include, but are not limited to, any process, policy, device, practice or other conditions and/or actions which maintain and/or modify *risk* (3.10).

Note 2 to entry:—_Controls may not always exert the intended or assumed modifying effect.

[SOURCE: ISO/IEC 27002:2022, 3.1.8]

Formatted: English (United Kingdom)

3.3

external context

external environment in which the *organization* (3.9) seeks to achieve its objectives

Note 1 to entry:—_External context can include the following:

- the cultural, social, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local;
- key drivers and trends having impact on the objectives of the *organization* (3.9);
- relationships with, and perceptions and values of, external stakeholders.

[SOURCE: ISO/IEC 27000:2018, 3.22]

3.4

information security

preservation of confidentiality, integrity and availability of information

Note 1 to entry:—_In addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved.

[SOURCE: ISO/IEC 27000:2018, 3.28]

3.5

information security incident

single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening *information security* (3.4)

[SOURCE: ISO/IEC 27000:2018, 3.31]

3.6

information system

set of applications, services, information technology assets, or other information-handling components

[SOURCE: ISO/IEC 27000:2018, 3.35]

3.7

internal context

internal environment in which the *organization* (3.9) seeks to achieve its objectives

Note 1 to entry:—_Internal context can include:

- governance, organizational structure, roles and accountabilities;
- policies, objectives, and the strategies that are in place to achieve them;

Formatted: Font: Not Bold

Formatted: Left, Space Before: 18 pt, Line spacing: Exactly 12 pt

Formatted: Font: Not Bold, English (United Kingdom)

Formatted: Font: 9 pt

Formatted: Font: 9 pt

Formatted: Font: 9 pt

Formatted: Font: 9 pt

Formatted: Font: 11 pt

Formatted: Space Before: 18 pt, Line spacing: Exactly 12 pt

Formatted: Right

- the capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, processes, systems and technologies);
- *information systems* (3.6), information flows and decision-making processes (both formal and informal);
- relationships with, and perceptions and values of, internal stakeholders;
- the *organization's* (3.9) culture;
- standards, guidelines and models adopted by the *organization* (3.9);
- form and extent of contractual relationships.

[SOURCE: ISO/IEC 27000:2018, 3.38]

3.8 management system

set of interrelated or interacting elements of an *organization* (3.9) to establish policies and objectives, and processes to achieve those objectives

Note 1 to entry: A management system can address a single discipline or several disciplines, e.g. quality management, financial management or environmental management.

Note 2 to entry: The management system elements establish the *organization's* (3.9) structure, roles and responsibilities, planning, operation, policies, practices, rules, beliefs, objectives and processes to achieve those objectives.

Note 3 to entry: The scope of a management system can include the whole of the *organization* (3.9), specific and identified functions of the *organization* (3.9), specific and identified sections of the *organization* (3.9), or one or more functions across a group of *organizations* (3.9).

Note 4 to entry: This constitutes one of the common terms and core definitions for ISO management system standards given in Annex SL of the Consolidated ISO Supplement to the ISO/IEC Directives, Part 1. The original definition has been modified by modifying Notes 1 to 3 to entry.

[SOURCE: ISO 9000:2015, 3.5.3]

Formatted: Default Paragraph Font

3.9 organization

person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its objectives

Note 1 to entry:—The concept of organization includes but is not limited to sole-trader, company, corporation, firm, enterprise, authority, partnership, charity or institution, or part or combination thereof, whether incorporated or not, public or private.

[SOURCE: ISO/IEC 27000:2018, 3.50]

3.10 risk
effect of uncertainty on objectives

Note 1 to entry:—An effect is a deviation from the expected — positive or negative.

Note 2 to entry:—Uncertainty is the state, even partial, of deficiency of information related to, understanding of knowledge of, an event, its consequence, or likelihood.

Formatted: Font: 9 pt

Formatted: Font: 9 pt

Formatted: Font: 9 pt

Formatted: Font: 9 pt

Formatted: Left, Space Before: 18 pt, Line spacing: Exactly 12 pt

Formatted: Font: 11 pt, Not Bold

Formatted: Font: Not Bold

Formatted: Space Before: 18 pt, Line spacing: Exactly 12 pt

Formatted: Font: Not Bold

ISO/IEC DIS FDIS 27006-1:2023(E)

Formatted: Font: 11.5 pt

Formatted: Font: 11.5 pt

Note 3 to entry:—Risk is often characterized by reference to potential “events” (as defined in ISO Guide 73:2009, 3.5.1.3) and “consequences” (as defined in ISO Guide 73:2009, 3.6.1.3), or a combination of these.

Note 4 to entry:—Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated “likelihood” (as defined in ISO Guide 73:2009, 3.6.1.1) of occurrence.

Note 5 to entry:—In the context of information security management systems, information security risks can be expressed as an effect of uncertainty on information security objectives.

Note 6 to entry:—Information security risk is associated with the potential that threats will exploit vulnerabilities of an information asset or group of information assets and thereby cause harm to an *organization* (3.9).

Formatted: cite_sec

[SOURCE: ISO/IEC 27000:2018, 3.61 ~~with Note 5 editorially modified~~]

3.11 risk analysis

process to comprehend the nature of *risk* (3.10) and to determine the level of risk

Note 1 to entry:—Risk analysis provides the basis for risk evaluation and decisions about *risk treatment* (3.14).

Note 2 to entry:—Risk analysis includes risk estimation.

[SOURCE: ISO/IEC 27000:2018, 3.63]

3.12 risk assessment

overall process of risk identification, *risk analysis* (3.11) and risk evaluation

[SOURCE: ISO/IEC 27000:2018, 3.64]

3.13 risk management

coordinated activities to direct and control an *organization* (3.9) with regard to *risk* (3.10)

[SOURCE: ISO/IEC 27000:2018, 3.69]

3.14 risk treatment

process to modify *risk* (3.10)

Note 1 to entry:—Risk treatment can involve:

- avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk;
- taking or increasing risk in order to pursue an opportunity;
- removing the risk source;
- changing the likelihood;
- changing the consequences;
- sharing the risk with another party or parties (including contracts and risk financing);
- retaining the risk -by informed choice.

Formatted: Font: Not Bold

Formatted: Left, Space Before: 18 pt, Line spacing: Exactly 12 pt

Formatted: Font: Not Bold, English (United Kingdom)

Formatted: Font: 9 pt

Formatted: Font: 9 pt

Formatted: Font: 9 pt

Formatted: Font: 9 pt

Formatted: Font: 11 pt

Formatted: Space Before: 18 pt, Line spacing: Exactly 12 pt