The ISMS family of standards (ISO 27k)

by Andrey Prozorov, CISM, CIPP/E, CDPSE, LA 27001

www.patreon.com/AndreyProzorov

2.0, 09.10.2023

Agenda

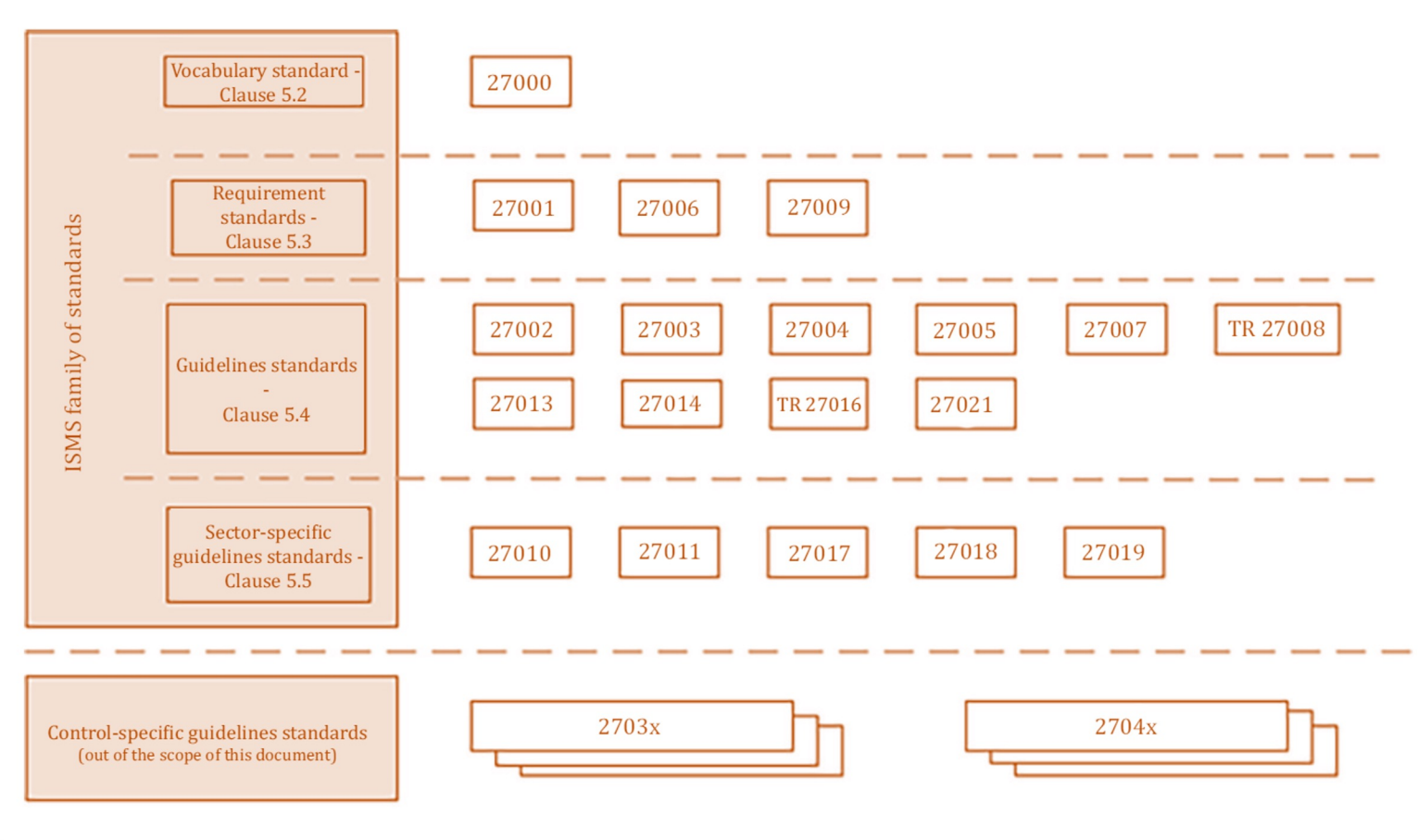
1. The ISO/IEC 27000 family
2. Stages of Publishing a Standard
3. IS Controls for Industries
4. Topic-specific sets (27033-27036)
5. Available languages, pages, and price (examples)
6. ISO 27000
7. ISO 27001
8. ISO 27002
9. ISO 27003
10. ISO 27004
11. ISO 27005
12. ISO 27701
13. ISO 27007 and ISO 27008
14. ISO 27014
15. ISO 27022
16. All standards
17. For Beginners / Advanced / Experts

IT security, cybersecurity and privacy protection are vital for companies and organizations today. The **ISO/IEC 27000 family** of standards keeps them safe.

ISO/IEC 27001 is the world's best-known standard for **information security management systems (ISMS)** and their requirements. Additional best practice in data protection and cyber resilience are covered by more than a dozen standards in the ISO/IEC 27000 family. Together, they enable organizations of all sectors and sizes to manage the security of assets such as financial information, intellectual property, employee data and information entrusted by third parties.

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**

The ISMS family of standards (ISO 27k)



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

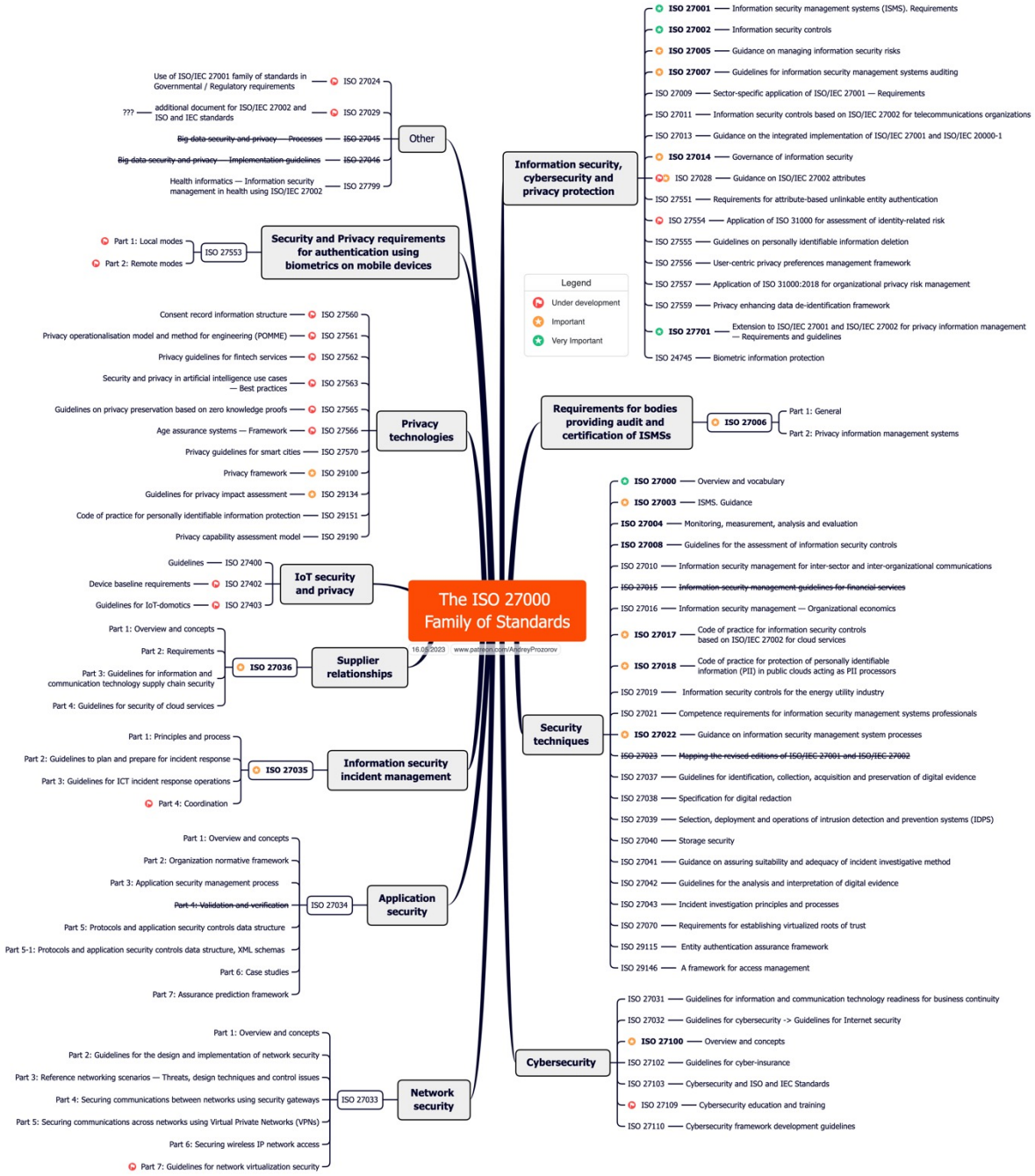
a) define requirements for an ISMS and for those certifying such systems

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. There's no single list, it changes continuously…



The most important:

1. ISO 27000: ISMS. Overview and vocabulary
2. **ISO 27001: ISMS. Requirements**
3. ISO 27002: Information security controls
4. ISO 27003: ISMS Guidance
5. ISO 27005: Guidance on managing information security risks
6. ISO 27701: Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management (PIMS) — Requirements and guidelines

Valuable:

1. ISO 27004: Monitoring, measurement, analysis and evaluation
2. ISO 27007: Guidelines for information security management systems auditing
3. ISO 27008: Guidelines for the assessment of information security controls
4. ISO 27014: Governance of information security
5. ISO 27022: Guidance on ISMS processes

Stages of Publishing a Standard

Any standard published by ISO goes through these stages:

1. **Proposal Stage** - an NP (New Project) is under consideration
2. **Preparatory stage** - a WD (Working Draft) is under consideration
3. **Committee stage** - a CD (Committee Draft) is under consideration
4. **Enquiry stage** - a DIS (Draft International Standard) is under consideration
5. **Approval stage** - an FDIS (Final Draft International Standard) is under consideration
6. **Publication stage** – an International Standard is being prepared for publication

International harmonized stage codes

STAGE	SUBSTAGE			90 Decision			
	00 Registration	20 Start of main action	60 Completion of main action	92 Repeat an earlier phase	93 Repeat current phase	98 Abandon	99 Proceed
00 Preliminary	00.00 Proposal for new project received	00.20 Proposal for new project under review	00.60 Close of review			00.98 Proposal for new project abandoned	00.99 Approval to ballot proposal for new project
10 Proposal	10.00 Proposal for new project registered	10.20 New project ballot initiated	10.60 Close of voting	10.92 Proposal returned to submitter for further definition		10.98 New project rejected	10.99 New project approved
20 Preparatory	20.00 New project registered in TC/SC work programme	20.20 Working draft (WD) study initiated	20.60 Close of comment period			20.98 Project deleted	20.99 WD approved for registration as CD
30 Committee	30.00 Committee draft (CD) registered	30.20 CD study initiated	30.60 Close of comment period	30.92 CD referred back to Working Group		30.98 Project cancelled	30.99 CD approved for registration as DIS
40 Enquiry	40.00 DIS registered	40.20 DIS ballot initiated: 12 weeks	40.60 Close of voting	40.92 Full report circulated: DIS referred back to TC or SC	40.93 Full report circulated: decision for new DIS ballot	40.98 Project cancelled	40.99 Full report circulated: DIS approved for registration as FDIS
50 Approval	50.00 Final text received or FDIS registered for formal approval	50.20 Proof sent to secretariat or FDIS ballot initiated: 8 weeks	50.60 Close of voting. Proof returned by secretariat	50.92 FDIS or proof referred back to TC or SC		50.98 Project cancelled	50.99 FDIS or proof approved for publication
60 Publication	60.00 International Standard under publication		60.60 International Standard published				
90 Review		90.20 International Standard under systematic review	90.60 Close of review	90.92 International Standard to be revised	90.93 International Standard confirmed		90.99 Withdrawal of International Standard proposed by TC or SC
95 Withdrawal		95.20 Withdrawal ballot initiated	95.60 Close of voting	95.92 Decision not to withdraw International Standard			95.99 Withdrawal of International Standard

IS Controls for Industries

1. *ISO/IEC 27011:2016 Information technology — Security techniques — Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations [New revision is under development]*
2. ~~*ISO/IEC TR 27015:2012 Information technology — Security techniques — Information security management guidelines for financial services*~~ *[Withdrawn]*
3. *ISO/IEC 27017:2015 Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services [New revision is under development]*
4. *ISO/IEC 27018:2019 Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*
5. *ISO/IEC 27019:2017 Information technology — Security techniques — Information security controls for the energy utility industry [Reviewed and confirmed in 2022]*
6. *ISO/IEC AWI TR 27024 ISO/IEC 27001 family of standards references list — Use of ISO/IEC 27001 family of standards in Governmental / Regulatory requirements [Under development]*
7. *ISO 27799:2016 Health informatics — Information security management in health using ISO/IEC 27002 [New revision is under development]*

Topic-specific sets

1. *ISO 27033: Network Security*
2. *ISO 27034: Application Security*
3. *ISO 27035: Information security incident management*
4. *ISO 27036: Supplier relationships*

ISO 27033
Network Security

- *ISO/IEC 27033-1:2015 Information technology — Security techniques — Network security — Part 1: Overview and concepts*
- *ISO/IEC 27033-2:2012 Information technology — Security techniques — Network security — Part 2: Guidelines for the design and implementation of network security*
- *ISO/IEC 27033-3:2010 Information technology — Security techniques — Network security — Part 3: Reference networking scenarios — Threats, design techniques and control issues*
- *ISO/IEC 27033-4:2014 Information technology — Security techniques — Network security — Part 4: Securing communications between networks using security gateways*
- *ISO/IEC 27033-5:2013 Information technology — Security techniques — Network security — Part 5: Securing communications across networks using Virtual Private Networks (VPNs)*
- *ISO/IEC 27033-6:2016 Information technology — Security techniques — Network security — Part 6: Securing wireless IP network access*
- *ISO/IEC 27033-7 Information technology – Network security — Part 7: Guidelines for network virtualization security [Under development]*

ISO 27034
Application Security

- *ISO/IEC 27034-1:2011 Information technology — Security techniques — Application security — Part 1: Overview and concepts*
- *ISO/IEC 27034-2:2015 Information technology — Security techniques — Application security — Part 2: Organization normative framework*
- *ISO/IEC 27034-3:2018 Information technology — Application security — Part 3: Application security management process*
- ~~*ISO/IEC DIS 27034-4 Information technology — Security techniques — Application security — Part 4: Validation and verification*~~ *[Deleted]*
- *ISO/IEC 27034-5:2017 Information technology — Security techniques — Application security — Part 5: Protocols and application security controls data structure*
- *ISO/IEC TS 27034-5-1:2018 Information technology — Application security — Part 5-1: Protocols and application security controls data structure, XML schemas*
- *ISO/IEC 27034-6:2016 Information technology — Security techniques — Application security — Part 6: Case studies*
- *ISO/IEC 27034-7:2018 Information technology — Application security — Part 7: Assurance prediction framework*

ISO 27035
Information security incident management

- *ISO/IEC 27035-1:2023 Information technology — Information security incident management — Part 1: Principles and process*
- *ISO/IEC 27035-2:2023 Information technology — Information security incident management — Part 2: Guidelines to plan and prepare for incident response*
- *ISO/IEC 27035-3:2020 Information technology — Information security incident management — Part 3: Guidelines for ICT incident response operations*
- *ISO/IEC DIS 27035-4 Information technology — Information security incident management — Part 4: Coordination [Under development]*

