ISO 27001:2022. What has changed?

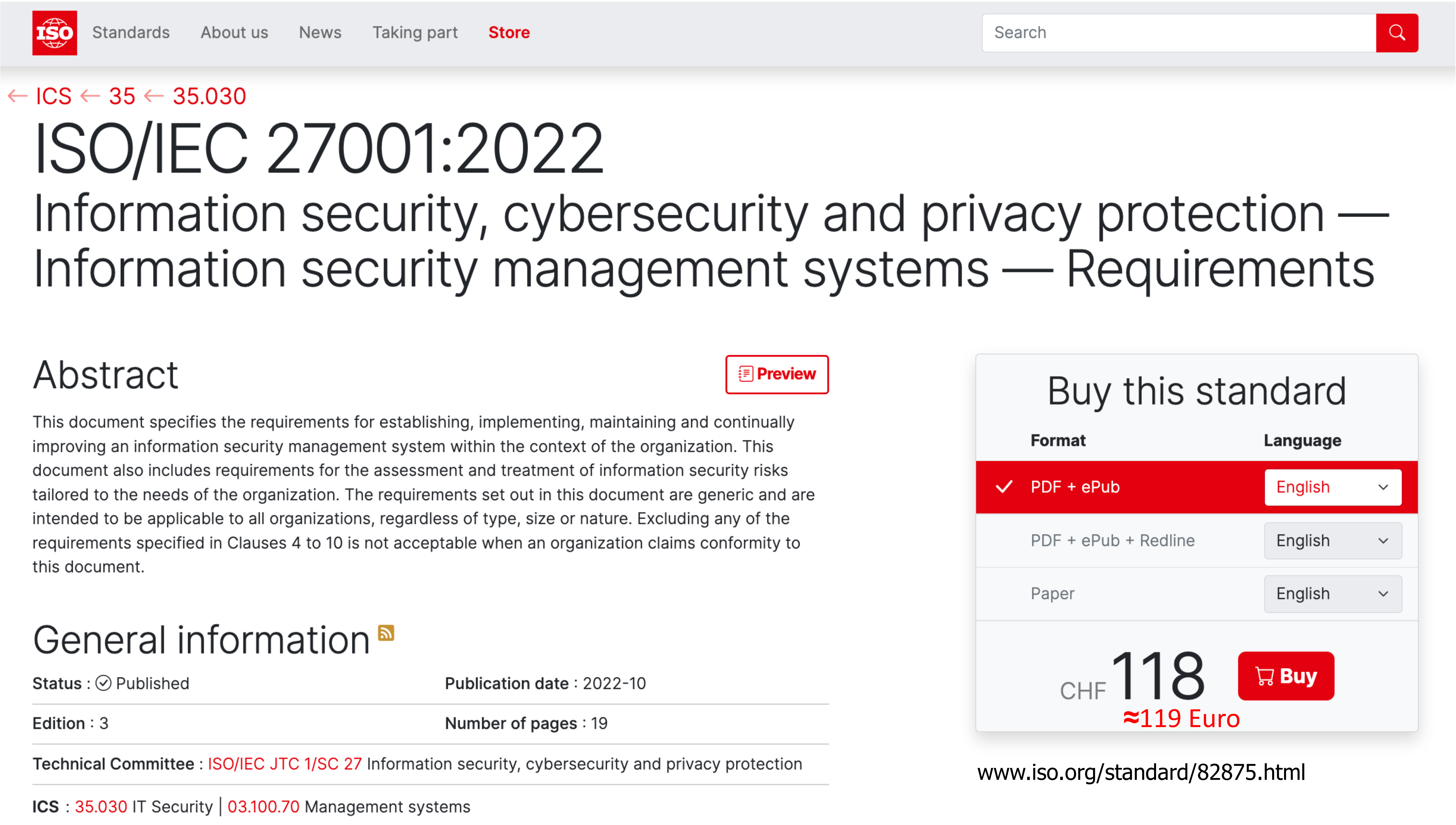
by Andrey Prozorov, CISM, CIPP/E, CDPSE, LA 27001

www.patreon.com/AndreyProzorov

1.0, 25.10.2022

Agenda

1. Purchasing
2. Life cycle
3. New Name
4. Abstract
5. Number of pages
6. New terminology databases
7. New relevant requirements, 4.2
8. More focus on processses, 4.4 ISMS
9. New requirements for 6.2 IS objectives
10. Planning for changes (NEW)
11. New requirements for 7.4 Communication
12. New requirements for 8.1 Planning
13. New requirements for 9.1 Monitoring
14. New structure of 9.2 and 9.3, and a new input for Management Review
15. New structure of 10 Improvement
16. NEW Annex A. IS Controls
17. IS Control list and Mapping
18. ISO 27002:2022. Example of Attributes
19. If you have the ISMS, you will need to do
20. Contacts



ISO/IEC 27001:2022

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

Abstract

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.

