SO/IEC 27002 Information security, cybersecurity and privacy protection - Information security controls

Agenda

1. Intro and main terms
2. The ISMS family of standards
3. Why is ISO 27001 so popular?
4. Benefits of implementing the ISMS
5. ISO Survey 2021 (certificates)
6. ISMS Implementation Phases
7. Required activities (desired state)
8. Annex A. Information Security Controls
9. What you need to know about the ISMS
10. ISMS Implementation Plan and the first steps

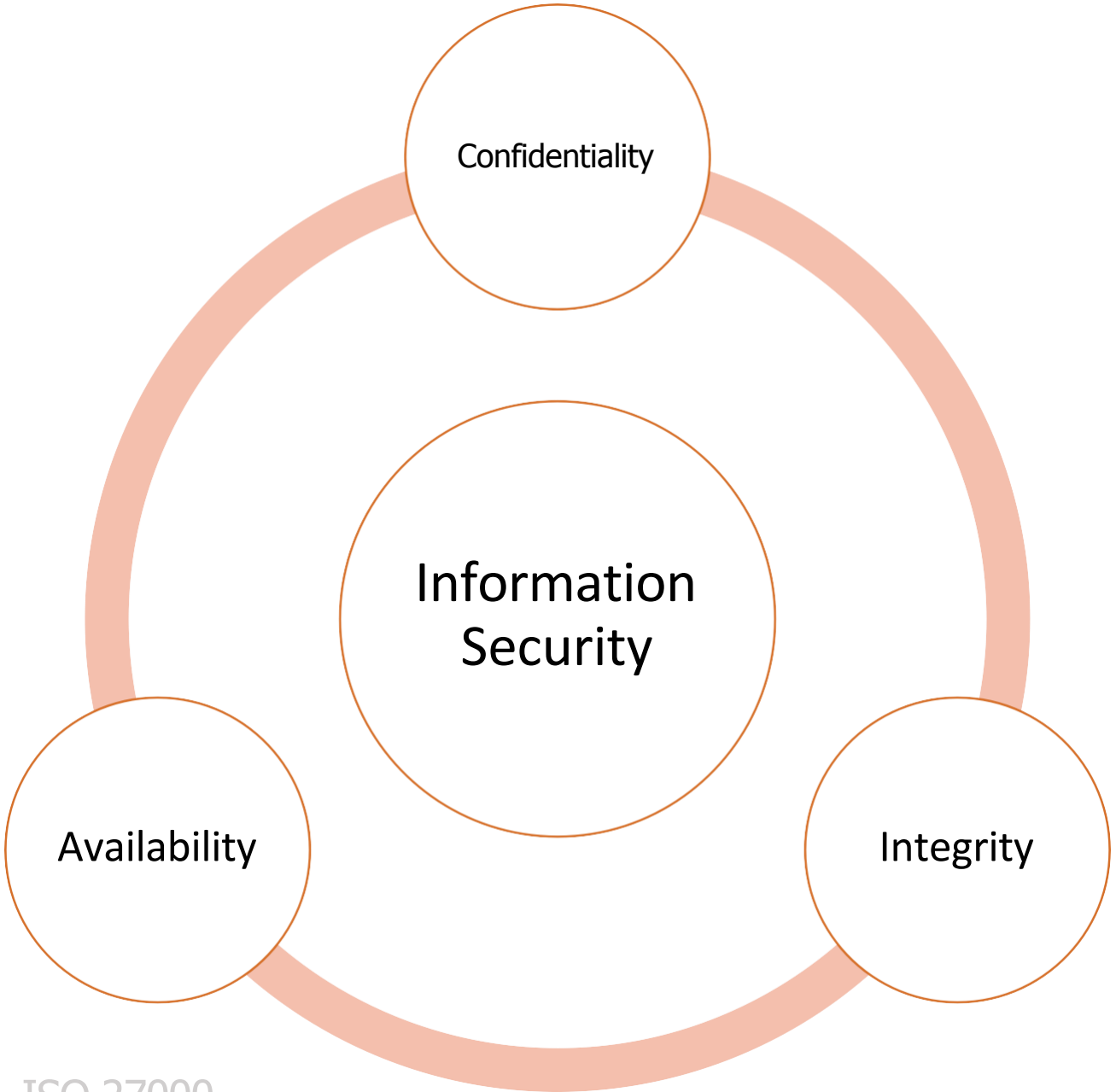
Organizations of all types and sizes:

a) collect, process, store, and transmit **information**

b) recognize that **information**, and related processes, systems, networks and people are important **assets** for achieving organization **objectives**

c) face a range of **risks** that can affect the functioning of **assets**

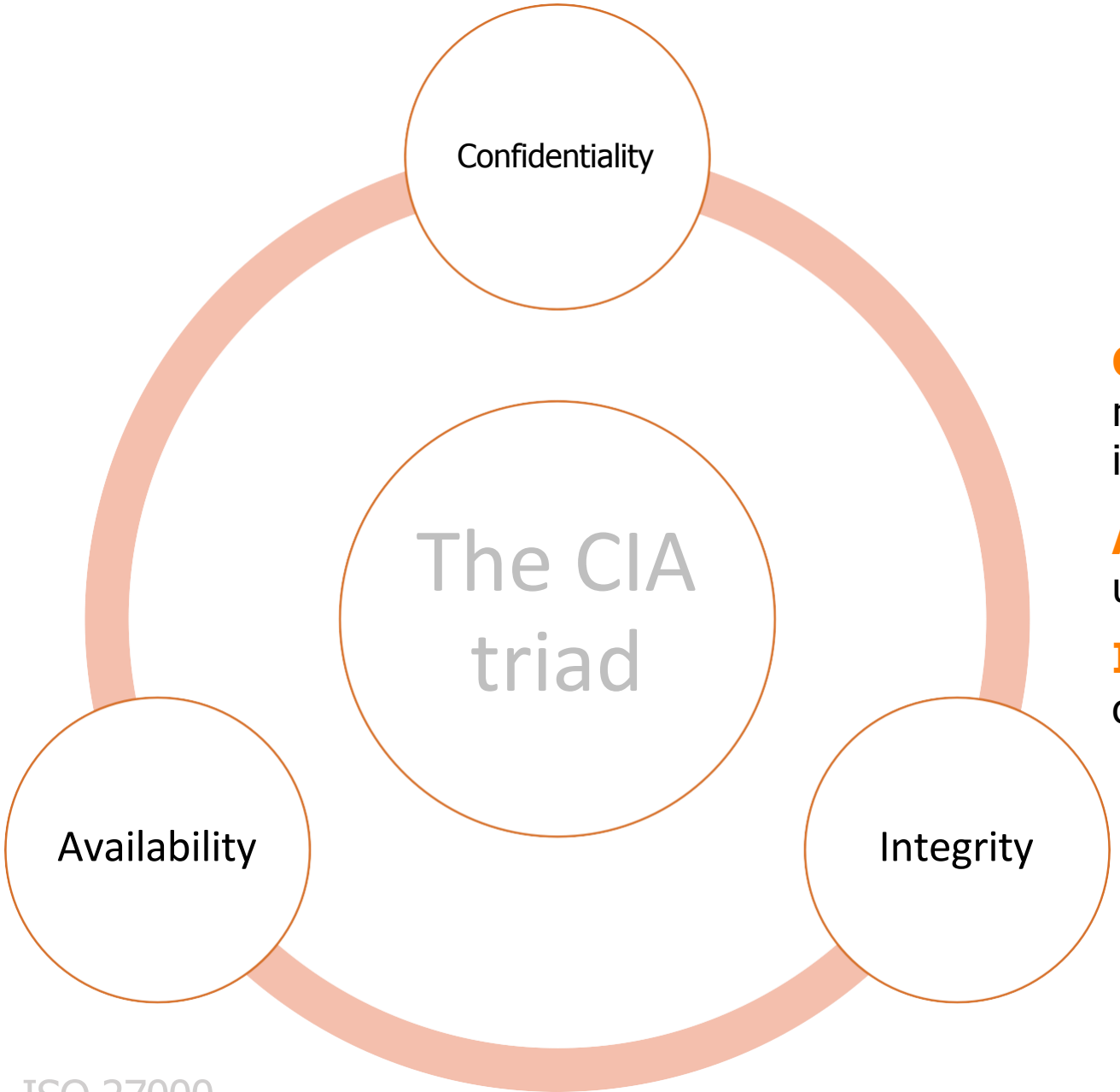
d) address their perceived risk exposure by implementing **information security controls**