ISO 27036
Supplier relationships

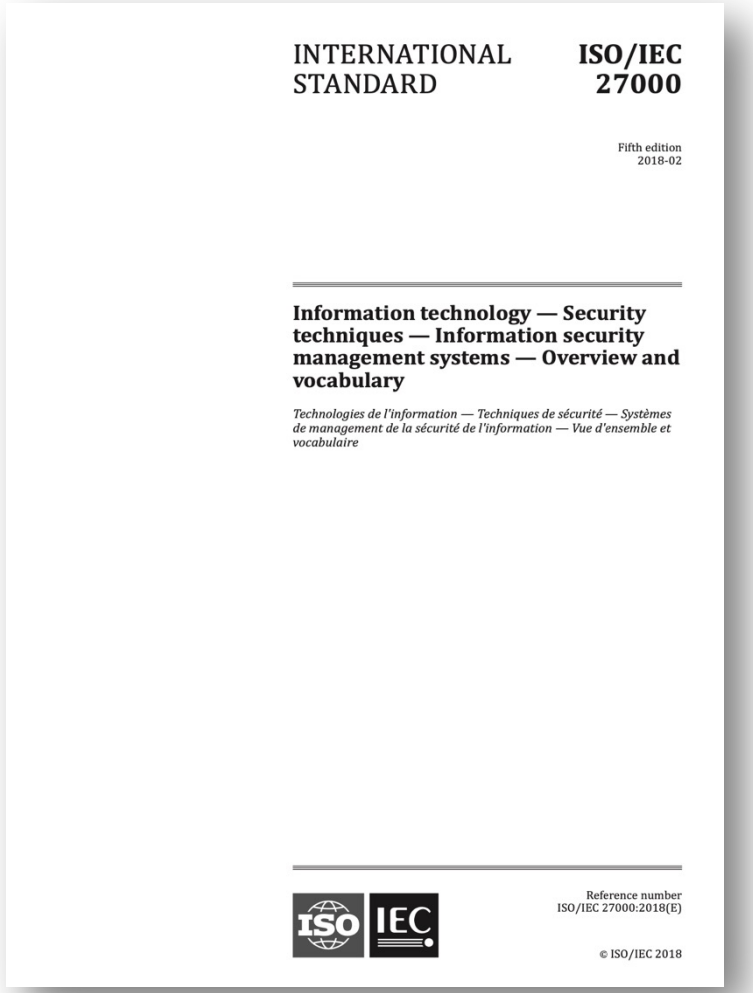
- *ISO/IEC 27036-1:2021 Cybersecurity — Supplier relationships — Part 1: Overview and concepts*
- *ISO/IEC 27036-2:2022 Cybersecurity — Supplier relationships — Part 2: Requirements*
- *ISO/IEC 27036-3:2023 Cybersecurity — Supplier relationships — Part 3: Guidelines for hardware, software, and services supply chain security*
- *ISO/IEC 27036-4:2016 Information technology — Security techniques — Information security for supplier relationships — Part 4: Guidelines for security of cloud services*

Available languages, pages, and price (ISO.org)

ISO 27000:2018	English, French	27 pages	CHF 174, but it is a Publicly Available Standard
ISO 27001:2022	English, French	19 pages	CHF 124
ISO 27002:2022	English, French	152 pages	CHF 208
ISO 27003:2017	English	45 pages	CHF 166
ISO 27004:2016	English	58 pages	CHF 187
ISO 27005:2022	English, French	62 pages	CHF 187
ISO 27701:2019	English, French	66 pages	CHF 187

Swiss franc (CHF) ≈ EUR

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

ISO IEC

Reference number
ISO/IEC 27000:2018(E)

© ISO/IEC 2018

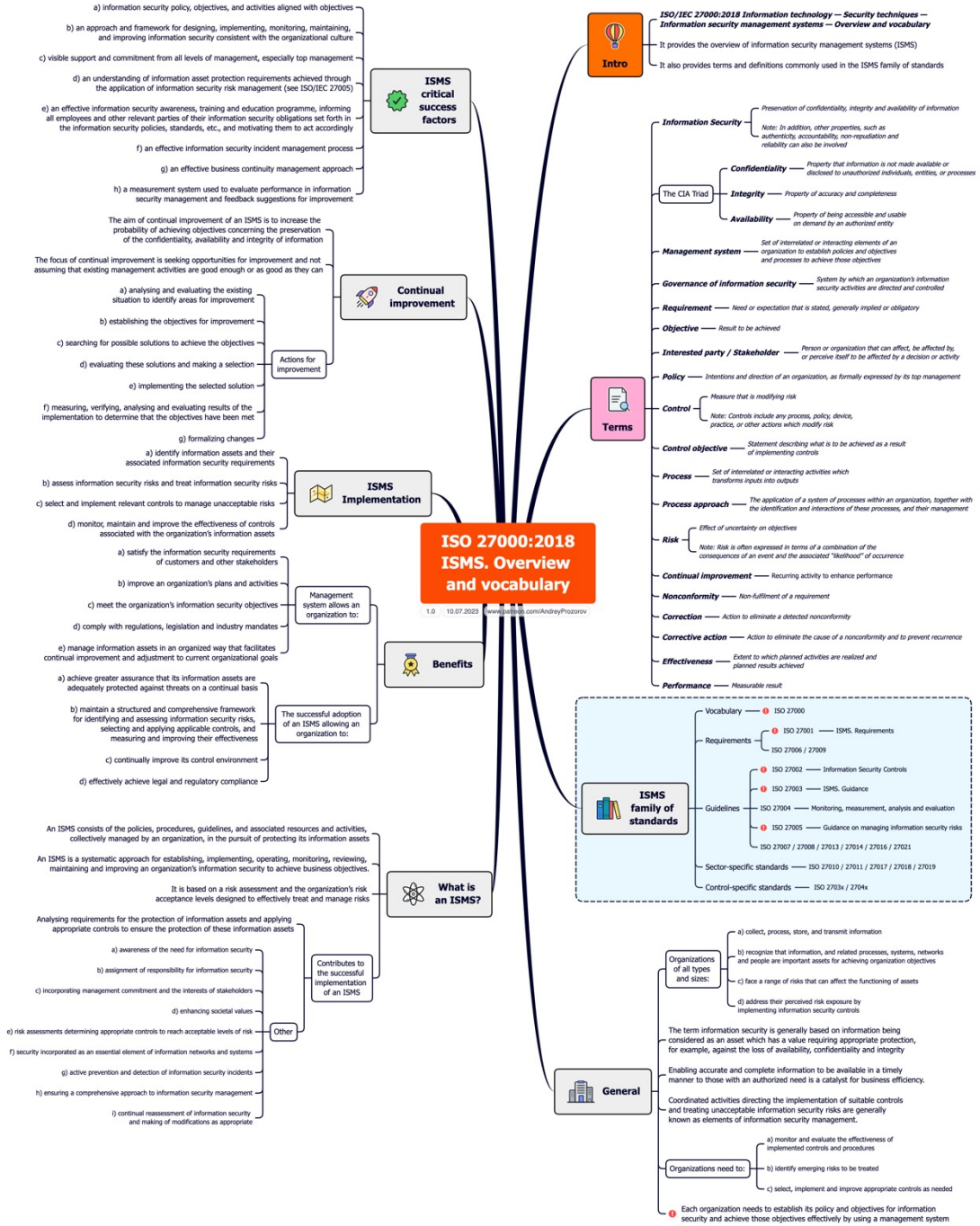
ISO/IEC 27000:2018 provides **the overview** of **information security management systems (ISMS)**.

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.

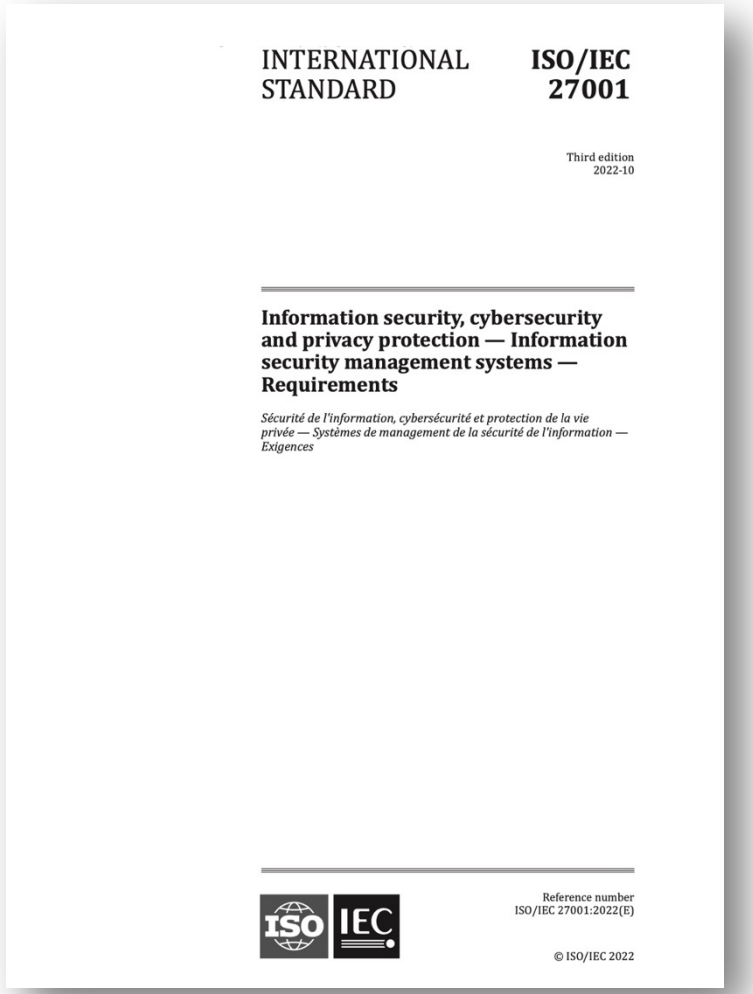
Number of pages: 27



Contents

Page

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

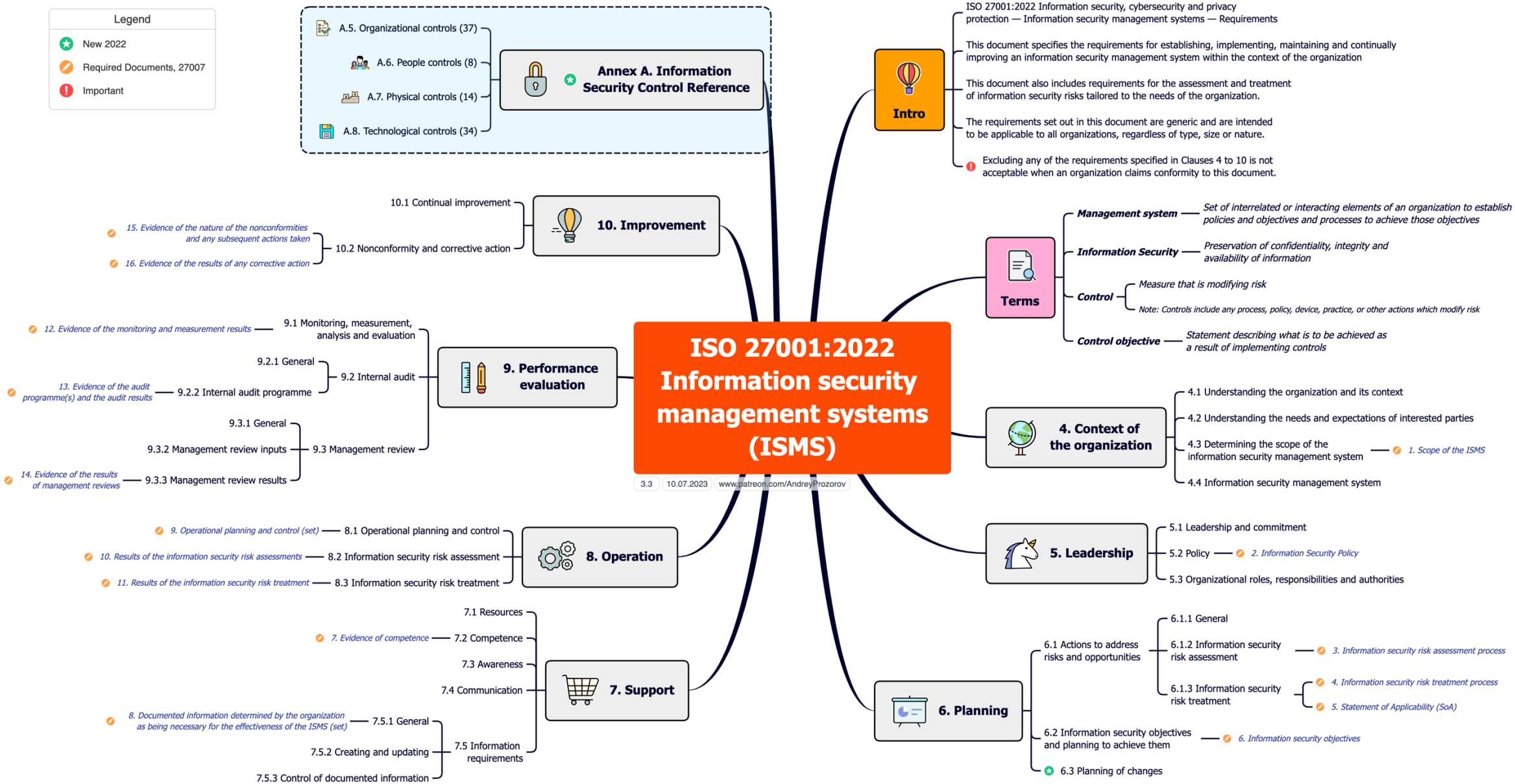
This standard specifies the **requirements** for establishing, implementing, maintaining and continually improving an **information security management system (ISMS)** within the context of the organization.

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.

Number of pages: 19


Legend
New 2022
Required Documents, 27007
Important
ISO 27001:2022 Information security management systems (ISMS)
3.3
10.07.2023
www.patreon.com/AndreyProzorov
Intro
ISO 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements
This document specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system 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.
Terms
Management system
Set of interrelated or interacting elements of an organization to establish policies and objectives and processes to achieve those objectives
Information Security
Preservation of confidentiality, integrity and availability of information
Control
Measure that is modifying risk
Note: Controls include any process, policy, device, practice, or other actions which modify risk
Control objective
Statement describing what is to be achieved as a result of implementing controls
4. Context of the organization
4.1 Understanding the organization and its context
4.2 Understanding the needs and expectations of interested parties
4.3 Determining the scope of the information security management system
1. Scope of the ISMS
4.4 Information security management system
5. Leadership
5.1 Leadership and commitment
5.2 Policy
2. Information Security Policy
5.3 Organizational roles, responsibilities and authorities
6. Planning
6.1 Actions to address risks and opportunities
6.1.1 General
6.1.2 Information security risk assessment
3. Information security risk assessment process
6.1.3 Information security risk treatment
4. Information security risk treatment process
5. Statement of Applicability (SoA)
6.2 Information security objectives and planning to achieve them
6. Information security objectives
6.3 Planning of changes
7. Support
7.1 Resources
7.2 Competence
7. Evidence of competence
7.3 Awareness
7.4 Communication
7.5 Information requirements
7.5.1 General
8. Documented information determined by the organization as being necessary for the effectiveness of the ISMS (set)
7.5.2 Creating and updating
7.5.3 Control of documented information
8. Operation
8.1 Operational planning and control
9. Operational planning and control (set)
8.2 Information security risk assessment
10. Results of the information security risk assessments
8.3 Information security risk treatment
11. Results of the information security risk treatment
9. Performance evaluation
9.1 Monitoring, measurement, analysis and evaluation
12. Evidence of the monitoring and measurement results
9.2 Internal audit
9.2.1 General
9.2.2 Internal audit programme
13. Evidence of the audit programme(s) and the audit results
9.3 Management review
9.3.1 General
9.3.2 Management review inputs
9.3.3 Management review results
14. Evidence of the results of management reviews
10. Improvement
10.1 Continual improvement
10.2 Nonconformity and corrective action
15. Evidence of the nature of the nonconformities and any subsequent actions taken
16. Evidence of the results of any corrective action
Annex A. Information Security Control Reference
A.5. Organizational controls (37)
A.6. People controls (8)
A.7. Physical controls (14)
A.8. Technological controls (34)

ISO 27001:2022. ISMS Requirements and Information security controls

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

ISMS Requirements (ISO 27001)

4. Context of the organization
4.1 Understanding the organization and its context / 4.2 Understanding the needs and expectations of interested parties / 4.3 Determining the scope of the ISMS / 4.4 ISMS

5. Leadership
5.1 Leadership and commitment / 5.2 Policy / 5.3 Organizational roles, responsibilities and authorities

6. Planning
6.1 Actions to address risks and opportunities / 6.2 Information security objectives and planning to achieve them / 6.3 Planning of changes

7. Support
7.1 Resources / 7.2 Competence / 7.3 Awareness / 7.4 Communication / 7.5 Documented information

8. Operation
8.1 Operational planning and control / 8.2 Information security risk assessment / 8.3 Information security risk treatment