General information

Status : Published

Publication date : 2022-10

Edition : 3

Number of pages : 19

Technical Committee : ISO/IEC JTC 1/SC 27 Information security, cybersecurity and privacy protection

ICS : 35.030 IT Security | 03.100.70 Management systems

Buy this standard

Format	Language
✓ PDF + ePub	English
PDF + ePub + Redline	English
Paper	English

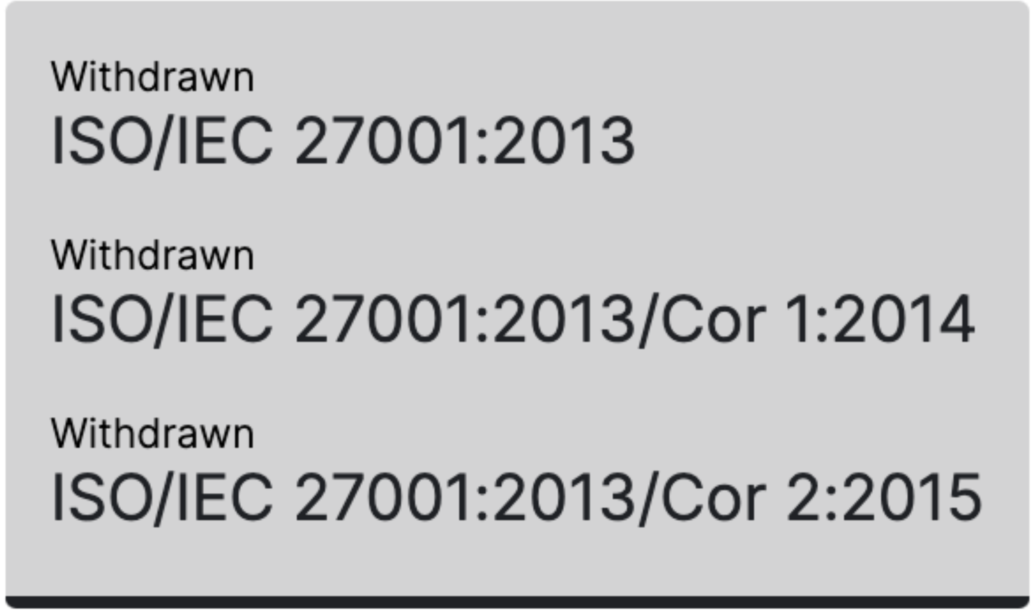
CHF 118

≈119 Euro

www.iso.org/standard/82875.html

Life cycle

Previously



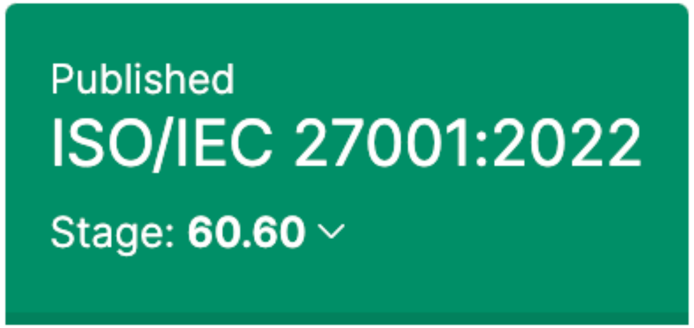
Withdrawn
ISO/IEC 27001:2013

Withdrawn
ISO/IEC 27001:2013/Cor 1:2014

Withdrawn
ISO/IEC 27001:2013/Cor 2:2015

→

Now



Published
ISO/IEC 27001:2022

Stage: **60.60**

1. New Name

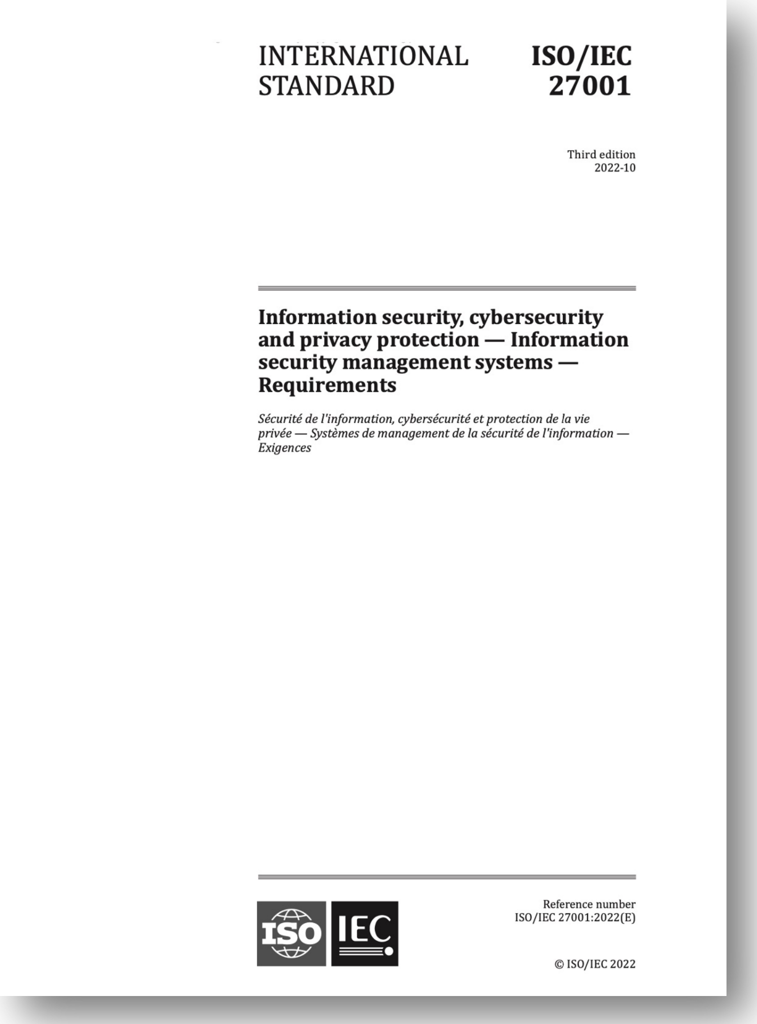
ISO/IEC 27001:2013

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

ISO/IEC 27001:2022

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

2. Abstract



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

Reference number
ISO/IEC 27001:2022(E)

© ISO/IEC 2022

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. [New 2022]

3. Number of pages

ISO/IEC 27001:2013	ISO/IEC 27001:2022
23	19

4. New terminology databases

ISO/IEC 27001:2013

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000 apply.

ISO/IEC 27001:2022

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000 apply.

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

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

5. New relevant requirements, 4.2

ISO/IEC 27001:2013

4.2 Understanding the needs and expectations of interested parties

The organization shall determine:

a) interested parties that are relevant to the information security management system; and

b) the requirements of these interested parties relevant to information security.

ISO/IEC 27001:2022

4.2 Understanding the needs and expectations of interested parties

The organization shall determine:

a) interested parties that are relevant to the information security management system;

b) the relevant requirements of these interested parties;

c) which of these requirements will be addressed through the information security management system.

6. More focus on processses, 4.4 ISMS

ISO/IEC 27001:2013

4.4 Information security management system

The organization shall establish, implement, maintain and continually improve an information security management system, in accordance with the requirements of this International Standard.

ISO/IEC 27001:2022

4.4 Information security management system

The organization shall establish, implement, maintain and continually improve an information security management system, **including the processes needed and their interactions**, in accordance with the requirements of this document.

7. New requirements for 6.2 IS objectives

ISO/IEC 27001:2013

6.2 Information security objectives and planning to achieve them