Information security:
preservation of confidentiality, integrity and availability of information

In addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved

ISO 27000



Confidentiality: property that information is not made available or disclosed to unauthorized individuals, entities, or processes

Availability: property of being accessible and usable on demand by an authorized entity

Integrity: property of accuracy and completeness

ISO 27000

An **Information Security Management System (ISMS)** is a systematic approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organization's **information security** to **achieve business objectives**

Components of an ISMS

a) Policy

b) Persons with defined responsibilities

d) Documented information

e) Information security risk assessment

f) Information security risk treatment, including determination and implementation of controls

c) Management processes related to:

1. Policy establishment
2. Awareness and competence provision
3. Planning
4. Implementation
5. Operation
6. Performance assessment
7. Management review
8. Improvement

a-d: common components of any management systems
e-f: additional ISMS components

Risk: effect of uncertainty on objectives

Risk is often expressed in terms of a combination of the consequences of an event and the associated "likelihood" of occurrence

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

An **ISMS** is based on a **risk assessment** and the organization's risk acceptance levels designed to effectively treat and manage risks

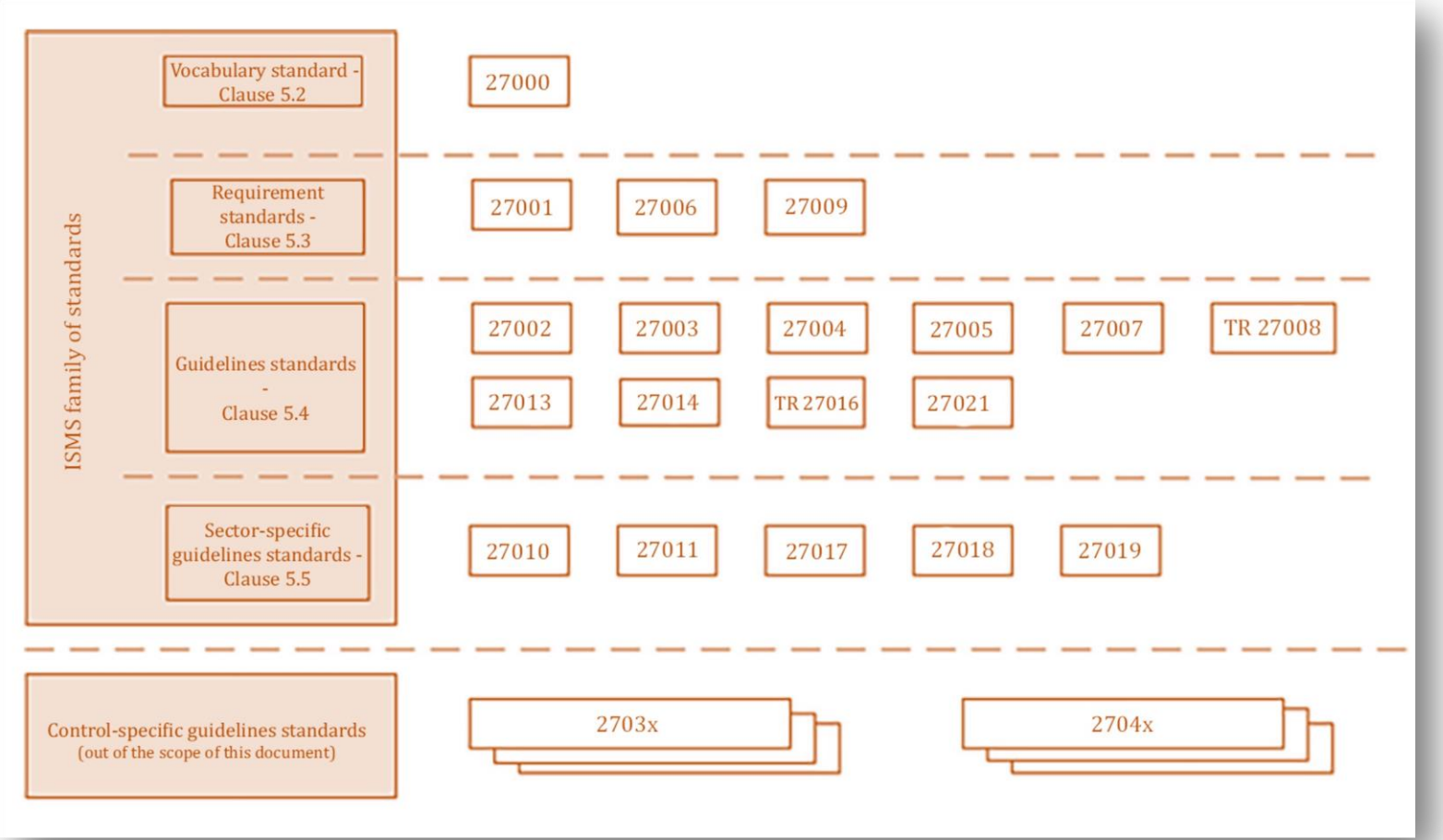
Analysing **requirements** for the protection of information assets and applying appropriate **controls** to ensure the protection of these information assets, as required, contributes to the successful implementation of an **ISMS**

The **benefits** of implementing an ISMS primarily result from a **reduction in information security risks** (i.e. reducing the probability of and/or impact caused by information security incidents)…

see other benefits later in this presentation

ISO 27001 is the commonly used standard for ISMS implementation and certification

The ISMS family of standards (ISO 27k)



The **ISMS family of standards** includes standards that:

a) define requirements for an ISMS and for those certifying such systems

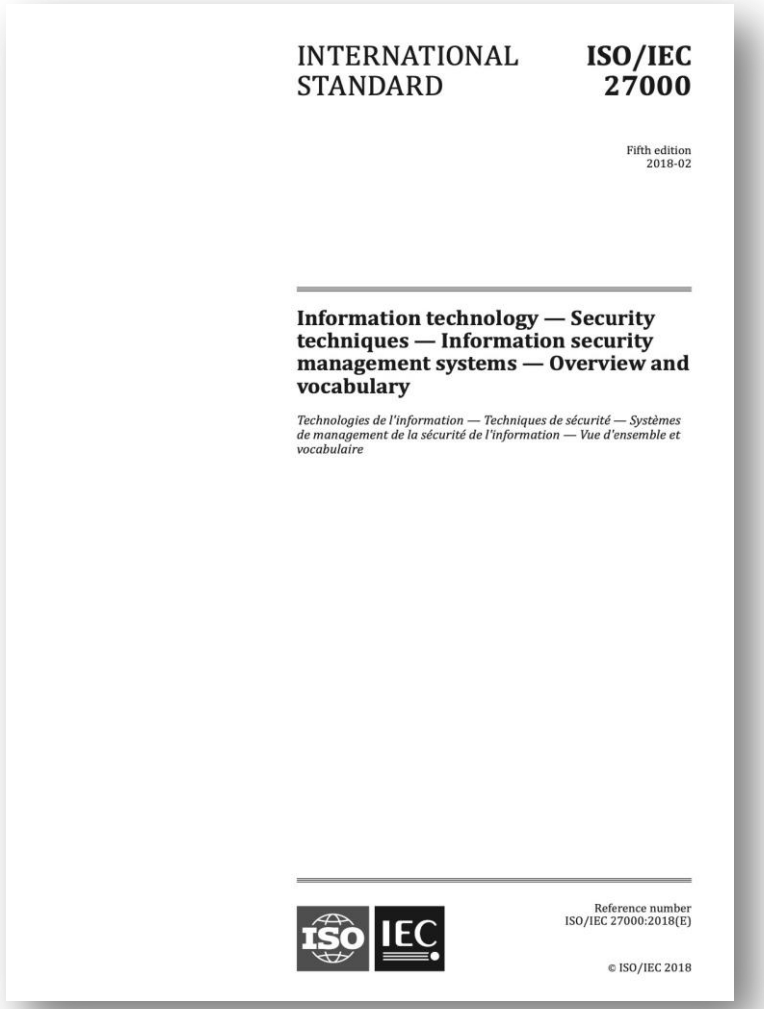
b) provide direct support, detailed guidance and/or interpretation for the overall process to establish, implement, maintain, and improve an ISMS

c) address sector-specific guidelines for ISMS

d) address conformity assessment for ISMS

70+ standards

ISO 27000 Overview and vocabulary


INTERNATIONAL STANDARD

ISO/IEC 27000

Fifth edition
2018-02

Information technology — Security techniques — Information security management systems — Overview and vocabulary

Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Vue d'ensemble et vocabulaire

Reference number
ISO/IEC 27000:2018(E)

© ISO/IEC 2018

ISO/IEC 27000:2018 provides the overview of **information security management systems (ISMS)**.