9. Performance evaluation
9.1 Monitoring, measurement, analysis and evaluation / 9.2 Internal audit / 9.3 Management review

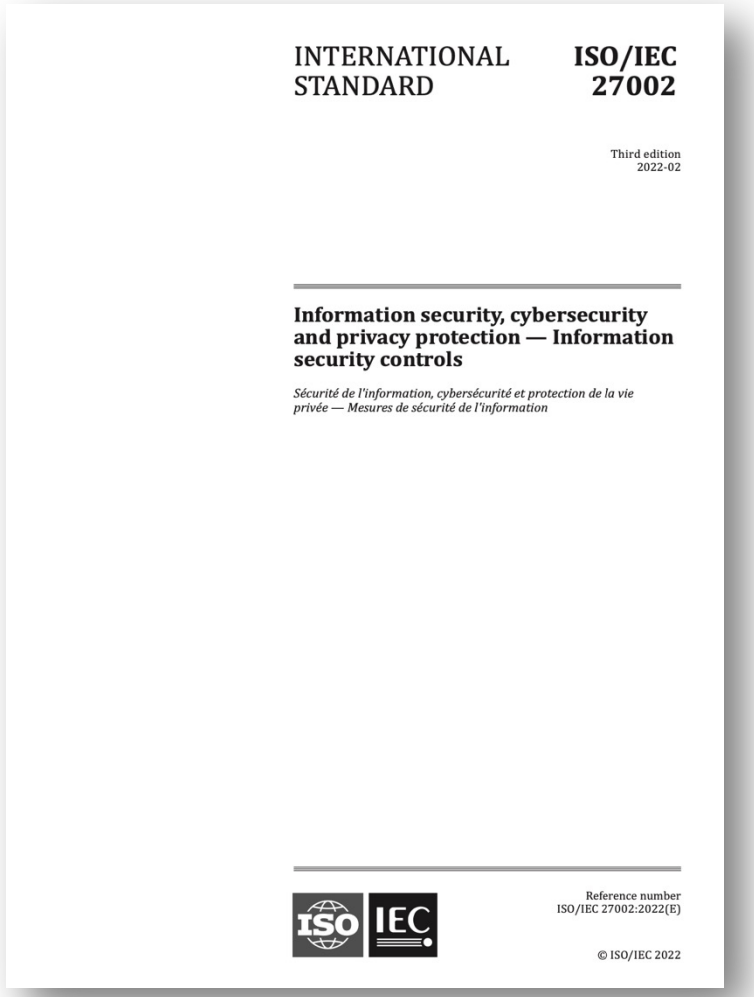
10. Improvement
10.1 Continual improvement / 10.2 Nonconformity and corrective action

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 controls, 2022

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.

Number of pages: 152

Control*: *measure that is modifying risk

Note 1 to entry: Controls include any process, policy, device, practice, or other actions which modify risk

Note 2 to entry: It is possible that controls not always exert the intended or assumed modifying effect

5.1 Policies for information security

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Governance	#Governance_and_Eco-system #Resilience

Control

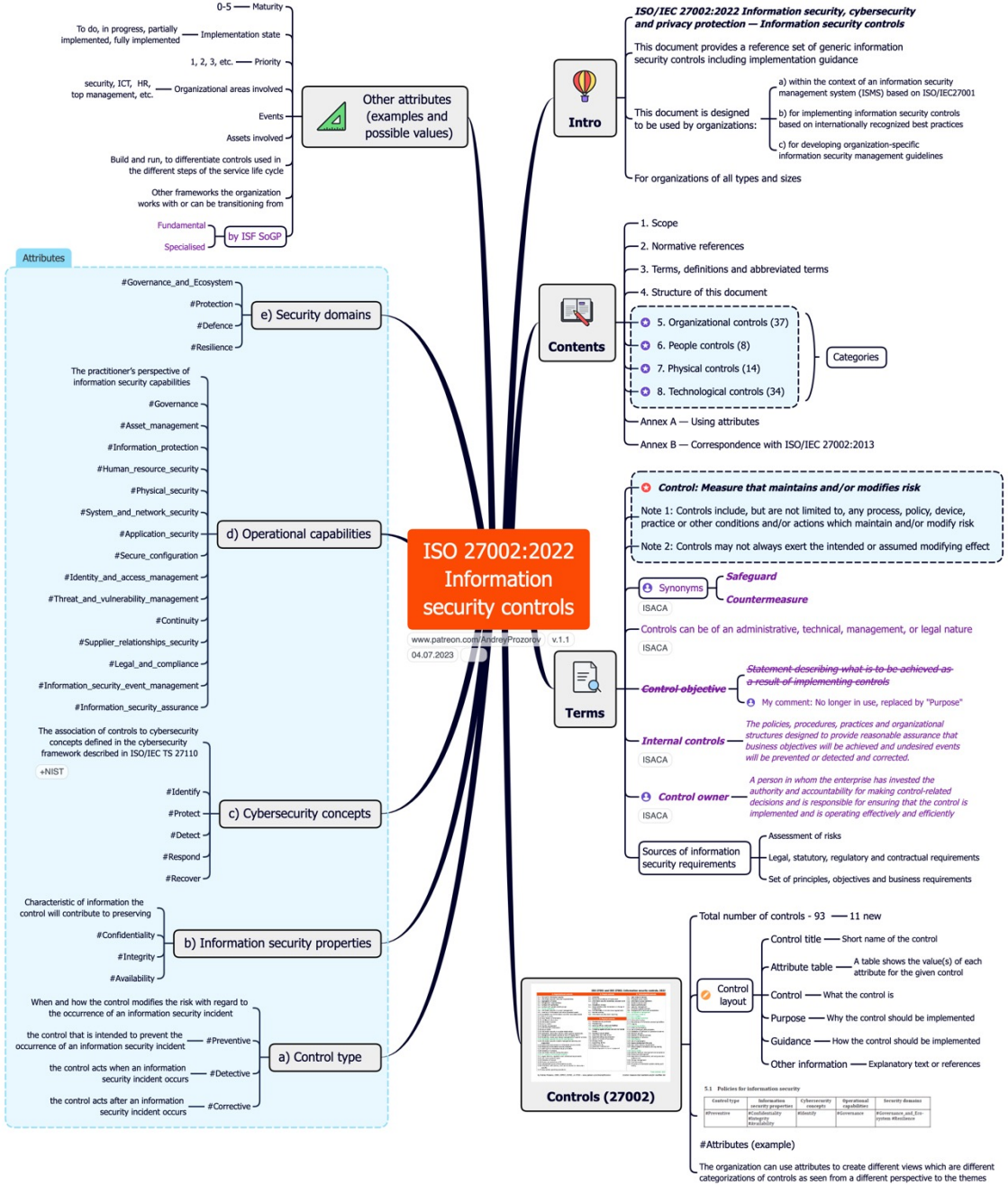
Information security policy and topic-specific policies should be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.

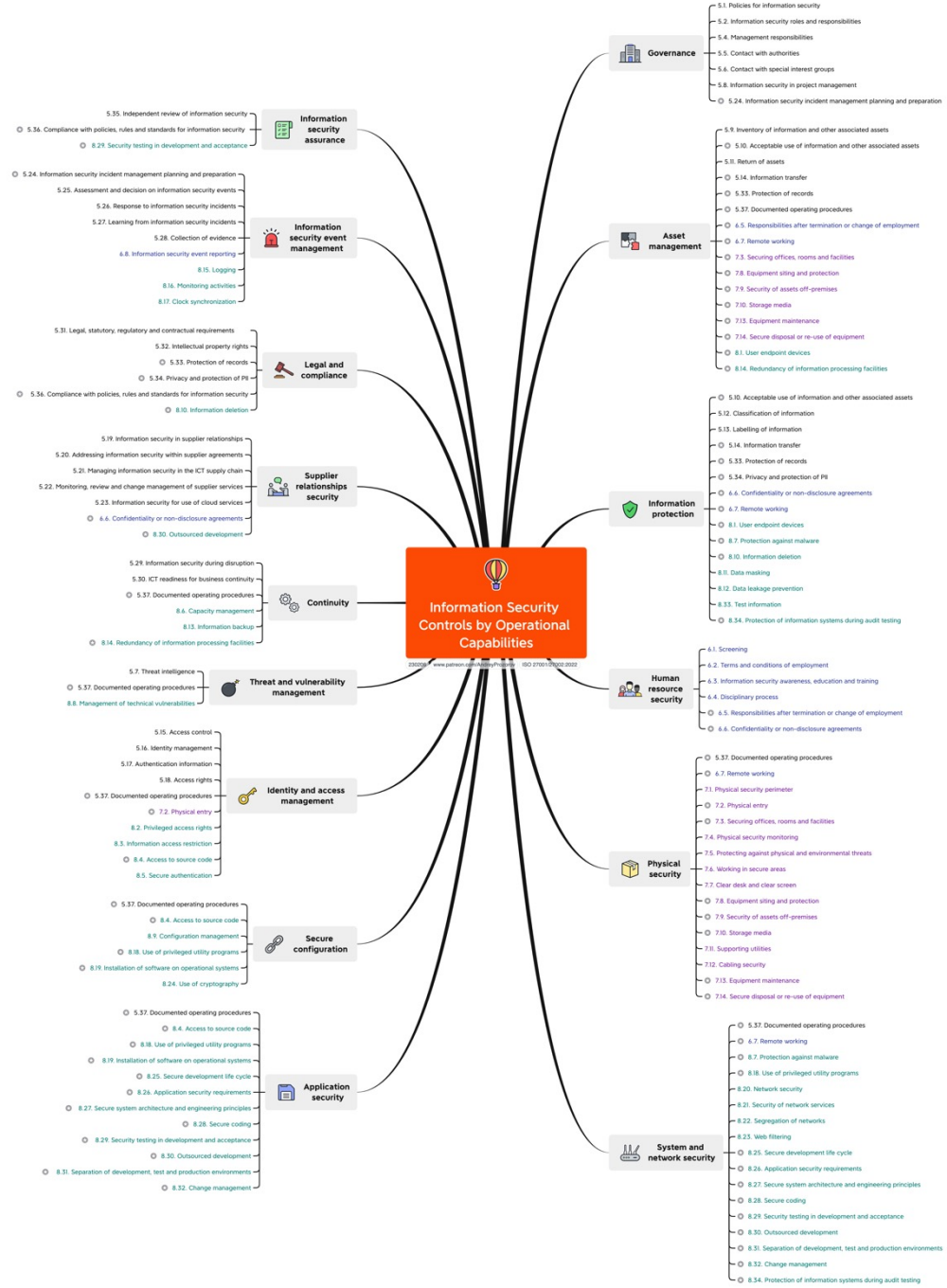
Purpose

To ensure continuing suitability, adequacy, effectiveness of management direction and support for information security in accordance with business, legal, statutory, regulatory and contractual requirements.

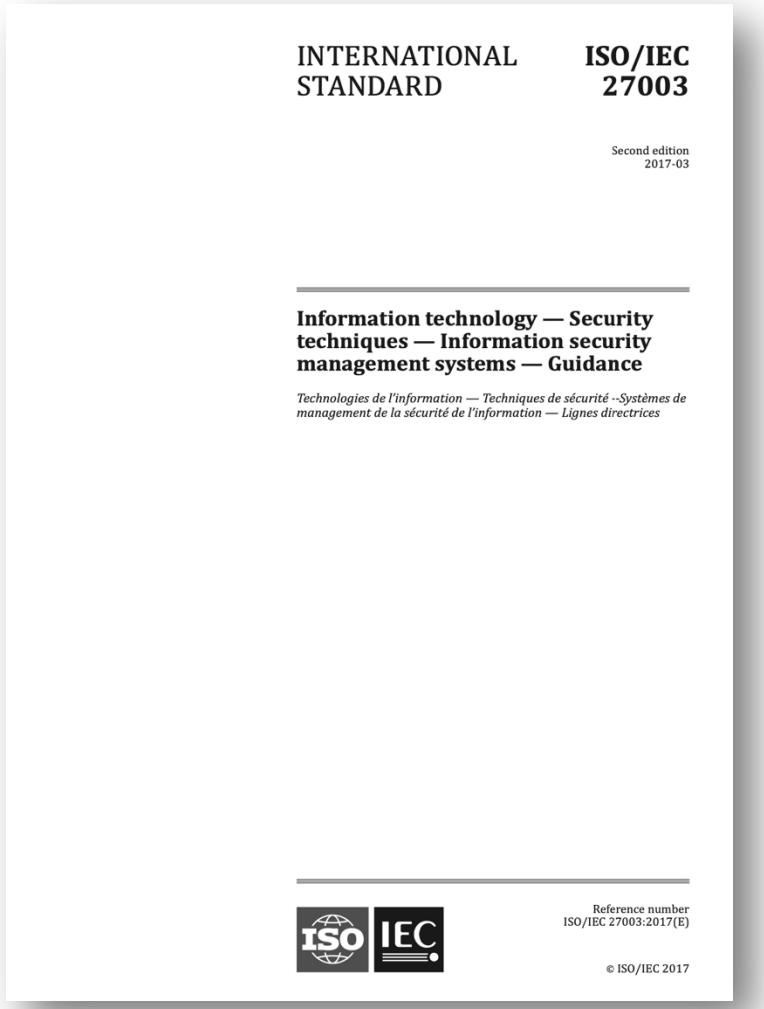
ISO 27002:2022, Attributes

Control type	Information security properties (CIA)	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive #Detective #Corrective	#Confidentiality #Integrity #Availability	#Identify #Protect #Detect #Respond #Recover	#Governance #Asset_management #Information_protection #Human_resource_security #Physical_security #System_and_network_security #Application_security #Secure_configuration #Identity_and_access_management #Threat_and_vulnerability_management #Continuity #Supplier_relationships_security #Legal_and_ compliance #Information_security_event_management #Information_security_assurance	#Governance_and_ Ecosystem #Protection #Defence #Resilience


ISO 27002:2022 Information security controls
www.patreon.com/AndreyProzorov
v.1.1
04.07.2023
Intro
ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls
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/IEC27001
b) for implementing information security controls based on internationally recognized best practices
c) for developing organization-specific information security management guidelines
For organizations of all types and sizes
Contents
1. Scope
2. Normative references
3. Terms, definitions and abbreviated terms
4. Structure of this document
5. Organizational controls (37)
6. People controls (8)
7. Physical controls (14)
8. Technological controls (34)
Categories
Annex A — Using attributes
Annex B — Correspondence with ISO/IEC 27002:2013
Terms
Control: Measure that maintains and/or modifies risk
Note 1: Controls include, but are not limited to, any process, policy, device, practice or other conditions and/or actions which maintain and/or modify risk
Note 2: Controls may not always exert the intended or assumed modifying effect
Synonyms
Safeguard
Countermeasure
ISACA
Controls can be of an administrative, technical, management, or legal nature
ISACA
Control objective
Statement describing what is to be achieved as a result of implementing controls
My comment: No longer in use, replaced by "Purpose"
Internal controls
The policies, procedures, practices and organizational structures designed to provide reasonable assurance that business objectives will be achieved and undesired events will be prevented or detected and corrected.
ISACA
Control owner
A person in whom the enterprise has invested the authority and accountability for making control-related decisions and is responsible for ensuring that the control is implemented and is operating effectively and efficiently
ISACA
Sources of information security requirements
Assessment of risks
Legal, statutory, regulatory and contractual requirements
Set of principles, objectives and business requirements
Controls (27002)
Total number of controls - 93
11 new
Control layout
Control title — Short name of the control
Attribute table — A table shows the value(s) of each attribute for the given control
Control — What the control is
Purpose — Why the control should be implemented
Guidance — How the control should be implemented
Other information — Explanatory text or references
#Attributes (example)
The organization can use attributes to create different views which are different categorizations of controls as seen from a different perspective to the themes
Other attributes (examples and possible values)
Maturity
0-5
Implementation state
To do, in progress, partially implemented, fully implemented
Priority
1, 2, 3, etc.
Organizational areas involved
security, ICT, HR, top management, etc.
Events
Assets involved
Build and run, to differentiate controls used in the different steps of the service life cycle
Other frameworks the organization works with or can be transitioning from
by ISF SoGP
Fundamental
Specialised
Attributes
e) Security domains
#Governance_and_Ecosystem
#Protection
#Defence
#Resilience
d) Operational capabilities
The practitioner's perspective of information security capabilities
#Governance
#Asset_management
#Information_protection
#Human_resource_security
#Physical_security
#System_and_network_security
#Application_security
#Secure_configuration
#Identity_and_access_management
#Threat_and_vulnerability_management
#Continuity
#Supplier_relationships_security
#Legal_and_compliance
#Information_security_event_management
#Information_security_assurance
c) Cybersecurity concepts
The association of controls to cybersecurity concepts defined in the cybersecurity framework described in ISO/IEC TS 27110
+NIST
#Identify
#Protect
#Detect
#Respond
#Recover
b) Information security properties
Characteristic of information the control will contribute to preserving
#Confidentiality
#Integrity
#Availability
a) Control type
When and how the control modifies the risk with regard to the occurrence of an information security incident
the control that is intended to prevent the occurrence of an information security incident
#Preventive
the control acts when an information security incident occurs
#Detective
the control acts after an information security incident occurs
#Corrective


Information Security Controls by Operational Capabilities
Governance
5.1. Policies for information security
5.2. Information security roles and responsibilities
5.4. Management responsibilities
5.5. Contact with authorities
5.6. Contact with special interest groups
5.8. Information security in project management
5.24. Information security incident management planning and preparation
Asset 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
5.14. Information transfer
5.33. Protection of records
5.37. Documented operating procedures
6.5. Responsibilities after termination or change of employment
6.7. Remote working
7.3. Securing offices, rooms and facilities
7.8. Equipment siting and protection
7.9. Security of assets off-premises
7.10. Storage media
7.13. Equipment maintenance
7.14. Secure disposal or re-use of equipment
8.1. User endpoint devices
8.14. Redundancy of information processing facilities
Information protection
5.10. Acceptable use of information and other associated assets
5.12. Classification of information
5.13. Labelling of information
5.14. Information transfer
5.33. Protection of records
5.34. Privacy and protection of PII
6.6. Confidentiality or non-disclosure agreements
6.7. Remote working
8.1. User endpoint devices
8.7. Protection against malware
8.10. Information deletion
8.11. Data masking
8.12. Data leakage prevention
8.33. Test information
8.34. Protection of information systems during audit testing
Human resource security
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
Physical security
5.37. Documented operating procedures
6.7. Remote working
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
System and network security
5.37. Documented operating procedures
6.7. Remote working
8.7. Protection against malware
8.18. Use of privileged utility programs
8.20. Network security
8.21. Security of network services
8.22. Segregation of networks
8.23. Web filtering
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
8.34. Protection of information systems during audit testing
Application security
5.37. Documented operating procedures
8.4. Access to source code
8.18. Use of privileged utility programs
8.19. Installation of software on operational systems
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
Secure configuration
5.37. Documented operating procedures
8.4. Access to source code
8.9. Configuration management
8.18. Use of privileged utility programs
8.19. Installation of software on operational systems
8.24. Use of cryptography
Identity and access management
5.15. Access control
5.16. Identity management
5.17. Authentication information
5.18. Access rights
5.37. Documented operating procedures
7.2. Physical entry
8.2. Privileged access rights
8.3. Information access restriction
8.4. Access to source code
8.5. Secure authentication
Threat and vulnerability management
5.7. Threat intelligence
5.37. Documented operating procedures
8.8. Management of technical vulnerabilities
Continuity
5.29. Information security during disruption
5.30. ICT readiness for business continuity
5.37. Documented operating procedures
8.6. Capacity management
8.13. Information backup
8.14. Redundancy of information processing facilities
Supplier relationships security
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
6.6. Confidentiality or non-disclosure agreements
8.30. Outsourced development
Legal and compliance
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
5.36. Compliance with policies, rules and standards for information security
8.10. Information deletion
Information security event management
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
6.8. Information security event reporting
8.15. Logging
8.16. Monitoring activities
8.17. Clock synchronization
Information security assurance
5.35. Independent review of information security
5.36. Compliance with policies, rules and standards for information security
8.29. Security testing in development and acceptance

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

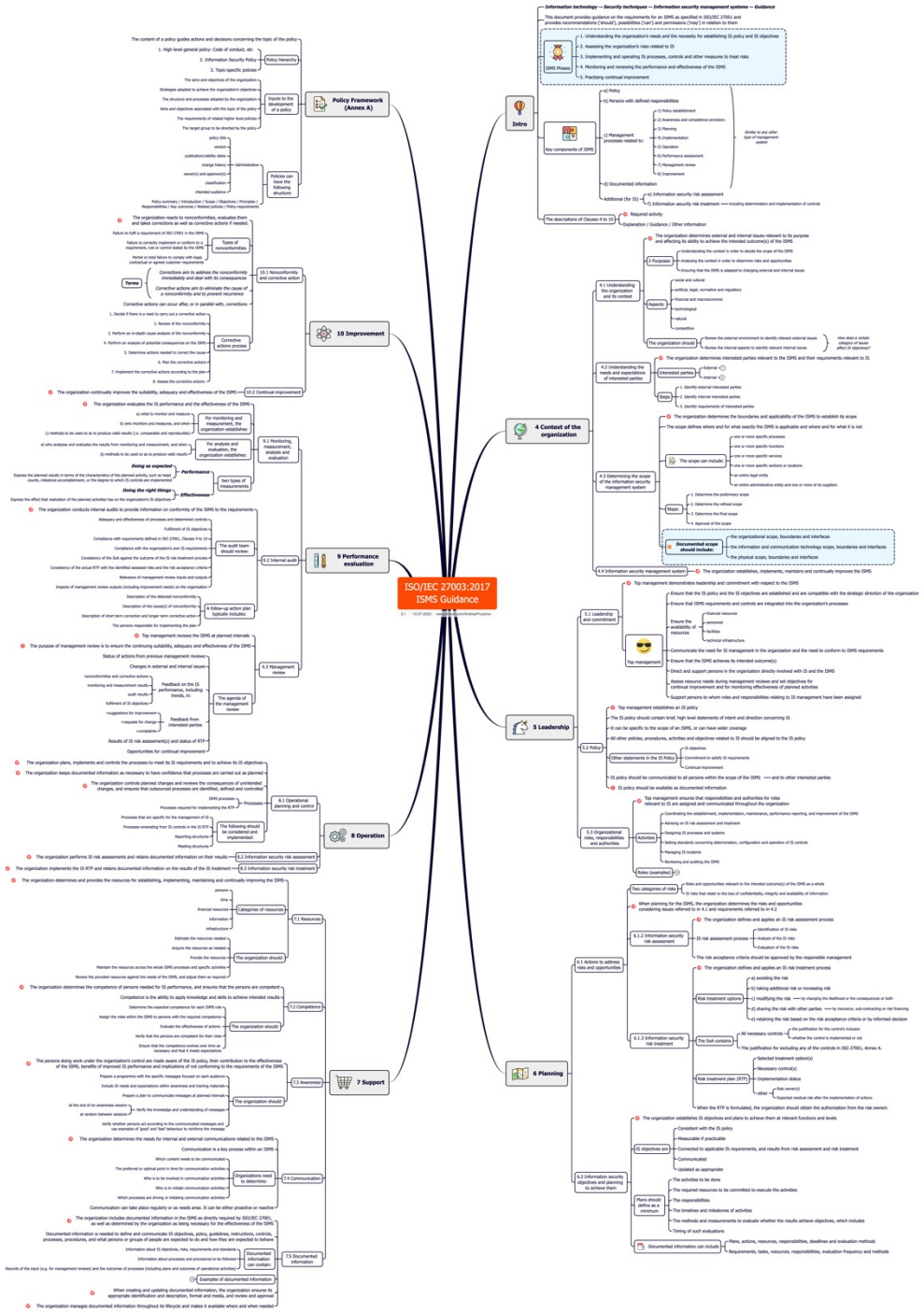
Reference number
ISO/IEC 27003:2017(E)

© 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.

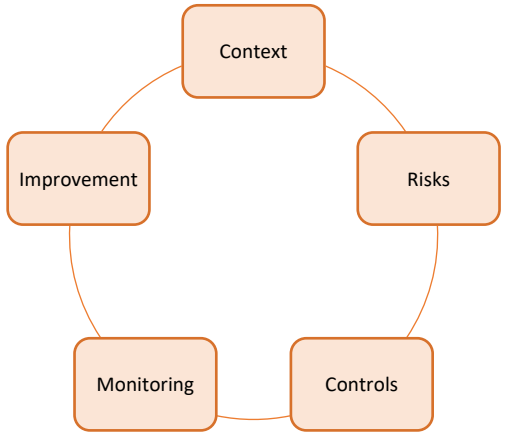
Number of pages: 45



Contents

ISO 27003: 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



ISO 27003: ISMS Components

An ISMS, similar to any other type of management system, includes the following key components:

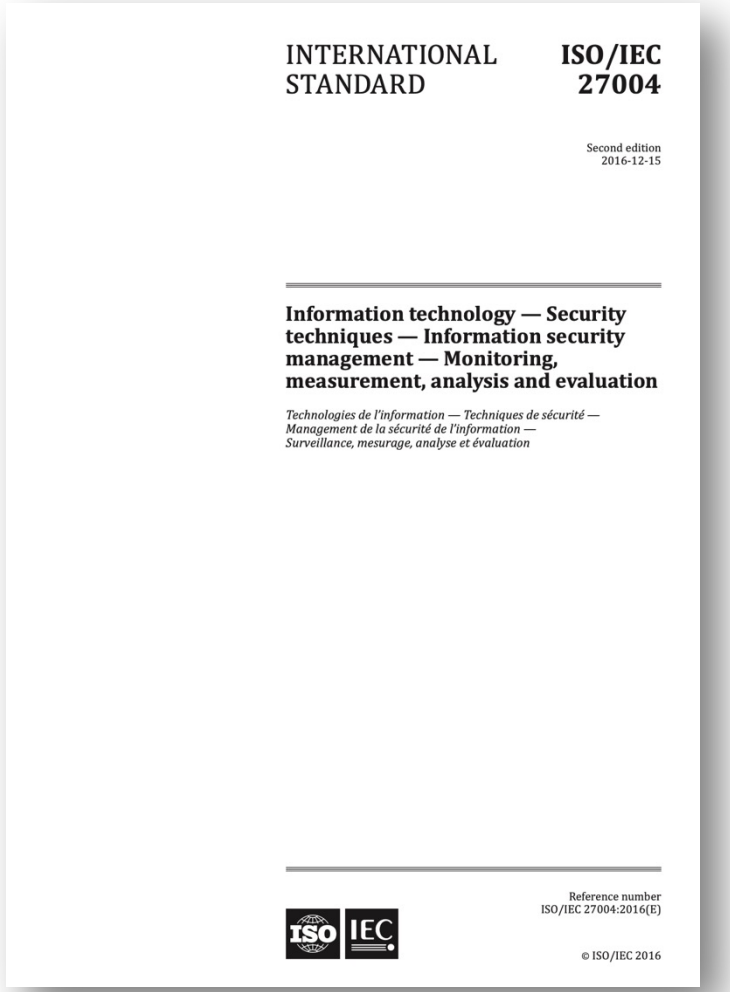
1. Policy
2. Persons with defined responsibilities
3. Management processes related to:
    1) policy establishment
    2) awareness and competence provision
    3) planning
    4) implementation
    5) operation
    6) performance assessment
    7) management review
    8) improvement
4. Documented information

An ISMS has additional key components such as:

5. Information security risk assessment; and
6. information security risk treatment, including determination and implementation of controls.

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

ISO 27004 Monitoring and Measurement


INTERNATIONAL STANDARD

ISO/IEC 27004

Second edition
2016-12-15

Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation

Technologies de l'information — Techniques de sécurité — Management de la sécurité de l'information — Surveillance, mesurage, analyse et évaluation

Reference number
ISO/IEC 27004:2016(E)

© ISO/IEC 2016

This document provides guidelines intended to assist organizations in **evaluating the information security performance and the effectiveness** of an information security management system in order to fulfil the requirements of ISO/IEC 27001:2013, 9.1.

It establishes:

a) the monitoring and measurement of information security performance;

b) the monitoring and measurement of the effectiveness of an information security management system (ISMS) including its processes and controls;

c) the analysis and evaluation of the results of monitoring and measurement.

Number of pages: 58

Contents

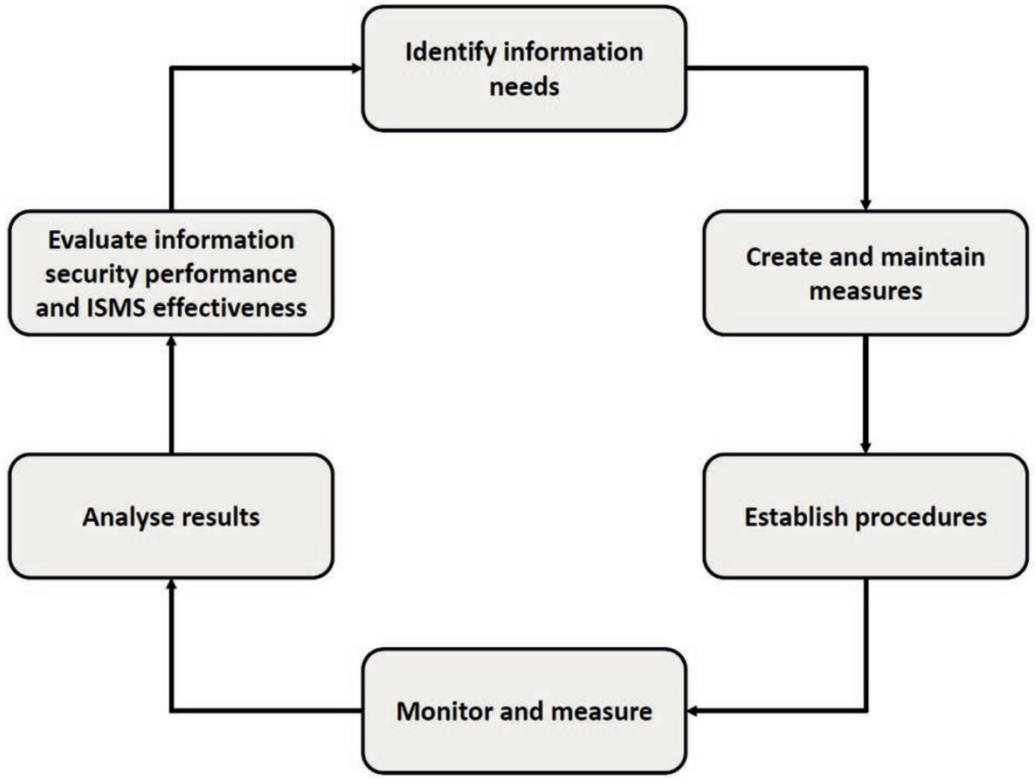


Figure 2 — Monitoring, measurement, analysis and evaluation processes

Table 1 — Example security measure descriptors

Information descriptor	Meaning or purpose
Measure ID	Specific identifier.
Information need	Over-arching need for understanding to which the measure contributes.
Measure	Statement of measurement, generally described using a word such as "percentage", "number", "frequency" and "average".
Formula/scoring	How the measure should be evaluated, calculated or scored.
Target	Desired result of the measurement, e.g., a milestone or a statistical measure or a set of thresholds. Note that ongoing monitoring can be required to ensure continued attainment of the target.
Implementation evidence	Evidence that validates that the measurement is performed, helps identify possible causes of poor results, and provides input to the process. Data to provide input into the formula.
Frequency	How frequently the data should be collected and reported. There can be a reason for having multiple frequencies.
Responsible parties	The person responsible for gathering and processing the measure. At the least, an Information Owner, Information Collector and Measurement Client should be identified.
Data source	Potential data sources can be databases, tracking tools, other parts of, the organization, external organizations, or specific individual roles.
Reporting format	How the measure should be collected and reported, e.g., as text, numerically, graphically (pie chart, line chart, bar graph etc.), as part of a 'dashboard' or another form of presentation.