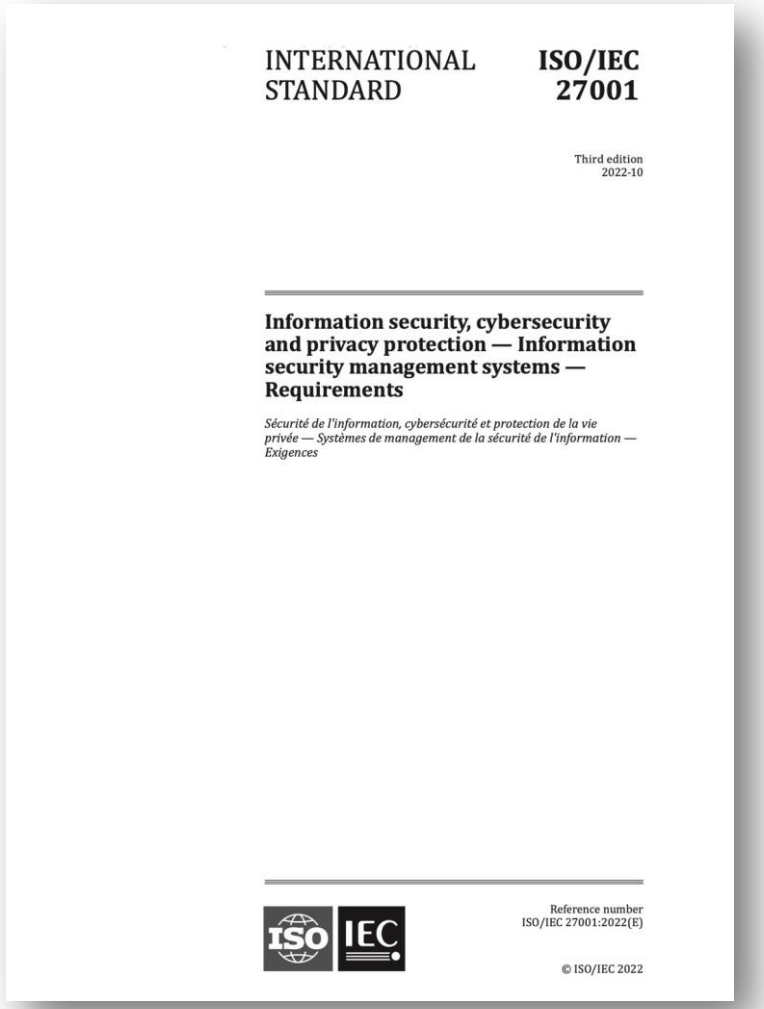
It also provides terms and definitions commonly used in the ISMS family of standards. This document is applicable to all types and sizes of organization (e.g. commercial enterprises, government agencies, not-for-profit organizations).

The terms and definitions provided in this document

- cover commonly used terms and definitions in the ISMS family of standards;
- do not cover all terms and definitions applied within the ISMS family of standards; and
- do not limit the ISMS family of standards in defining new terms for use.

https://standards.iso.org/ittf/PubliclyAvailableStandards

ISO 27001 ISMS Requirements


INTERNATIONAL STANDARD

ISO/IEC 27001

Third edition
2022-10

Information security, cybersecurity and privacy protection — Information security management systems — Requirements

Sécurité de l'information, cybersécurité et protection de la vie privée — Systèmes de management de la sécurité de l'information — Exigences

ISO IEC

Reference number
ISO/IEC 27001:2022(E)

© ISO/IEC 2022

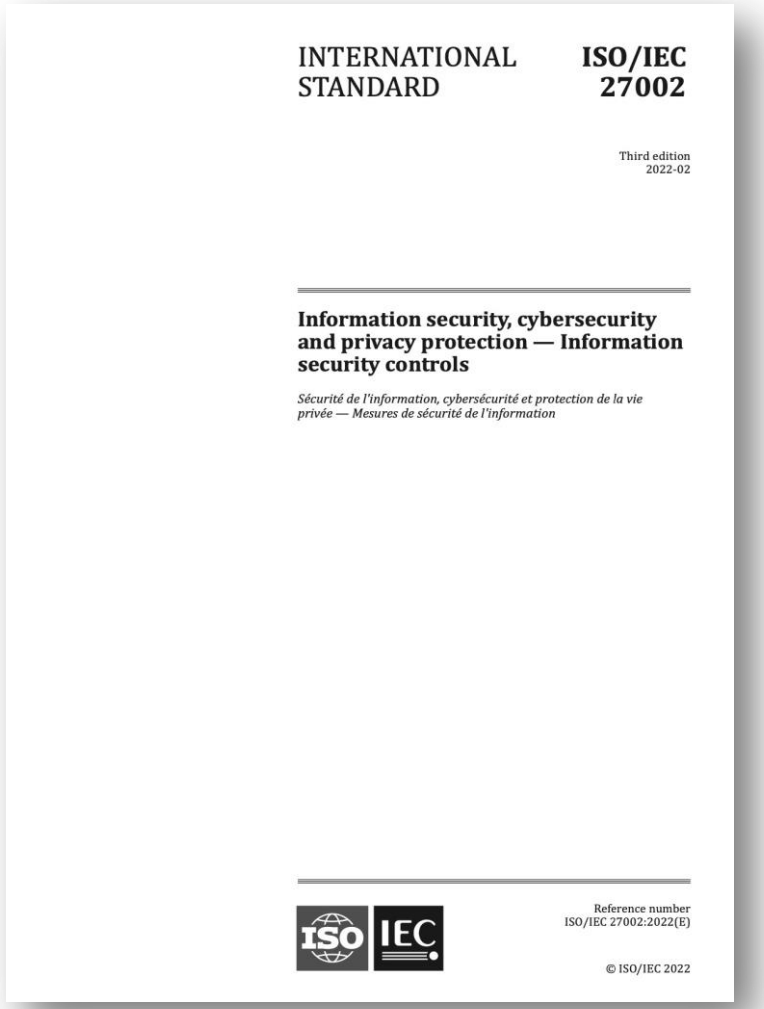
This standard specifies the **requirements** for establishing, implementing, maintaining and continually improving an **information security management system (ISMS)** within the context of the organization.

This document also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization.

The requirements set out in this document are generic and are intended to be applicable to all organizations, regardless of type, size or nature.

Excluding any of the requirements specified in Clauses 4 to 10 is not acceptable when an organization claims conformity to this document.