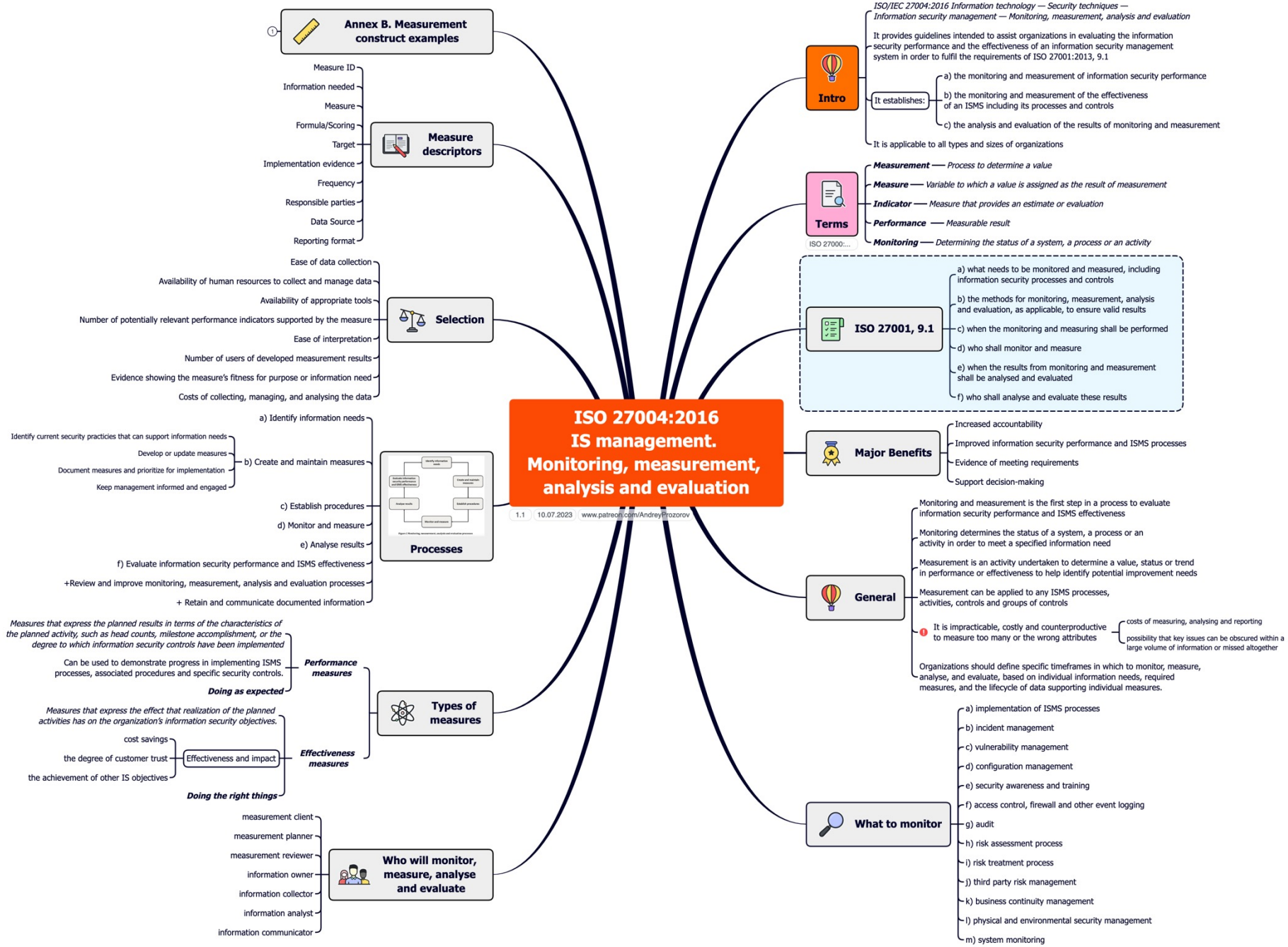
B.2 Resource allocation
B.3 Policy review
B.4 Management commitment
B.5 Risk exposure
B.6 Audit programme
B.7 Improvement actions
B.8 Security incidents cost
B.9 Learning form information security incidents
B.10 Corrective action implementation
B.11 ISMS training or ISMS awareness
B.12 Information security training
B.13 Information security awareness compliance
B.14 ISMS awareness campaigns effectiveness
B.15 Social engineering preparedness
B.16 Password quality – manual
B.17 Password quality – automated
B.18 Review of user access rights
B.19 Physical entry controls system evaluation
B.20 Physical entry controls effectiveness
B.21 Management of periodic maintenance
B.22 Change management
B.23 Protection against malicious code
B.24 Anti-malware
B.25 Total availability
B.26 Firewall rules
B.27 Log files review
B.28 Device configuration
B.29 Pentest and vulnerability assessment
B.30 Vulnerability landscape
B.31.1/B.31.2 Security in third party agreements
B.32 Security incident management effectiveness
B.33 Security incidents trend
B.34 Security event reporting
B.35 ISMS review process
B.36 Vulnerability coverage

35 examples

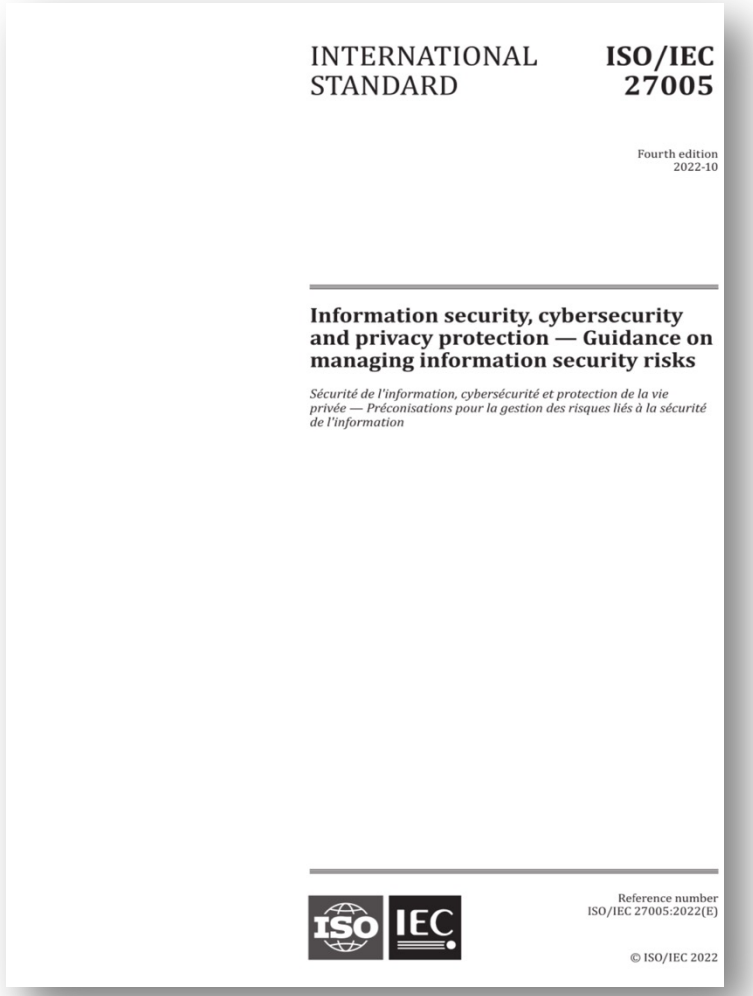
B.3 Policy review

Information descriptor	Meaning or purpose
Measure ID	Organization-defined
Information need	To evaluate whether the policies for information security are reviewed at planned intervals or if significant changes occur
Measure	Percentage of policy reviewed
Formula/scoring	Number of information security policies that were reviewed in previous year/ Number of information security policies in place * 100
Target	Green: >80, Orange >=40%, Red <40%
Implementation evidence	Document history mentioning review of document or document list indicating date of last review
Frequency	Collect: after planned interval defined for reviews (e.g. yearly or after significant changes) Report: for each collection
Responsible parties	Information owner: Policy owner who has approved management responsibility for the development, review and evaluation of the policy Information collector: Internal auditor Measurement client: Chief information security officer
Data source	Review plan of policies, history section of a security policy, list of documents
Reporting format	Pie chart for current situation and line chart for compliance evolution representation

Relationship	ISO/IEC 27001:2013, A.5.1.2: Review of the policies for information security ISO/IEC 27001:2013, 7.5.2: Creating and updating of documented information


ISO 27004:2016
IS management.
Monitoring, measurement, analysis and evaluation
1.1
10.07.2023
www.patreon.com/AndreyProzorov
Intro
ISO/IEC 27004:2016 Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation
It provides guidelines intended to assist organizations in evaluating the information security performance and the effectiveness of an information security management system in order to fulfil the requirements of ISO 27001:2013, 9.1
It establishes:
a) the monitoring and measurement of information security performance
b) the monitoring and measurement of the effectiveness of an ISMS including its processes and controls
c) the analysis and evaluation of the results of monitoring and measurement
It is applicable to all types and sizes of organizations
Terms
ISO 27000:...
Measurement — Process to determine a value
Measure — Variable to which a value is assigned as the result of measurement
Indicator — Measure that provides an estimate or evaluation
Performance — Measurable result
Monitoring — Determining the status of a system, a process or an activity
ISO 27001, 9.1
a) what needs to be monitored and measured, including information security processes and controls
b) the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results
c) when the monitoring and measuring shall be performed
d) who shall monitor and measure
e) when the results from monitoring and measurement shall be analysed and evaluated
f) who shall analyse and evaluate these results
Major Benefits
Increased accountability
Improved information security performance and ISMS processes
Evidence of meeting requirements
Support decision-making
General
Monitoring and measurement is the first step in a process to evaluate information security performance and ISMS effectiveness
Monitoring determines the status of a system, a process or an activity in order to meet a specified information need
Measurement is an activity undertaken to determine a value, status or trend in performance or effectiveness to help identify potential improvement needs
Measurement can be applied to any ISMS processes, activities, controls and groups of controls
It is impracticable, costly and counterproductive to measure too many or the wrong attributes
costs of measuring, analysing and reporting
possibility that key issues can be obscured within a large volume of information or missed altogether
Organizations should define specific timeframes in which to monitor, measure, analyse, and evaluate, based on individual information needs, required measures, and the lifecycle of data supporting individual measures.
What to monitor
a) implementation of ISMS processes
b) incident management
c) vulnerability management
d) configuration management
e) security awareness and training
f) access control, firewall and other event logging
g) audit
h) risk assessment process
i) risk treatment process
j) third party risk management
k) business continuity management
l) physical and environmental security management
m) system monitoring
Who will monitor, measure, analyse and evaluate
measurement client
measurement planner
measurement reviewer
information owner
information collector
information analyst
information communicator
Types of measures
Performance measures
Measures that express the planned results in terms of the characteristics of the planned activity, such as head counts, milestone accomplishment, or the degree to which information security controls have been implemented
Can be used to demonstrate progress in implementing ISMS processes, associated procedures and specific security controls.
Doing as expected
Effectiveness measures
Measures that express the effect that realization of the planned activities has on the organization's information security objectives.
Effectiveness and impact
cost savings
the degree of customer trust
the achievement of other IS objectives
Doing the right things
Processes
a) Identify information needs
b) Create and maintain measures
Identify current security practicies that can support information needs
Develop or update measures
Document measures and prioritize for implementation
Keep management informed and engaged
c) Establish procedures
d) Monitor and measure
e) Analyse results
f) Evaluate information security performance and ISMS effectiveness
+Review and improve monitoring, measurement, analysis and evaluation processes
+ Retain and communicate documented information
Selection
Ease of data collection
Availability of human resources to collect and manage data
Availability of appropriate tools
Number of potentially relevant performance indicators supported by the measure
Ease of interpretation
Number of users of developed measurement results
Evidence showing the measure's fitness for purpose or information need
Costs of collecting, managing, and analysing the data
Measure descriptors
Measure ID
Information needed
Measure
Formula/Scoring
Target
Implementation evidence
Frequency
Responsible parties
Data Source
Reporting format
Annex B. Measurement construct examples

ISO 27005 Guidance on managing IS risks



This document provides guidance to assist organizations to:

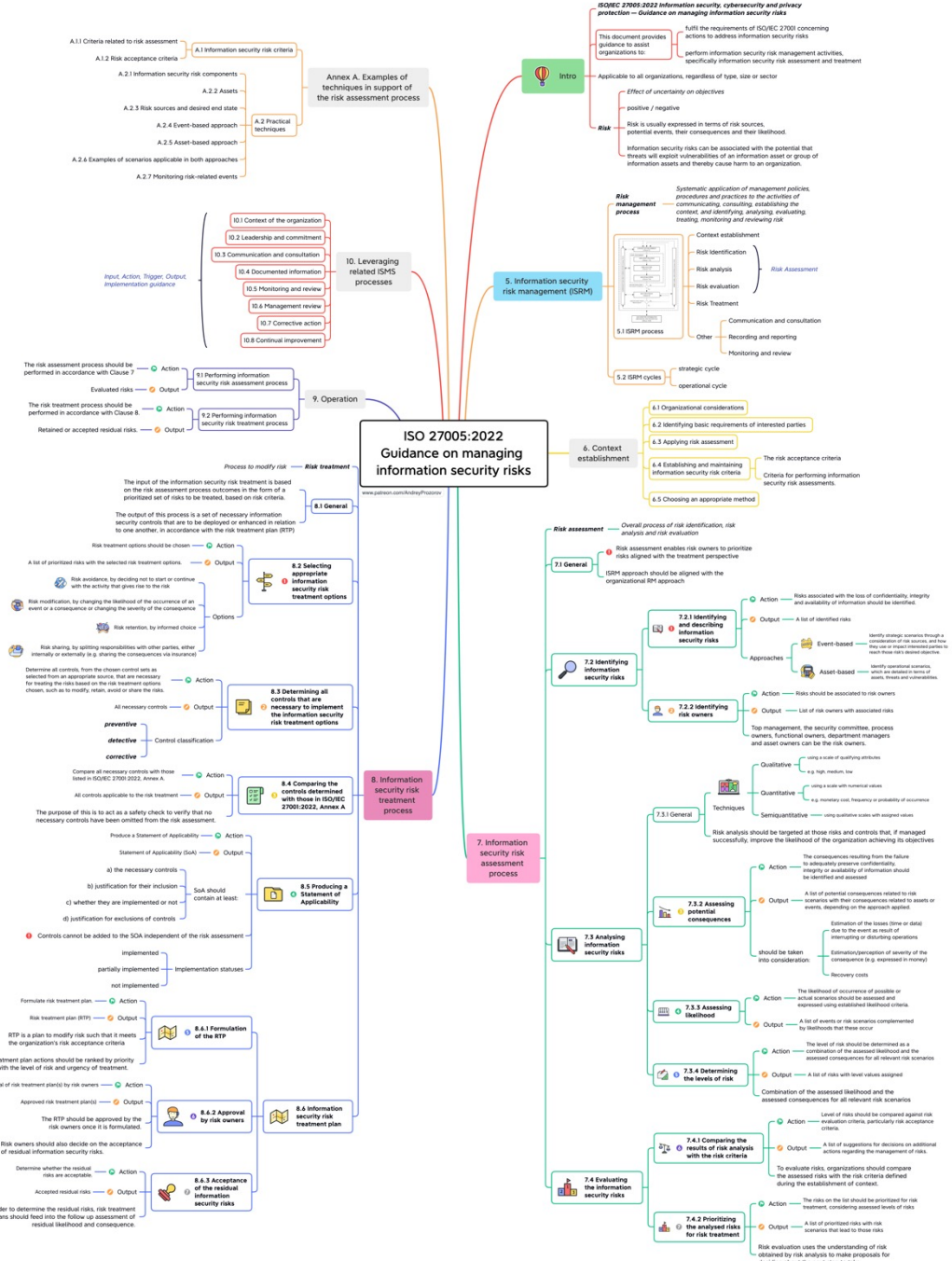
- fulfil the requirements of ISO/IEC 27001 concerning actions to address **information security risks**;
- perform information security risk management activities, specifically **information security risk assessment and treatment**.