ISO 27002 Information Security controls


INTERNATIONAL STANDARD

ISO/IEC 27002

Third edition
2022-02

Information security, cybersecurity and privacy protection — Information security controls

Sécurité de l'information, cybersécurité et protection de la vie privée — Mesures de sécurité de l'information

Reference number
ISO/IEC 27002:2022(E)

© ISO/IEC 2022

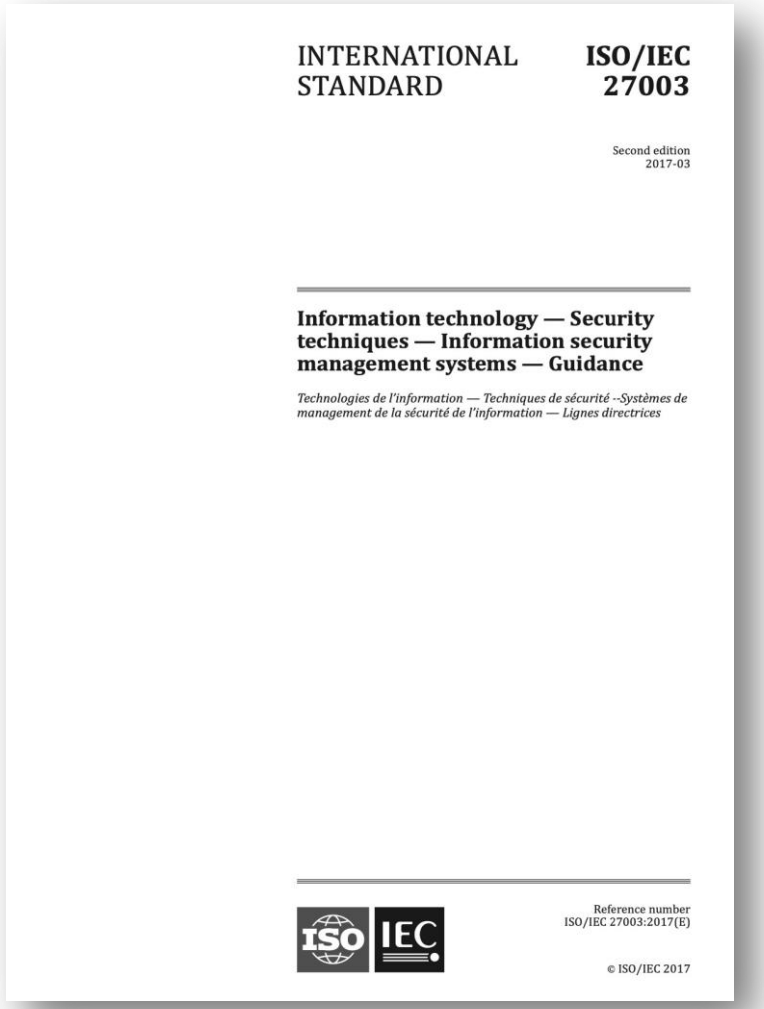
This document provides a reference set of generic **information security controls** including implementation guidance. This document is designed to be used by organizations:

a) within the context of an information security management system (ISMS) based on ISO/IEC 27001;

b) for implementing information security controls based on internationally recognized best practices;

c) for developing organization-specific information security management guidelines.

ISO 27003 ISMS Guidance


INTERNATIONAL STANDARD

ISO/IEC 27003

Second edition
2017-03

Information technology — Security techniques — Information security management systems — Guidance

Technologies de l'information — Techniques de sécurité --Systèmes de management de la sécurité de l'information — Lignes directrices

ISO IEC

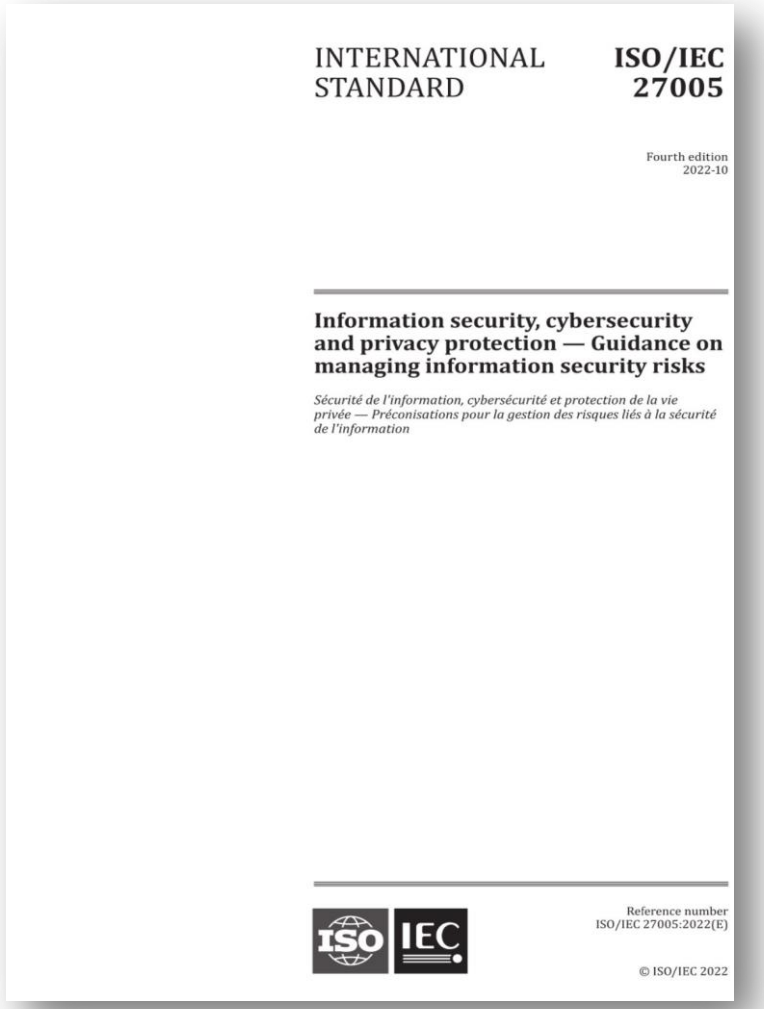
Reference number
ISO/IEC 27003:2017(E)

© ISO/IEC 2017

This document provides **guidance on the requirements** for an **information security management system (ISMS)** as specified in ISO/IEC 27001 and provides recommendations ('should'), possibilities ('can') and permissions ('may') in relation to them.

It is not the intention of this document to provide general guidance on all aspects of information security.

ISO 27005 Guidance on managing IS risks

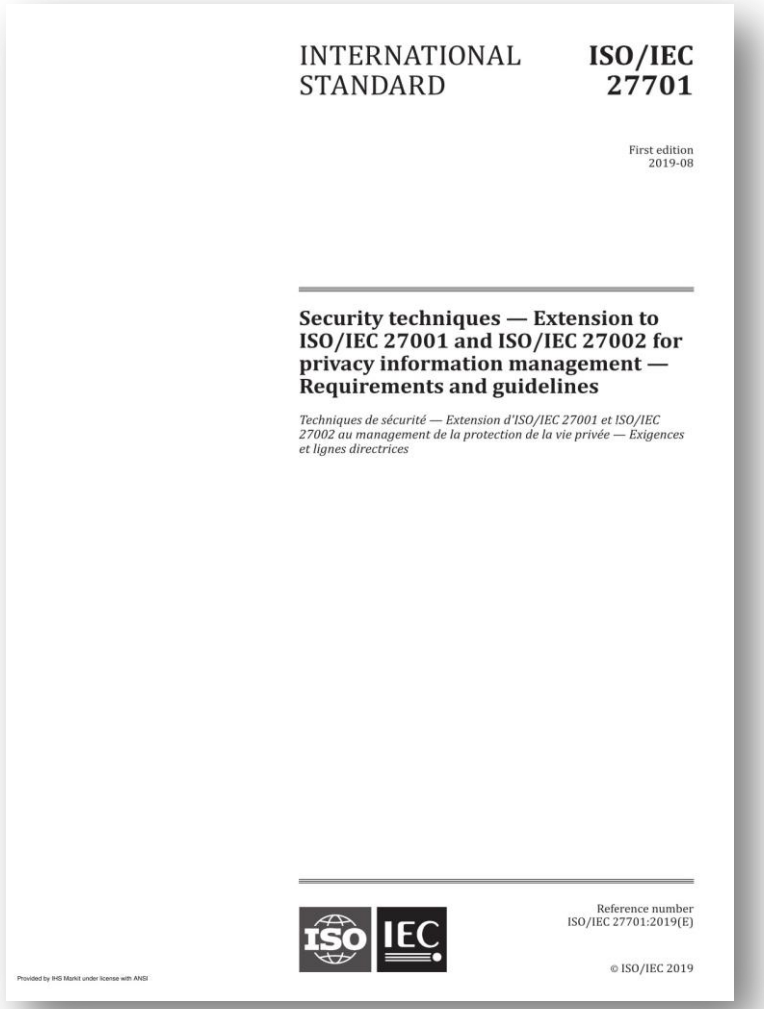


This document provides guidance to assist organizations to:

- fulfil the requirements of ISO/IEC 27001 concerning actions to address **information security risks**;
- perform information security risk management activities, specifically **information security risk assessment and treatment**.

This document is applicable to all organizations, regardless of type, size or sector.

ISO 27701 Extention for privacy



INTERNATIONAL STANDARD

ISO/IEC 27701

First edition
2019-08

Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines

Techniques de sécurité — Extension d'ISO/IEC 27001 et ISO/IEC 27002 au management de la protection de la vie privée — Exigences et lignes directrices

Reference number
ISO/IEC 27701:2019(E)

This document specifies requirements and provides guidance for establishing, implementing, maintaining and continually improving a **Privacy Information Management System (PIMS)** in the form of an extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy management within the context of the organization.

This document specifies PIMS-related requirements and provides guidance for PII controllers and PII processors holding responsibility and accountability for **PII processing**.

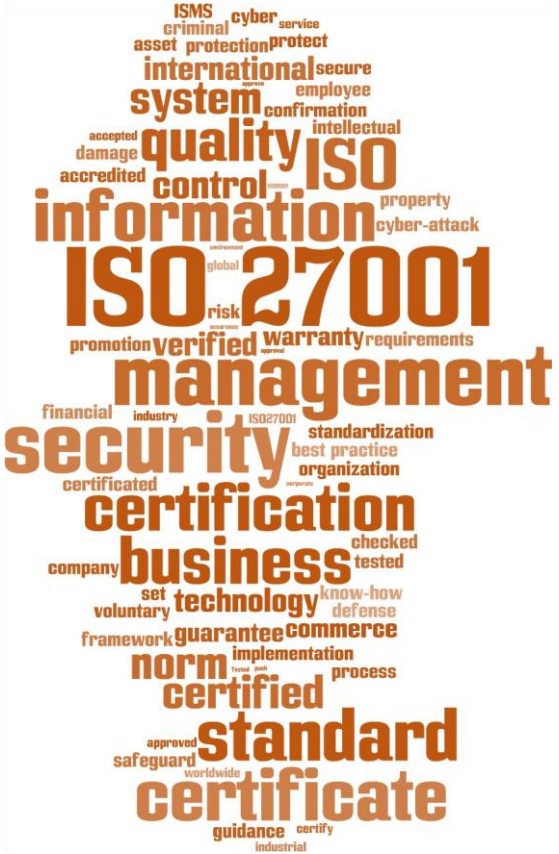
This document is applicable to all types and sizes of organizations, including public and private companies, government entities and not-for-profit organizations, which are **PII controllers and/or PII processors** processing PII within an ISMS.

Why is ISO 27001 so popular?

1. Applicable to all organizations, regardless of type, size or nature
2. It is short (21 pages) and simple (ISMS + IS controls)
3. It is aligned with other management systems (e.g., QMS, PIMS, SMS, BCMS)
4. It is time-tested (BS 7799-1 was published in 1995)
5. It contains simple but valuable principles (e.g., understanding the needs and expectations of interested parties, leadership and commitment, continual improvement, process approach, risk-based approach)
6. You can find many additional recommendations, guidelines and courses
7. You can certify your ISMS (for some countries / industries this is a mandatory requirement)
8. Many other IS standards and frameworks are inspired by ISO 27001
9. Many IS professionals use this standard, so they speak the same language…

Benefits of implementing the ISMS

1. Improved overall security (including incident response and cyber resilience)
2. Raising awareness and information security culture
3. Reducing business risks
4. Building stakeholder trust (external and internal)
5. Legal, regulatory and contractual compliance (information security and data protection)
6. A common approach to compliance with different information security requirements
7. Increasing the maturity of related processes (e.g., IT, HR, Governance)
8. Increasing the transparency and justification of information security budgets
9. Marketing opportunities



ISO Survey 2021

The latest results of the Survey shows an estimation of the number of valid certificates as of 31 December 2021.