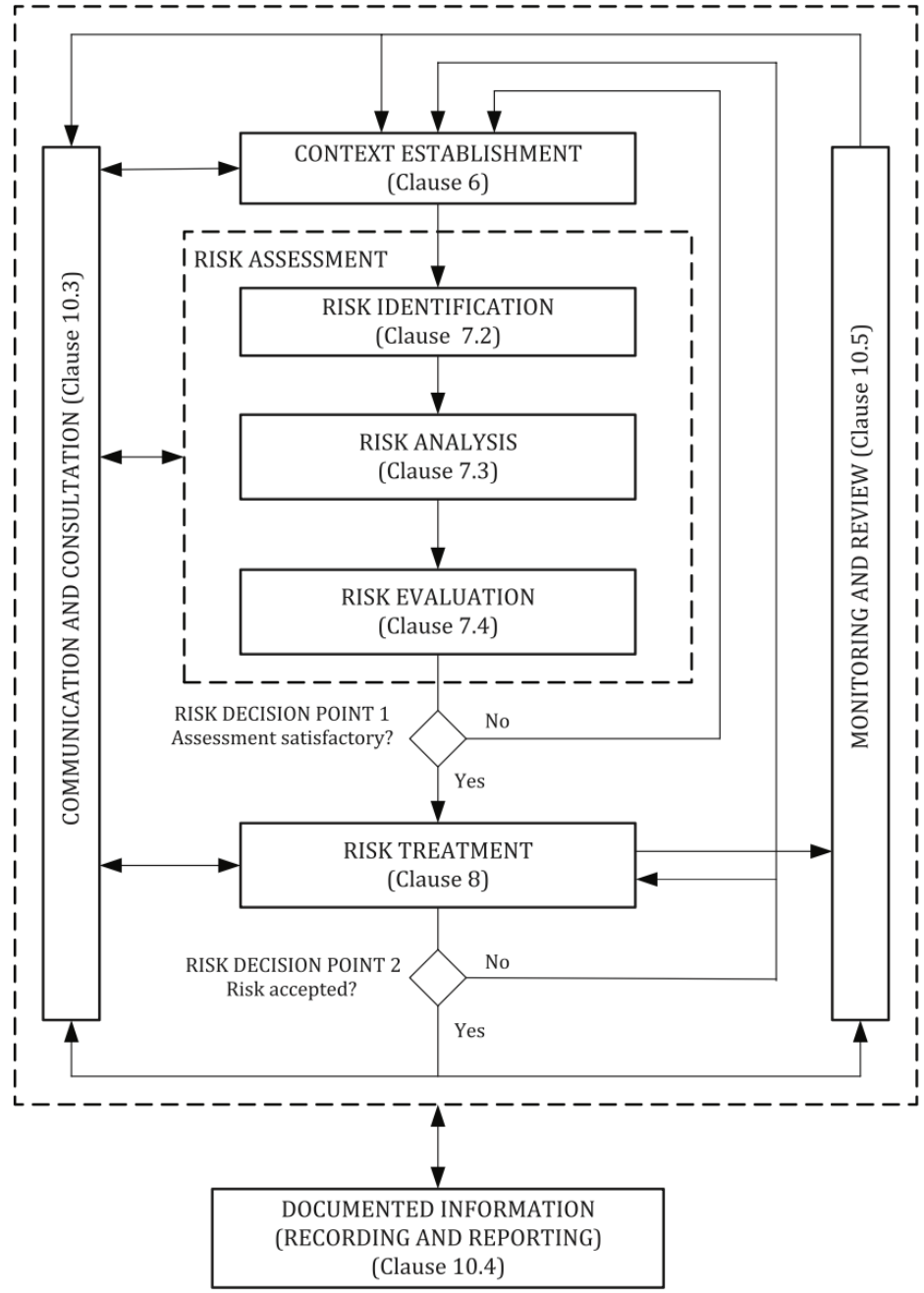
This document is applicable to all organizations, regardless of type, size or sector.

Number of pages: 62

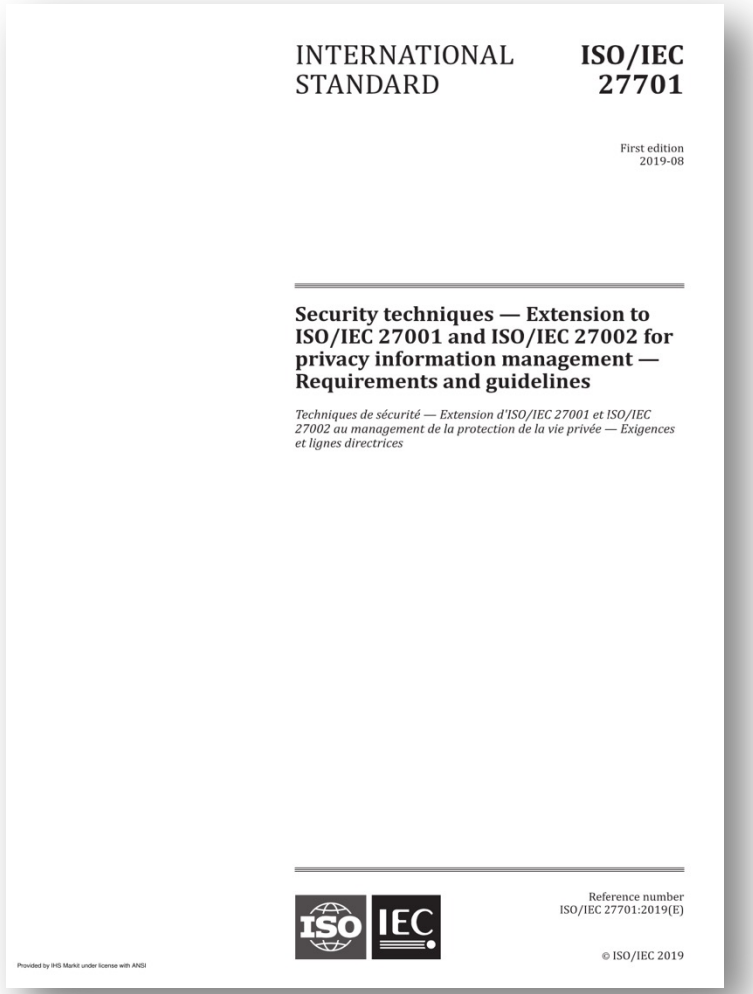
Contents

Page


ISO 27005:2022
Guidance on managing information security risks
www.patreon.com/AndreyProzorov
Intro
ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection — Guidance on managing information security 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
Applicable to all organizations, regardless of type, size or sector
Risk
Effect of uncertainty on objectives
positive / negative
Risk is usually expressed in terms of risk sources, potential events, their consequences and their likelihood.
Information security risks can be 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.
5. Information security risk management (ISRM)
Risk management process
Systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analysing, evaluating, treating, monitoring and reviewing risk
5.1 ISRM process
Context establishment
Risk Identification
Risk analysis
Risk evaluation
Risk Assessment
Risk Treatment
Communication and consultation
Other
Recording and reporting
Monitoring and review
5.2 ISRM cycles
strategic cycle
operational cycle
6. Context establishment
6.1 Organizational considerations
6.2 Identifying basic requirements of interested parties
6.3 Applying risk assessment
6.4 Establishing and maintaining information security risk criteria
The risk acceptance criteria
Criteria for performing information security risk assessments.
6.5 Choosing an appropriate method
7. Information security risk assessment process
Risk assessment
Overall process of risk identification, risk analysis and risk evaluation
7.1 General
Risk assessment enables risk owners to prioritize risks aligned with the treatment perspective
ISRM approach should be aligned with the organizational RM approach
7.2 Identifying information security risks
7.2.1 Identifying and describing information security risks
Action
Risks associated with the loss of confidentiality, integrity and availability of information should be identified.
Output
A list of identified risks
Approaches
Event-based
Identify strategic scenarios through a consideration of risk sources, and how they use or impact interested parties to reach those risk's desired objective.
Asset-based
Identify operational scenarios, which are detailed in terms of assets, threats and vulnerabilities.
7.2.2 Identifying risk owners
Action
Risks should be associated to risk owners
Output
List of risk owners with associated risks
Top management, the security committee, process owners, functional owners, department managers and asset owners can be the risk owners.
7.3 Analysing information security risks
7.3.1 General
Techniques
Qualitative
using a scale of qualifying attributes
e.g. high, medium, low
Quantitative
using a scale with numerical values
e.g. monetary cost, frequency or probability of occurrence
Semiquantitative
using qualitative scales with assigned values
Risk analysis should be targeted at those risks and controls that, if managed successfully, improve the likelihood of the organization achieving its objectives
7.3.2 Assessing potential consequences
Action
The consequences resulting from the failure to adequately preserve confidentiality, integrity or availability of information should be identified and assessed
Output
A list of potential consequences related to risk scenarios with their consequences related to assets or events, depending on the approach applied.
should be taken into consideration:
Estimation of the losses (time or data) due to the event as result of interrupting or disturbing operations
Estimation/perception of severity of the consequence (e.g. expressed in money)
Recovery costs
7.3.3 Assessing likelihood
Action
The likelihood of occurrence of possible or actual scenarios should be assessed and expressed using established likelihood criteria.
Output
A list of events or risk scenarios complemented by likelihoods that these occur
7.3.4 Determining the levels of risk
Action
The level of risk should be determined as a combination of the assessed likelihood and the assessed consequences for all relevant risk scenarios
Output
A list of risks with level values assigned
Combination of the assessed likelihood and the assessed consequences for all relevant risk scenarios
7.4 Evaluating the information security risks
7.4.1 Comparing the results of risk analysis with the risk criteria
Action
Level of risks should be compared against risk evaluation criteria, particularly risk acceptance criteria.
Output
A list of suggestions for decisions on additional actions regarding the management of risks.
To evaluate risks, organizations should compare the assessed risks with the risk criteria defined during the establishment of context.
7.4.2 Prioritizing the analysed risks for risk treatment
Action
The risks on the list should be prioritized for risk treatment, considering assessed levels of risks
Output
A list of prioritized risks with risk scenarios that lead to those risks
Risk evaluation uses the understanding of risk obtained by risk analysis to make proposals for deciding about the next step to take.
8. Information security risk treatment process
Process to modify risk
Risk treatment
8.1 General
The input of the information security risk treatment is based on the risk assessment process outcomes in the form of a prioritized set of risks to be treated, based on risk criteria.
The output of this process is a set of necessary information security controls that are to be deployed or enhanced in relation to one another, in accordance with the risk treatment plan (RTP)
8.2 Selecting appropriate information security risk treatment options
Risk treatment options should be chosen
Action
A list of prioritized risks with the selected risk treatment options.
Output
Options
Risk avoidance, by deciding not to start or continue with the activity that gives rise to the risk
Risk modification, by changing the likelihood of the occurrence of an event or a consequence or changing the severity of the consequence
Risk retention, by informed choice
Risk sharing, by splitting responsibilities with other parties, either internally or externally (e.g. sharing the consequences via insurance)
8.3 Determining all controls that are necessary to implement the information security risk treatment options
Determine all controls, from the chosen control sets as selected from an appropriate source, that are necessary for treating the risks based on the risk treatment options chosen, such as to modify, retain, avoid or share the risks.
Action
All necessary controls
Output
Control classification
preventive
detective
corrective
8.4 Comparing the controls determined with those in ISO/IEC 27001:2022, Annex A
Compare all necessary controls with those listed in ISO/IEC 27001:2022, Annex A.
Action
All controls applicable to the risk treatment
Output
The purpose of this is to act as a safety check to verify that no necessary controls have been omitted from the risk assessment.
8.5 Producing a Statement of Applicability
Produce a Statement of Applicability
Action
Statement of Applicability (SoA)
Output
SoA should contain at least:
a) the necessary controls
b) justification for their inclusion
c) whether they are implemented or not
d) justification for exclusions of controls
Controls cannot be added to the SOA independent of the risk assessment
Implementation statuses
implemented
partially implemented
not implemented
8.6 Information security risk treatment plan
8.6.1 Formulation of the RTP
Formulate risk treatment plan.
Action
Risk treatment plan (RTP)
Output
RTP is a plan to modify risk such that it meets the organization's risk acceptance criteria
The risk treatment plan actions should be ranked by priority in relation with the level of risk and urgency of treatment.
8.6.2 Approval by risk owners
Approval of risk treatment plan(s) by risk owners
Action
Approved risk treatment plan(s)
Output
The RTP should be approved by the risk owners once it is formulated.
Risk owners should also decide on the acceptance of residual information security risks.
8.6.3 Acceptance of the residual information security risks
Determine whether the residual risks are acceptable.
Action
Accepted residual risks
Output
In order to determine the residual risks, risk treatment plans should feed into the follow up assessment of residual likelihood and consequence.
9. Operation
9.1 Performing information security risk assessment process
The risk assessment process should be performed in accordance with Clause 7
Action
Evaluated risks
Output
9.2 Performing information security risk treatment process
The risk treatment process should be performed in accordance with Clause 8.
Action
Retained or accepted residual risks.
Output
10. Leveraging related ISMS processes
Input, Action, Trigger, Output, Implementation guidance
10.1 Context of the organization
10.2 Leadership and commitment
10.3 Communication and consultation
10.4 Documented information
10.5 Monitoring and review
10.6 Management review
10.7 Corrective action
10.8 Continual improvement
Annex A. Examples of techniques in support of the risk assessment process
A.1 Information security risk criteria
A.1.1 Criteria related to risk assessment
A.1.2 Risk acceptance criteria
A.2 Practical techniques
A.2.1 Information security risk components
A.2.2 Assets
A.2.3 Risk sources and desired end state
A.2.4 Event-based approach
A.2.5 Asset-based approach
A.2.6 Examples of scenarios applicable in both approaches
A.2.7 Monitoring risk-related events


CONTEXT ESTABLISHMENT
(Clause 6)
RISK ASSESSMENT
RISK IDENTIFICATION
(Clause 7.2)
RISK ANALYSIS
(Clause 7.3)
RISK EVALUATION
(Clause 7.4)
RISK DECISION POINT 1
Assessment satisfactory?
No
Yes
RISK TREATMENT
(Clause 8)
RISK DECISION POINT 2
Risk accepted?
No
Yes
DOCUMENTED INFORMATION
(RECORDING AND REPORTING)
(Clause 10.4)
COMMUNICATION AND CONSULTATION (Clause 10.3)
MONITORING AND REVIEW (Clause 10.5)

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**.

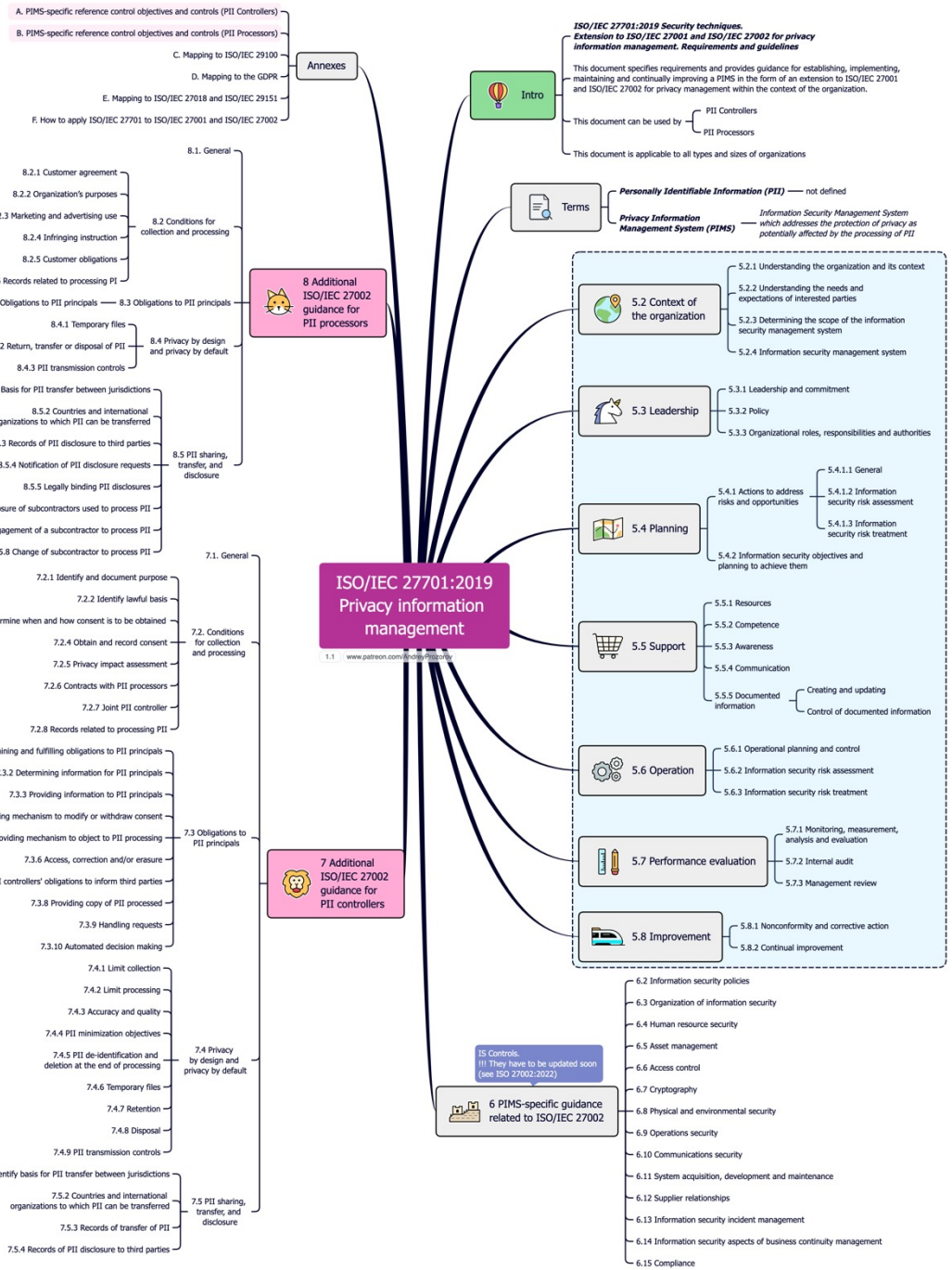
This document is applicable to all types and sizes of organizations, including public and private companies, government entities and not-for-profit organizations, which are **PII controllers and/or PII processors** processing PII within an ISMS.