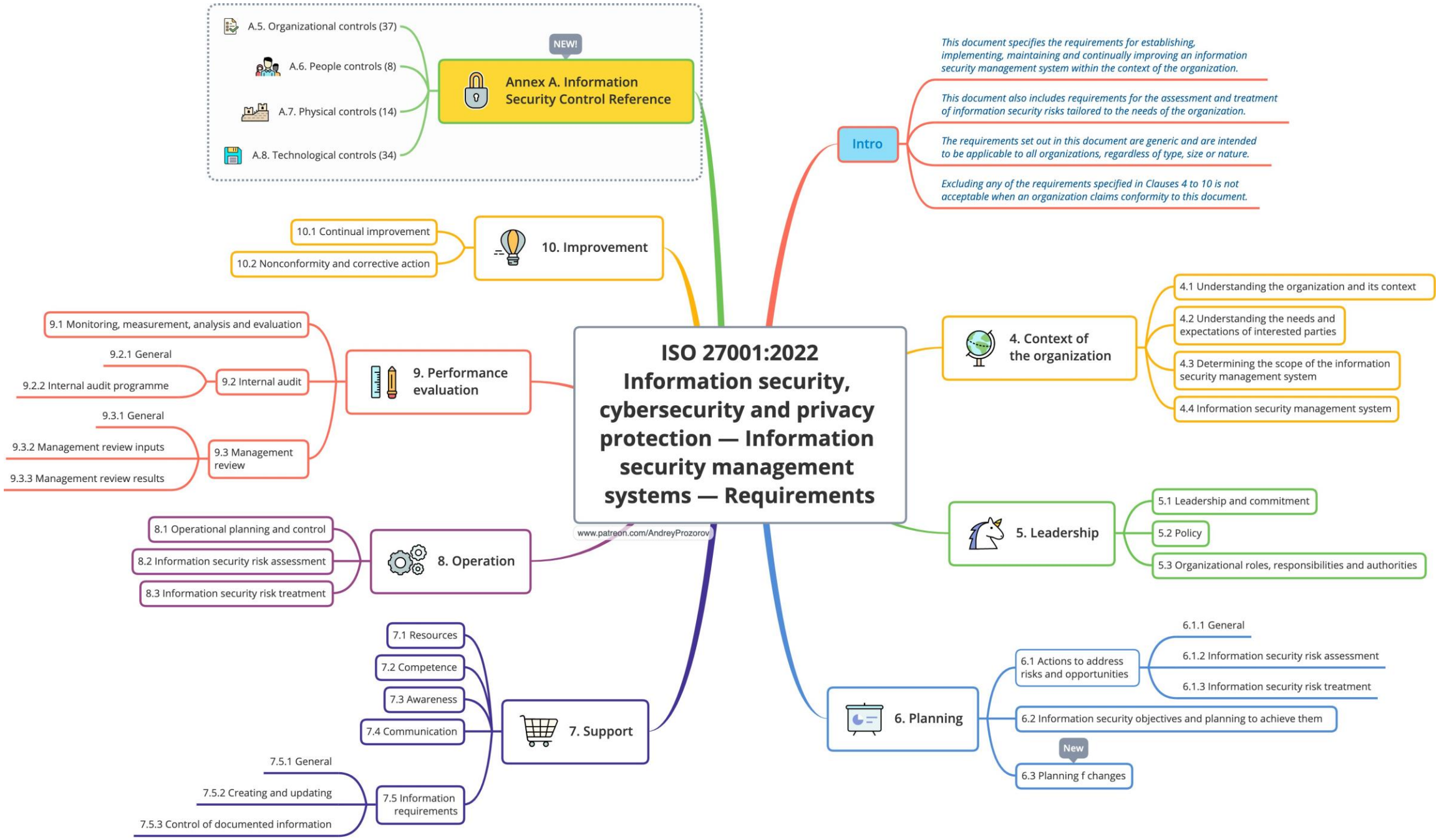
Global 2020: 44486 (+32%) / 84166

Finland 2020: 102 (+76%) / 185

	Total valid certificates	Total number of sites
ISO 9001:2015	1,077,884	1,447,080
ISO 14001:2015	420,433	610,924
ISO 45001:2018	294,420	369,897
ISO IEC 27001:2013	58,687	99,755
ISO 22000:2005&2018	36,124	42,937
ISO 13485:2016	27,229	38,503
ISO 50001:2011&2018	21,907	54,778
ISO 20000-1:2011&2018	11,769	13,998
ISO 37001:2016	2,896	7,982
ISO 22301:2012&2019	2,559	5,969
ISO 39001:2012	1,285	2,357
ISO 28000:2007	584	1,106
ISO 55001:2014	488	1,993
ISO 20121:2012	253	712
ISO 29001:2020	157	795
ISO 44001:2017	136	186

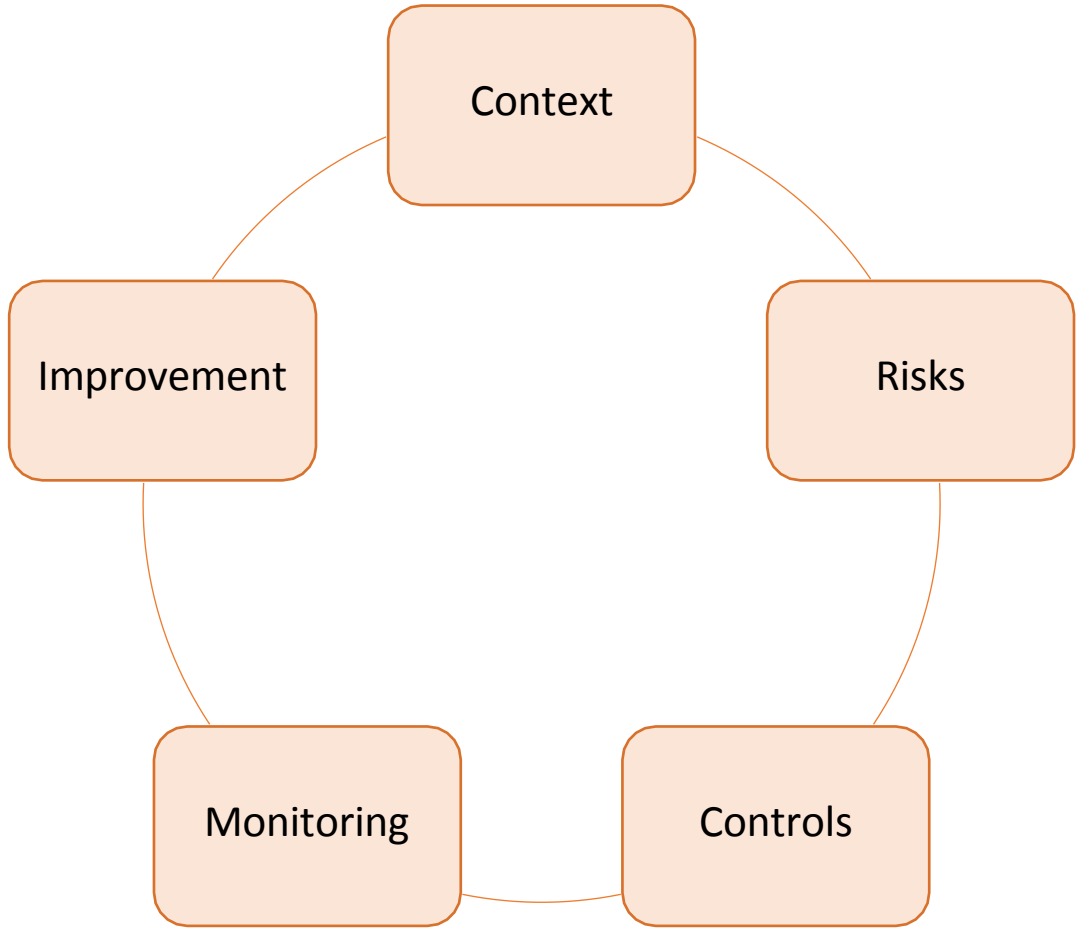
www.iso.org/the-iso-survey.html

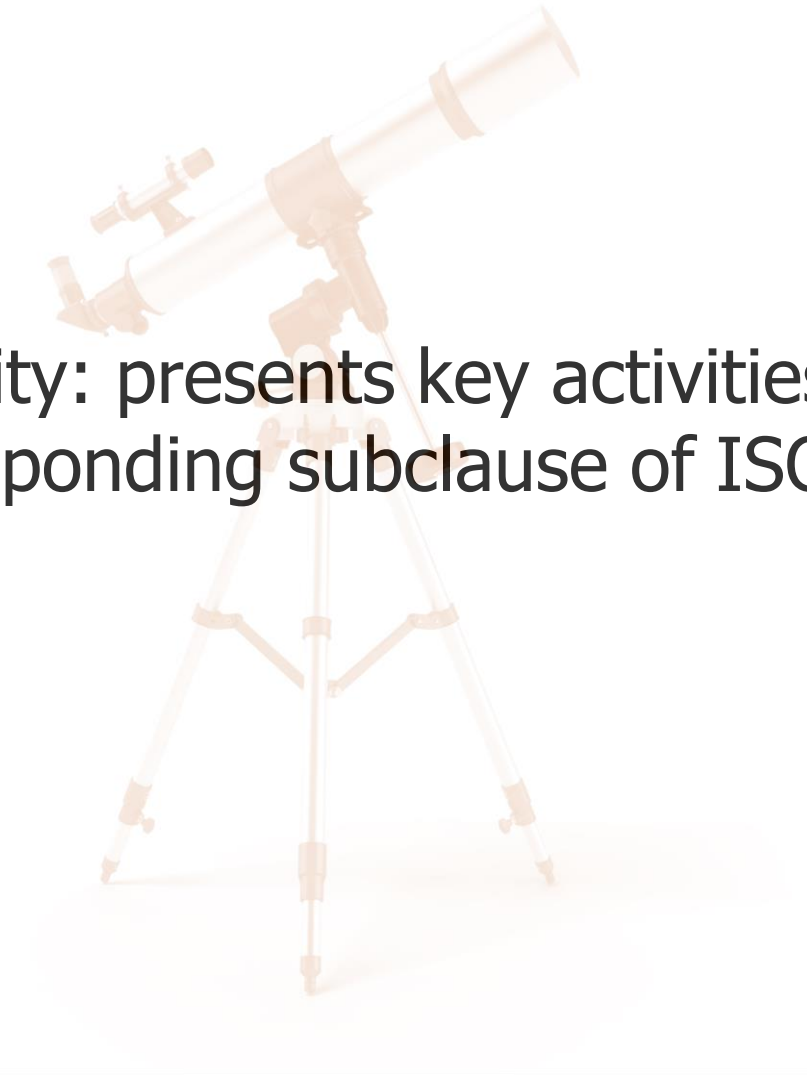
TOP 15 Countries	Certificates	Sites
China	18446	18569
Japan	6587	17784
United Kingdom of Great Britain and Northern Ireland	5256	8647
India	2775	6024
Italy	1924	3474
United States of America	1742	4504
Germany	1673	3486
Netherlands	1508	2421
Taiwan, Province of China	1129	3147
Israel	1056	1083
Romania	951	1211
Spain	949	1444
Poland	876	2210
Australia	775	2311
Turkey	706	1169



ISMS Implementation Phases

1. Understanding the organization's needs and the necessity for establishing information security policy and information security objectives
2. Assessing the organization's risks related to information security
3. Implementing and operating information security processes, controls and other measures to treat risks
4. Monitoring and reviewing the performance and effectiveness of the ISMS
5. Practising continual improvement





Required activity: presents key activities required in the corresponding subclause of ISO 27001

Required activities: 4. Context of the organization

4.1 Understanding the organization and its context	The organization determines external and internal issues relevant to its purpose and affecting its ability to achieve the intended outcome(s) of the information security management system (ISMS).
4.2 Understanding the needs and expectations of interested parties	The organization determines interested parties relevant to the ISMS and their requirements relevant to information security.
4.3 Determining the scope of the information security management system	The organization determines the boundaries and applicability of the ISMS to establish its scope.
4.4 Information security management system	The organization establishes, implements, maintains and continually improves the ISMS.

Required activities: 5. Leadership

1. Leadership and commitment	Top management demonstrates leadership and commitment with respect to the ISMS.
2. Policy	Top management establishes an information security policy.
3. Organizational roles, responsibilities and authorities	Top management ensures that responsibilities and authorities for roles relevant to information security are assigned and communicated throughout the organization.

Required activities: 6. Planning

6.1 Actions to address risks and opportunities	When planning for the ISMS, the organization determines the risks and opportunities considering issues referred to in 4.1 and requirements referred to in 4.2. The organization defines and applies an information security risk assessment process. The organization defines and applies an information security risk treatment process.
6.2 Information security objectives and planning to achieve them	The organization establishes information security objectives and plans to achieve them at relevant functions and levels.
6.3 Planning of changes	The organization determines the need for changes to the information security management system, the changes shall be carried out in a planned manner.

Required activities: 7. Support

7.1 Resources	The organization determines and provides the resources for establishing, implementing, maintaining and continually improving the ISMS.
7.2 Competence	The organization determines the competence of persons needed for information security performance, and ensures that the persons are competent.
7.3 Awareness	The persons doing work under the organization's control are made aware of the information security policy, their contribution to the effectiveness of the ISMS, benefits of improved information security performance and implications of not conforming to the requirements of the ISMS.
7.4 Communication	The organization determines the needs for internal and external communications related to the ISMS.
7.5 Documented information	The organization includes documented information in the ISMS as directly required by ISO/IEC 27001, as well as determined by the organization as being necessary for the effectiveness of the ISMS. When creating and updating documented information, the organization ensures its appropriate identification and description, format and media, and review and approval. The organization manages documented information throughout its lifecycle and makes it available where and when needed.

Required activities: 8. Operation

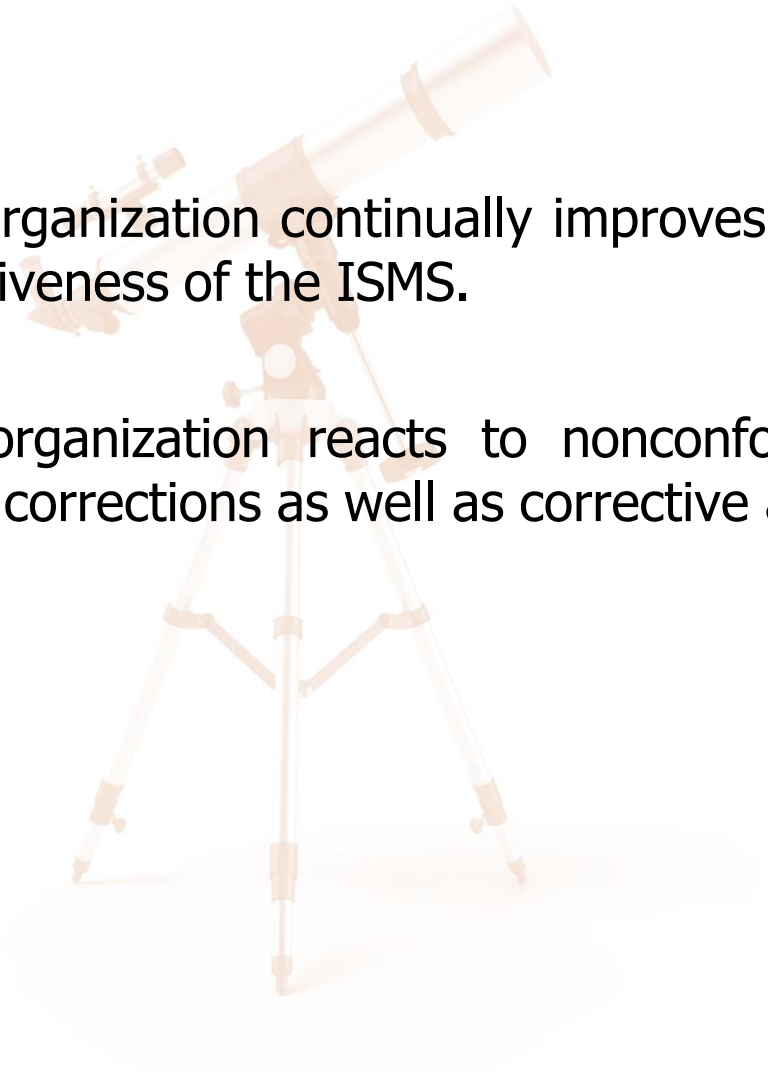
8.1 Operational planning and control	The organization plans, implements and controls the processes to meet its information security requirements and to achieve its information security objectives. The organization keeps documented information as necessary to have confidence that processes are carried out as planned. The organization controls planned changes and reviews the consequences of unintended changes, and ensures that outsourced processes are identified, defined and controlled.
8.2 Information security risk assessment	The organization performs information security risk assessments and retains documented information on their results.
8.3 Information security risk treatment	The organization implements the information security risk treatment plan and retains documented information on the results of the information security treatment.

Required activities: 9. Performance evaluation

1. Monitoring, measurement, analysis and evaluation	The organization evaluates the information security performance and the effectiveness of the ISMS.
2. Internal audit	The organization conducts internal audits to provide information on conformity of the ISMS to the requirements.
9.3 Management review	Top management reviews the ISMS at planned intervals.

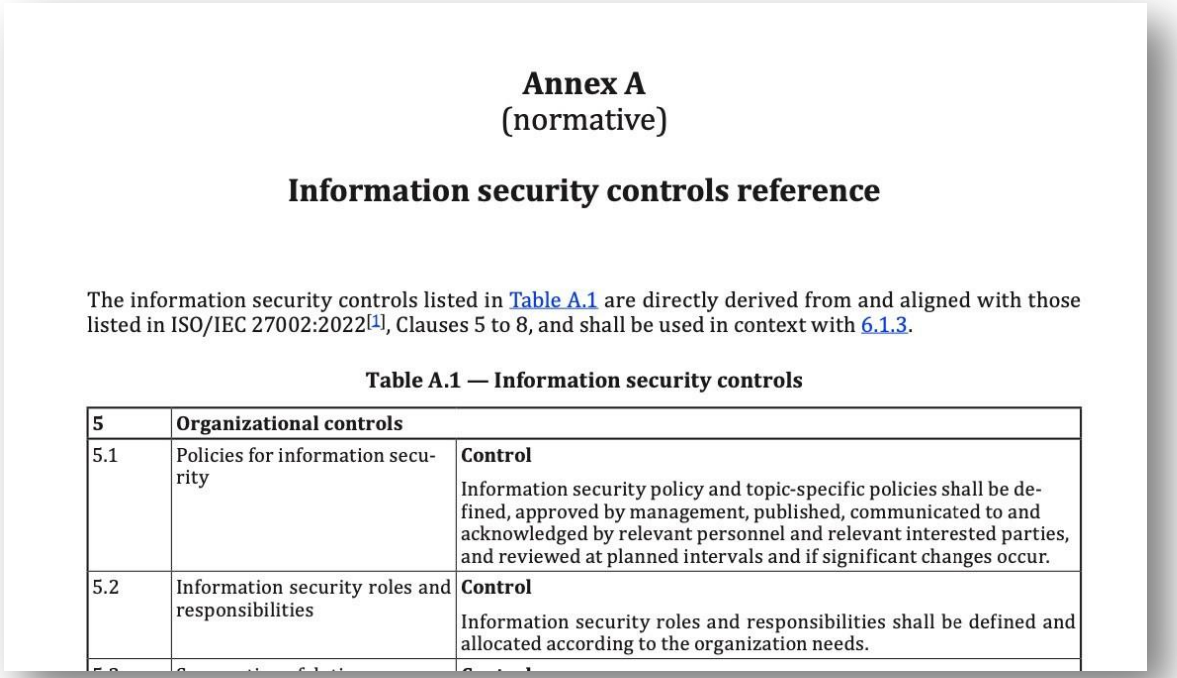
Required activities: 10. Improvement

10.1 Continual improvement	The organization continually improves the suitability, adequacy and effectiveness of the ISMS.
10.2 Nonconformity and corrective action	The organization reacts to nonconformities, evaluates them and takes corrections as well as corrective actions if needed.