Number of pages: 66

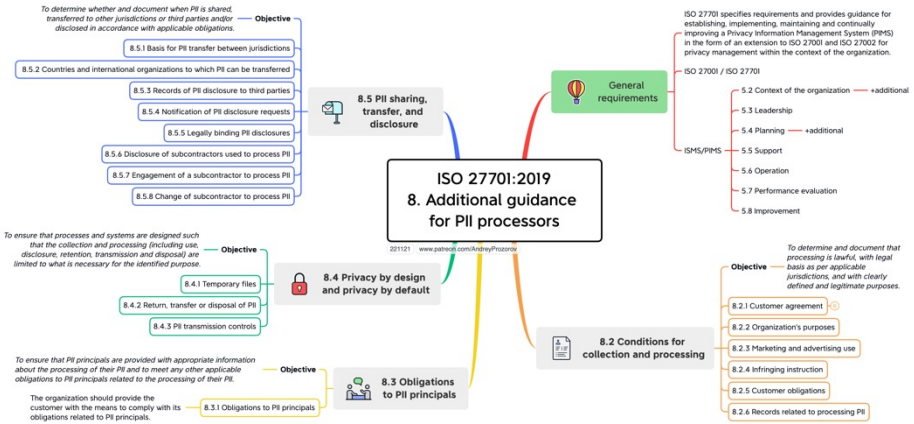
Contents

ISO/IEC 27701:2019(E)

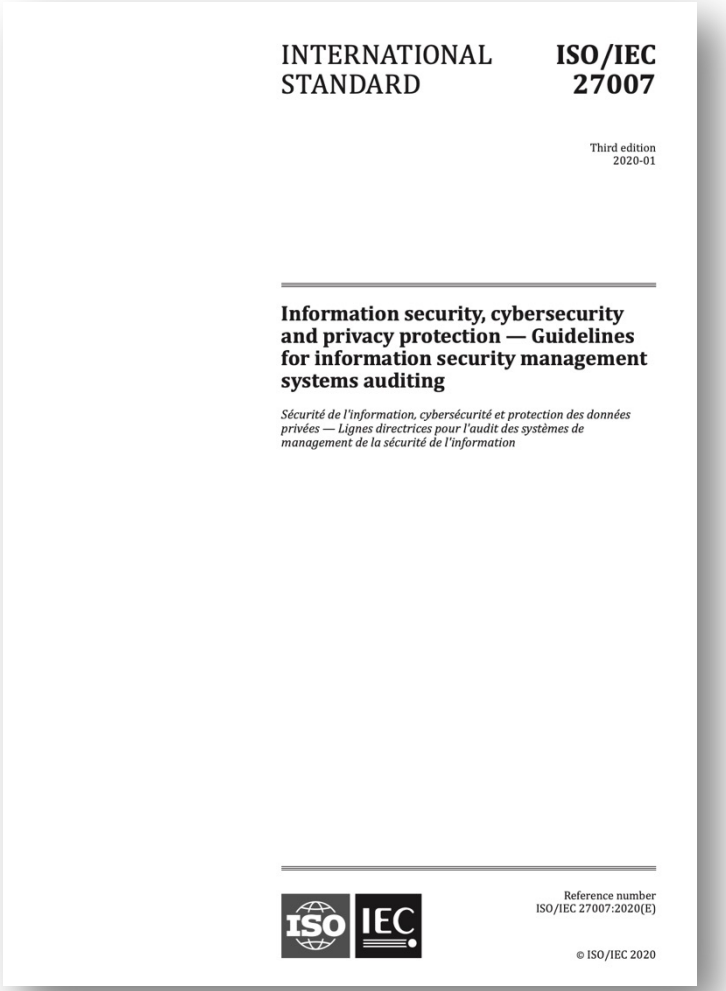
ISO/IEC 27701:2019(E)



Presented with xmind



ISO 27007 Guidelines for ISMS auditing


INTERNATIONAL STANDARD

ISO/IEC 27007

Third edition
2020-01

Information security, cybersecurity and privacy protection — Guidelines for information security management systems auditing

Sécurité de l'information, cybersécurité et protection des données privées — Lignes directrices pour l'audit des systèmes de management de la sécurité de l'information

Reference number
ISO/IEC 27007:2020(E)

© ISO/IEC 2020

This document provides guidance on managing an information security management system (ISMS) **audit programme**, on **conducting audits**, and on the competence of ISMS auditors, in addition to the guidance contained in **ISO 19011**.

This document is applicable to those needing to understand or conduct internal or external audits of an ISMS or to manage an ISMS audit programme.

Number of pages: 39

ISO 27008 Guidelines for the assessment of IS controls


TECHNICAL SPECIFICATION

ISO/IEC TS 27008

First edition 2019-01

Information technology — Security techniques — Guidelines for the assessment of information security controls

Technologies de l'information — Techniques de sécurité — Lignes directrices pour les auditeurs des contrôles de sécurité de l'information

ISO IEC

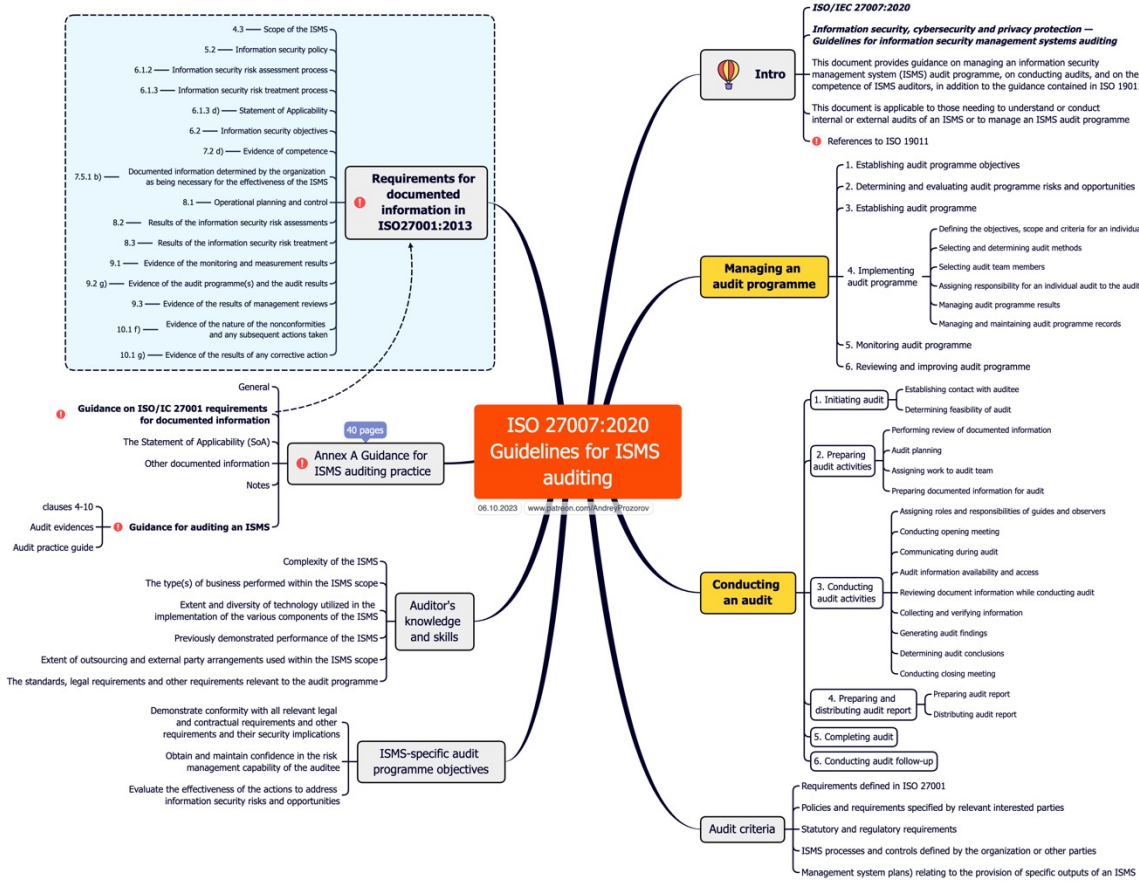
Reference number ISO/IEC TS 27008:2019(E)

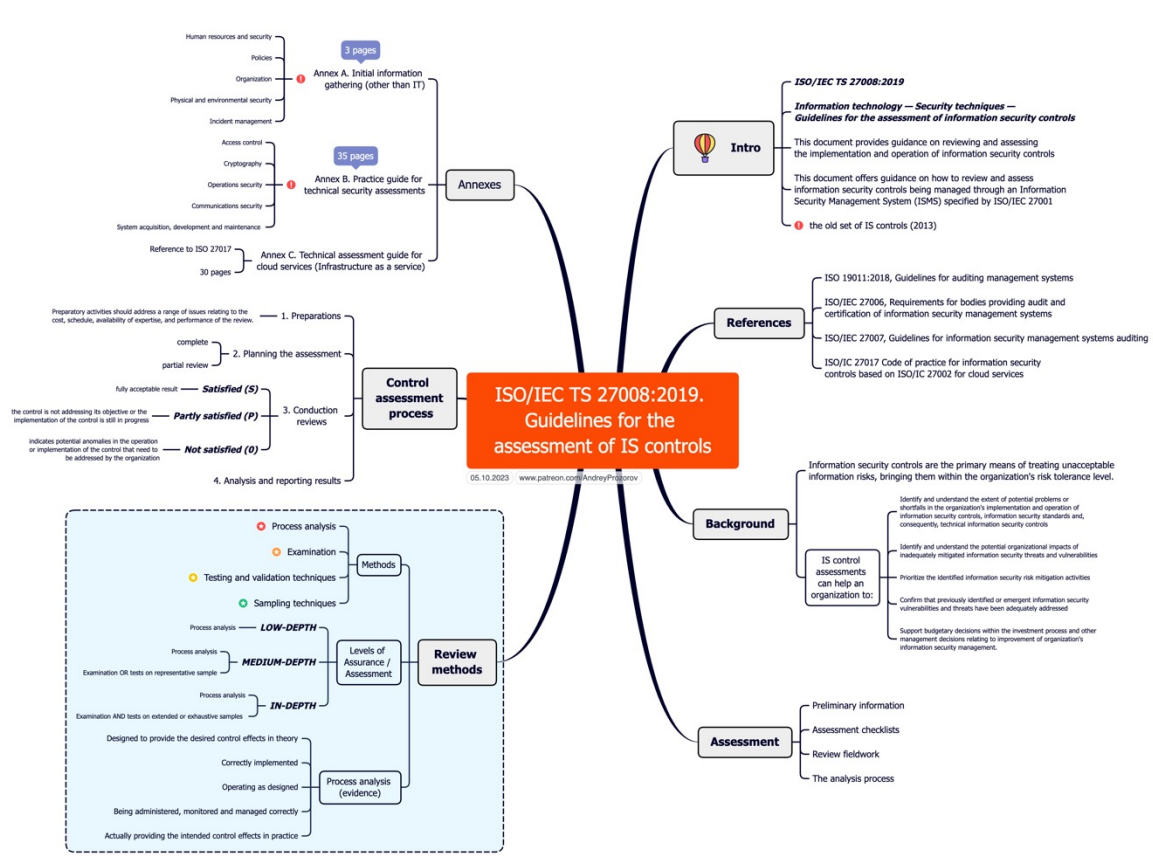
This document provides guidance on **reviewing and assessing the implementation and operation of information security controls**, including the technical assessment of information system controls, in compliance with an organization's established information security requirements including technical compliance against assessment criteria based on the information security requirements established by the organization.

This document offers guidance on **how to review and assess information security controls** being managed through an Information Security Management System specified by ISO/IEC 27001.

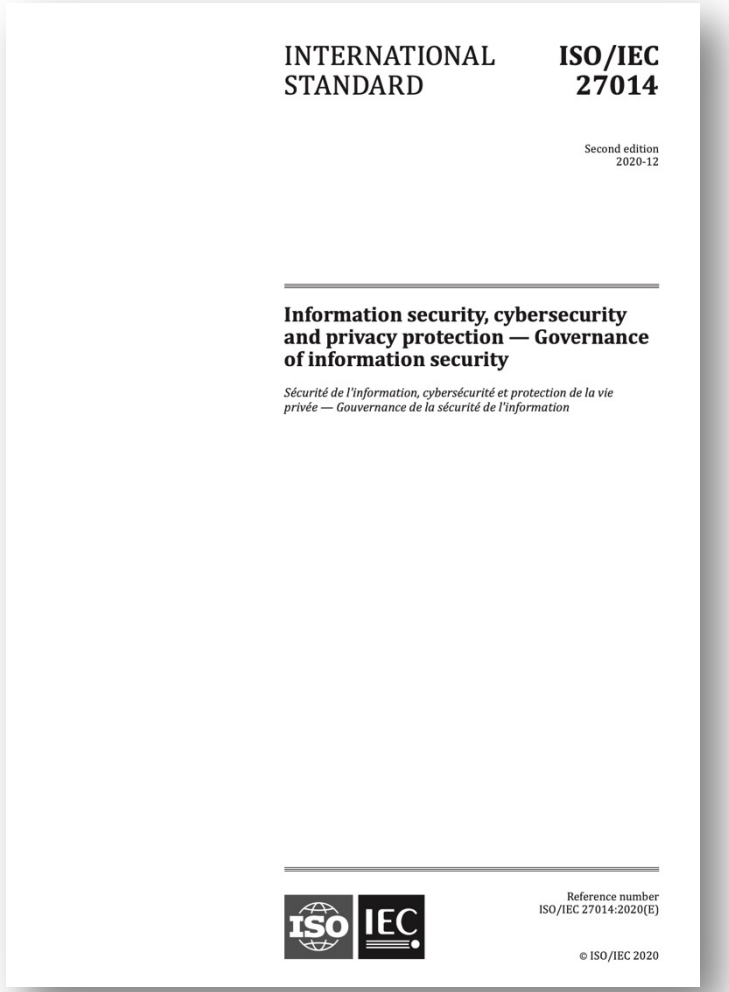
Number of pages: 91

For Audits and Assessments: 27007, 27008 and 19011





ISO 27014 IS Governance


INTERNATIONAL STANDARD

ISO/IEC 27014

Second edition
2020-12

Information security, cybersecurity and privacy protection — Governance of information security

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

Reference number
ISO/IEC 27014:2020(E)

© ISO/IEC 2020

This document provides guidance on concepts, objectives and processes for the **governance of information security**, by which organizations can evaluate, direct, monitor and communicate the information security-related processes within the organization.

The intended audience for this document is:

- governing body and top management;
- those who are responsible for evaluating, directing and monitoring an information security management system (ISMS) based on ISO/IEC 27001;
- those responsible for information security management that takes place outside the scope of an ISMS based on ISO/IEC 27001, but within the scope of governance.