Annex A. Information Security Controls

Control: measure that maintains and/or modifies risk



Annex A
(normative)

Information security controls reference

The information security controls listed in Table A.1 are directly derived from and aligned with those listed in ISO/IEC 27002:2022[1], Clauses 5 to 8, and shall be used in context with 6.1.3.

Table A.1 — Information security controls

5	**Organizational controls**	
5.1	Policies for information security	**Control** Information security policy and topic-specific policies shall be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.
5.2	Information security roles and responsibilities	**Control** Information security roles and responsibilities shall be defined and allocated according to the organization needs.

Total number of controls – 93, 11 new (2022)

Controls are categorized as:

a) People, if they concern individual people

b) Physical, if they concern physical objects

c) Technological, if they concern technology

d) otherwise they are categorized as **Organizational**

Five attributes only in ISO 27002:2022 (#):

1. Control type (Preventive, Detective, Corrective)
2. Information security properties (CIA)
3. Cybersecurity concepts
   (Identify, Protect, Detect, Respond and Recover)
4. Operational capabilities
5. Security domains

5. Organizational controls

5.1. Policies for information security
5.2. Information security roles and responsibilities
5.3. Segregation of duties
5.4. Management responsibilities
5.5. Contact with authorities
5.6. Contact with special interest groups
5.7. Threat intelligence
5.8. Information security in project management
5.9. Inventory of information and other associated assets
5.10. Acceptable use of information and other associated assets
5.11. Return of assets
5.12. Classification of information
5.13. Labelling of information
5.14. Information transfer
5.15. Access control
5.16. Identity management
5.17. Authentication information
5.18. Access rights
5.19. Information security in supplier relationships
5.20. Addressing information security within supplier agreements
5.21. Managing information security in the ICT supply chain
5.22. Monitoring, review and change management of supplier services
5.23. Information security for use of cloud services
5.24. Information security incident management planning and preparation
5.25. Assessment and decision on information security events
5.26. Response to information security incidents
5.27. Learning from information security incidents
5.28. Collection of evidence
5.29. Information security during disruption
5.30. ICT readiness for business continuity
5.31. Legal, statutory, regulatory and contractual requirements
5.32. Intellectual property rights
5.33. Protection of records
5.34. Privacy and protection of PII
5.35. Independent review of information security
5.36. Compliance with policies, rules and standards for information security
5.37. Documented operating procedures

6. People controls

6.1. Screening
6.2. Terms and conditions of employment
6.3. Information security awareness, education and training
6.4. Disciplinary process
6.5. Responsibilities after termination or change of employment
6.6. Confidentiality or non-disclosure agreements
6.7. Remote working
6.8. Information security event reporting

7. Physical controls

7.1. Physical security perimeter
7.2. Physical entry
7.3. Securing offices, rooms and facilities
7.4. Physical security monitoring
7.5. Protecting against physical and environmental threats
7.6. Working in secure areas
7.7. Clear desk and clear screen
7.8. Equipment siting and protection
7.9. Security of assets off-premises
7.10. Storage media
7.11. Supporting utilities
7.12. Cabling security
7.13. Equipment maintenance
7.14. Secure disposal or re-use of equipment

93

controls

8. Technological controls

8.1. User endpoint devices
8.2. Privileged access rights
8.3. Information access restriction
8.4. Access to source code
8.5. Secure authentication
8.6. Capacity management
8.7. Protection against malware
8.8. Management of technical vulnerabilities
8.9. Configuration management
8.10. Information deletion
8.11. Data masking
8.12. Data leakage prevention
8.13. Information backup
8.14. Redundancy of information processing facilities
8.15. Logging
8.16. Monitoring activities
8.17. Clock synchronization
8.18. Use of privileged utility programs
8.19. Installation of software on operational systems
8.20. Network security
8.21. Security of network services
8.22. Segregation of networks
8.23. Web filtering
8.24. Use of cryptography
8.25. Secure development life cycle
8.26. Application security requirements
8.27. Secure system architecture and engineering principles
8.28. Secure coding
8.29. Security testing in development and acceptance
8.30. Outsourced development
8.31. Separation of development, test and production environments
8.32. Change management
8.33. Test information
8.34. Protection of information systems during audit testing

*New control, 2022

ISMS Implementation Plan

Stage	Duration (days)						
	Optimistic	Realistic	Pessimistic	PERT	ΔPERT	Min	Max
0. Read ISO 27001 and additional materials	0,0	1,0	5,0	1,5	0,8	0,7	2,3
1. Conduct awareness trainings for the top management	0,5	1,0	5,0	1,6	0,8	0,8	2,3
2. Conduct a GAP analysis	2,0	5,0	10,0	5,3	1,3	4,0	6,7
3. Understand the Context	2,0	5,0	10,0	5,3	1,3	4,0	6,7
4. Plan the Implementation	1,0	3,0	5,0	3,0	0,7	2,3	3,7
5. Conduct the first IS Committee meeting	0,5	1,0	5,0	1,6	0,8	0,8	2,3
6. Establish Information Security Policy and Information Security Objectives	1,0	3,0	10,0	3,8	1,5	2,3	5,3
7. Take an inventory of the assets	3,0	6,0	15,0	7,0	2,0	5,0	9,0
8. Define a Method of Risk Assessment, identify and assess information security risks	5,0	15,0	30,0	15,8	4,2	11,7	20,0
9. Prepare Statement of Applicability (SoA) and Risk Treatment Plan (RTP)	5,0	10,0	20,0	10,8	2,5	8,3	13,3
10. Define requirements for documentation management	3,0	5,0	30,0	8,8	4,5	4,3	13,3
11. Develop ISMS Framework and define roles and responsibilities	5,0	10,0	30,0	12,5	4,2	8,3	16,7
12. Develop and implement a set of ISMS policies and procedures	30,0	90,0	180,0	95,0	25,0	70,0	120,0
13. Plan and implement additional information security measures	0,0	40,0	180,0	56,7	30,0	26,7	86,7
14. Plan, prepare and conduct awareness trainings	10,0	20,0	40,0	21,7	5,0	16,7	26,7
15. Operate the ISMS	60,0	120,0	360,0	150,0	50,0	100,0	200,0
16. Monitor the ISMS	5,0	10,0	20,0	10,8	2,5	8,3	13,3
17. Audit the ISMS	3,0	10,0	20,0	10,5	2,8	7,7	13,3
18. Conduct the ISMS Management review	2,0	5,0	10,0	5,3	1,3	4,0	6,7
19. Practice continual improvement	30,0	60,0	180,0	75,0	25,0	50,0	100,0
20. Prepare for the certification audit	20,0	30,0	60,0	33,3	6,7	26,7	40,0
Total	188,0	450,0	1225,0	535,5	172,8	362,7	708,3

PERT=(O+4R+P)/6
ΔPERT=(P-O)/6
Min=PERT-ΔPERT
Min=PERT+ΔPERT

By Andrey Prozorov, CISM, CIPP/E, CDPSE, LA 27001
www.patreon.com/AndreyProzorov