Number of pages: 13

ISO 27014. Governance of information security

1.1 10.07.2023 www.patreon.com/AndreyProzorov

Intro

ISO/IEC 27014:2020. Information security, cybersecurity and privacy protection — Governance of information security

This document provides guidance on concepts, objectives and processes for the governance of information security, by which organizations can evaluate, direct, monitor and communicate the information security-related processes within the organization

Other related standard — ISO/IEC 38500:2015. Information technology — Governance of IT for the organization

Terms

- ***Entity*** — *Organization and other bodies or parties*
- ***Organization*** — *Part of an entity which runs and manages an ISMS*
- ***Governing body (GB)*** — *Person or group of people who are accountable for the performance and conformance of the entity*
- ***Top management (TM)*** — *Person or group of people who directs and controls an organization at the highest level*
  - *Note: Top management has the power to delegate authority and provide resources within the organization*
  - *Note: Top management reports to the governing body*

Governance

Governance of information security is the use of resources to ensure effective implementation of information security, and provides assurance that:

- directives concerning information security will be followed
- the governing body will receive reliable and relevant reporting about information security–related activities

Governance of information security is the means by which an organization's governing body provides overall direction and control of activities that affect the security of an organization's information

A governing body realises its governance objectives by

- providing direction by setting strategies and policies
- monitoring the performance of the organization
- evaluating proposals and plans developed by managers

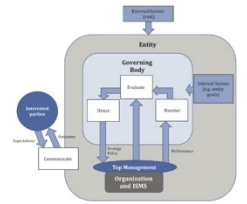
Governance activities within the scope of an ISMS

- ISO 27001, 4.1, 4.2, 4.3
- ISO 27001 Clauses 5, 6, 7, 8, 9, 10

Objectives

1. Establish integrated comprehensive entity-wide information security
2. Make decisions using a risk-based approach
3. Set the direction of acquisition
4. Ensure conformance with internal and external requirements
5. Foster a security-positive culture
6. Ensure the security performance meets current and future requirements of the entity

Governance Model



Processes

- Evaluate
- Direct
- Monitor
- Communicate

Organization and ISMS

GB should require the design of one or more ISMSs to support the entity's objectives

GB should also require the design of each ISMS to be consistent with overall entity policies and processes, including risk management

ISMS should adopt the same risk assessment process as that of GB, to enable clear communication of risk information

An ISMS can supply GB with management information relating to:

- Risks to the entity
- Effectiveness of the ISMS

GB should:

- Approve the creation of each ISMS
- Define the scope of each ISMS and for certification
- Provide direction to each ISMS including objectives, requirements, roles and resources
- Make decisions on acceptable levels of residual risk, or appropriate risk treatments
- Provide each ISMS with communications channels and the authority to use those channels to communicate the appropriate information to interested parties and all persons in the scope of that ISMs

4. Communicate

GB

- Report to external interested parties that the entity practices a level of information security commensurate with the nature of its activities and priorities
- Identify and prioritize regulatory obligations, interested parties' expectations, and the entity's requirements with regard to information security
- Advise top management of each ISMS of any matters that require its attention and decision
- Instruct relevant interested parties on detailed objectives to be taken in support of information security priorities
- Promote a positive information security culture
- Train and communicate with staff and other persons in scope of the ISMS on their responsibilities

3. Monitor

GB

- Receive the report on the effectiveness of the operation of each ISMS
- Evaluate these in the context of the priorities of the entity
- Communicate priorities to top management of each ISMS

TM

- Assess the effectiveness of information security management activities
- Ensure conformance with internal and external requirements
- Consider the changing entity, legal and regulatory environments, and any potential impact on information risk
- Select appropriate performance metrics and require reporting to take place in a timely manner from an organizational perspective;
- Provide feedback on information security performance results to the governing body
- Alert the governing body of new developments affecting information risks and information security

2. Direct

GB

- Set the overall strategic direction and objectives of the entity
- Define the entity's risk appetite
- Approve the information security strategy

TM

- Allocate adequate investment and resources
- Align organizational information security objectives with the entity's objectives
- Allocate roles and responsibilities for information security
- Establish an information security policy

1. Evaluate

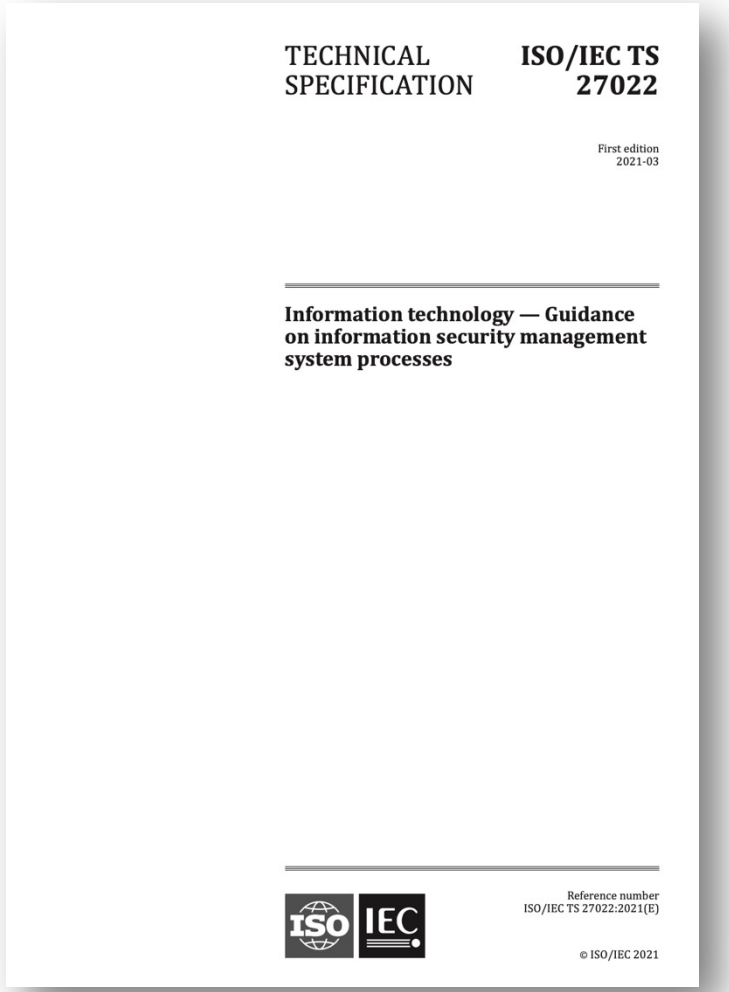
GB

- Ensure that initiatives take into account relevant risks and opportunities
- Respond to information security and ISMS measurements and reports by specifying and prioritising objectives in the context of each ISMS

TM

- Ensure that information security adequately supports and sustains the entity's objectives
- Submit new information security projects with significant impact to the governing body for approval

ISO 27022 Guidance on ISMS processes


TECHNICAL SPECIFICATION

ISO/IEC TS 27022

First edition 2021-03

Information technology — Guidance on information security management system processes

Reference number ISO/IEC TS 27022:2021(E)

© ISO/IEC 2021

This document defines a **process reference model (PRM)** for the domain of information security management, which is meeting the criteria defined in ISO/IEC 33004 for process reference models.

It is intended to guide users of ISO/IEC 27001 to:

- incorporate the process approach as described by ISO/IEC 27000:2018, 4.3, within the ISMS;
- be aligned to all the work done within other standards of the ISO/IEC 27000 family from the perspective of the operation of ISMS processes
- support users in the operation of an ISMS - this document is complementing the requirements-oriented perspective of ISO/IEC 27003 with an operational, process-oriented point of view.

Number of pages: 43

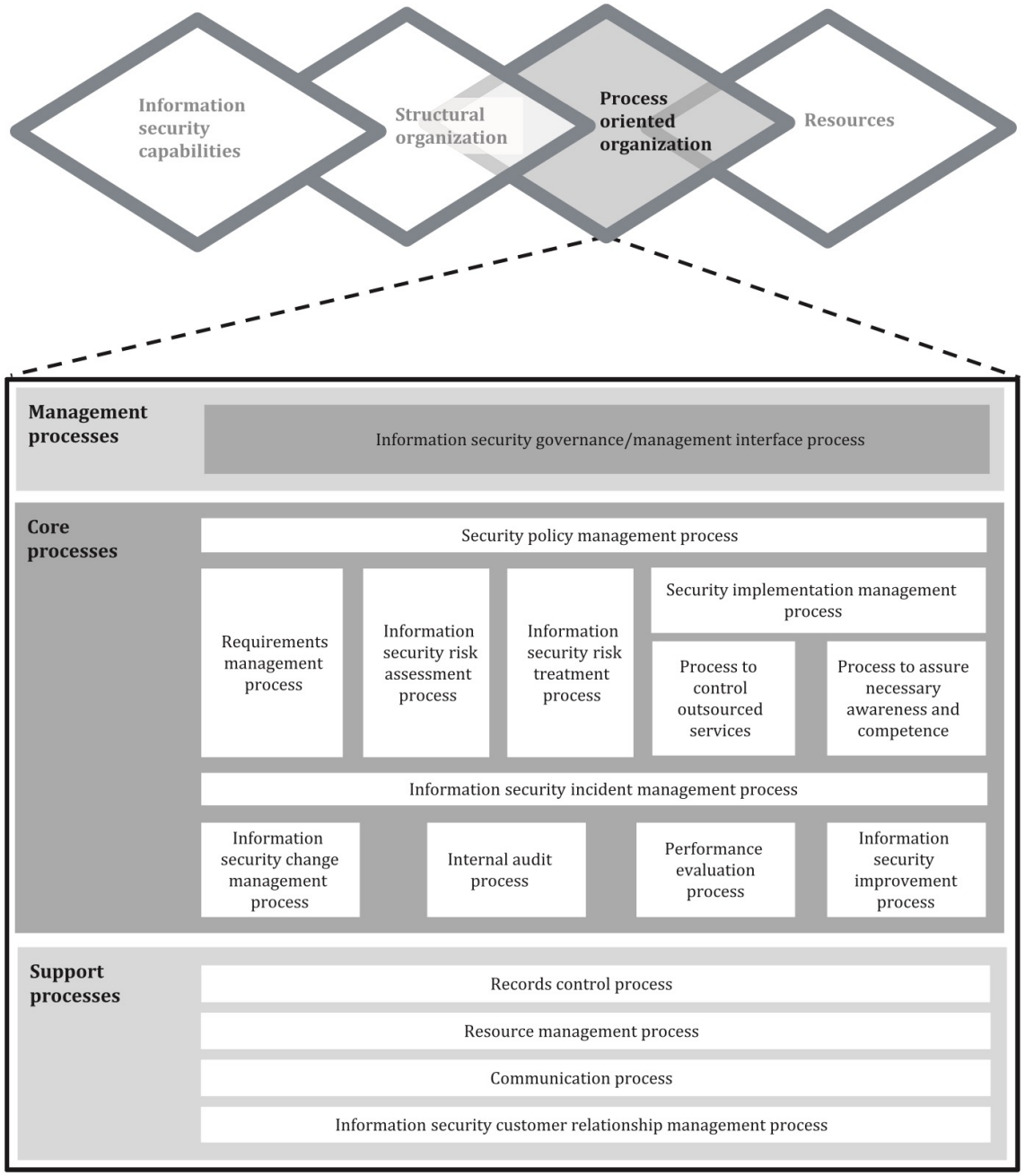


Figure 1 — ISMS process reference model

Each process of this PRM is described in terms of:

- process category
- brief description
- process flowchart
- objective/purposes
- input and results
- activities/functions
- references

- **ISO 27000: Overview and vocabulary**
- **ISO 27001: ISMS Requirements**
- **ISO 27002: IS controls**
- **ISO 27003: ISMS Guidance**
- ISO 27004: Monitoring and Measurement
- **ISO 27005: ISRM Guidance**
- ISO 27006: Requirements for bodies providing audit and certification of ISMS (and PIMS) (**set**)
- ISO 27007: Guidelines for ISMS auditing
- ISO 27008: Guidelines for the assessment of IS controls
- ~~ISO 27009: Sector-specific application of ISO 27001 [Withdrawn]~~
- ISO 27010: ISM for inter-sector and inter-organizational communications
- ISO 27011: IS controls for telecommunications organizations
- ISO 27012 – No standard
- ISO 27013: Guidance on the integrated implementation of ISO 27001 and ISO 20000-1
- ISO 27014: IS Governance
- ~~ISO 27015: ISM for financial services [Withdrawn]~~
- ISO 27016: Organizational economics
- ISO 27017: IS controls for cloud services
- ISO 27018: Code of practice for protection of PII in public clouds acting as PII processors
- ISO 27019: IS controls for the energy utility industry
- ISO 27020 – no ISMS standard
- ISO 27021: Competence requirements for ISMS professionals
- ISO 27022: Guidance on ISMS processes
- ~~ISO 27023: Mapping the revised editions (2005 and 2013) [withdrawn]~~
- ISO 27024: ISO 27001 in Governmental / Regulatory requirements [Under development]
- ISO 27026 and ISO 27027 – no ISMS standards
- ISO 27028 Guidance on ISO/IEC 27002 attributes [Under development]
- ISO 27029: Additional document for ISO/IEC 27002 and ISO and IEC standards [Under development]
- ISO 27030 – No standard
- ISO 27031: Guidelines for information and communication technology readiness for business continuity
- ISO 27032: Guidelines for Internet security
- ISO 27033: Network security (**set**)
- ISO 27034: Application security (**set**)
- ISO 27035: IS incident management (**set**)
- ISO 27036: Supplier relationships (**set**)
- ISO 27037: Guidelines for identification, collection, acquisition and preservation of digital evidence
- ISO 27038: Specification for digital redaction
- ISO 27039: IDPS
- ISO 27040: Storage security
- ISO 27041: Guidance on assuring suitability and adequacy of incident investigative method
- ISO 27042: Guidelines for the analysis and interpretation of digital evidence
- ISO 27043: Incident investigation principles and processes
- ISO 27071: Security recommendations for establishing trusted connections between devices and services
- ISO 27090: Guidance for addressing security threats and failures in AI systems [Under development]
- ISO 27091: Privacy protection (AI) [Under development]
- ISO 27099: Practices and policy framework (PKI)
- ISO 27100: Cybersecurity. Overview and concepts
- ISO 27102: Guidelines for cyber-insurance
- ISO 27103: Cybersecurity and ISO and IEC Standards
- ISO 27400: IoT security and privacy — Guidelines
- ISO 27550: Privacy engineering for system life cycle processes
- ISO 27555: Guidelines on PII deletion
- ISO 27556: User-centric privacy preferences management framework
- ISO 27557: Privacy risk management
- **ISO 27701: PIMS**
- ISO 27799: ISM in health

09.10.2023

For Beginners	For Advanced	For Experts
ISO 27000	ISO 27701	ISO 27004
ISO 27001	ISO 27035	ISO 27007
ISO 27002	ISO 27036	ISO 27008
ISO 27003	ISO 27100	ISO 27014
ISO 27005		ISO 27022
ISO 19011		Other (e.g., industry-specific)

Thanks, and good luck!

www.linkedin.com/in/andreyprozorov

www.patreon.com/AndreyProzorov

ISO Survey 2022: ISO 27001 certificates

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

15.09.2022

ISO 27001:2022. What has changed?

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

1.0, 25.10.2022

ISO 27005:2022 Overview

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

1.0, 28.10.2022

ISO 27001:2022. Implementation Approaches

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

1.0, 24.07.2023

ISO 27001 Introduction

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

1.0, 23.11.2022

ISO 27001:2022. How to implement an ISMS using the ISMS Implementation Toolkit

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

1.0, 06.08.2023

ISO 27001:2022. How to conduct an ISMS Gap Analysis

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

1.0, 15.05.2023

ISO 27001:2022. ISMS Scope

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

1.0, 19.07.2023

ISO 27001:2022 Tips and Tricks. How to accelerate the implementation

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

1.0, 01.06.2023

ISO 27001:2022. How to use ChatGPT for an ISMS implementation?

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

1.0, 25.05.2023

ISO 27001:2022. All about a Statement of Applicability (SoA)

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

1.0, 10.03.2023

ISO 27001:2022. How to prepare for a certification audit

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

1.2, 15.05.2023

My ISMS-related presentations - www.patreon.com/posts/quick-links-75788060

P.S. Have you seen my ISMS Implementation Toolkit?

lnkd.in/enzZdZ9