The organization shall establish information security objectives at relevant functions and levels.

The information security objectives shall:

a) be consistent with the information security policy;

b) be measurable (if practicable);

c) take into account applicable information security requirements, and results from risk assessment and risk treatment;

d) be communicated; and

e) be updated as appropriate.

ISO/IEC 27001:2022

6.2 Information security objectives and planning to achieve them

The organization shall establish information security objectives at relevant functions and levels.

The information security objectives shall:

a) be consistent with the information security policy;

b) be measurable (if practicable);

c) take into account applicable information security requirements, and results from risk assessment and risk treatment;

d) be monitored;

e) be communicated;

f) be updated as appropriate;

g) be available as documented information.

8. Planning for changes (NEW)

ISO/IEC 27001:2013

-

ISO/IEC 27001:2022

6.3 Planning of changes

When the organization determines the need for changes to the information security management system, the changes shall be carried out in a planned manner.

9. New requirements for 7.4 Communication

ISO/IEC 27001:2013

7.4 Communication

The organization shall determine the need for internal and external communications relevant to the information security management system including:

a) on what to communicate;

b) when to communicate;

c) with whom to communicate;

d) who shall communicate; and

e) the processes by which communication shall be effected.

ISO/IEC 27001:2022

7.4 Communication

The organization shall determine the need for internal and external communications relevant to the information security management system including:

a) on what to communicate;

b) when to communicate;

c) with whom to communicate;

d) how to communicate.

10. New requirements for 8.1 Planning

ISO/IEC 27001:2013

8.1 Operational planning and control

The organization shall plan, implement and control the processes needed to meet information security requirements, and to implement the actions determined in 6.1. The organization shall also implement plans to achieve information security objectives determined in 6.2.

The organization shall keep documented information to the extent necessary to have confidence that the processes have been carried out as planned.

The organization shall control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary.

The organization shall ensure that outsourced processes are determined and controlled.

ISO/IEC 27001:2022

8.1 Operational planning and control

The organization shall plan, implement and control the processes needed to meet requirements, and to implement the actions determined in Clause 6, by:

— establishing criteria for the processes;

— implementing control of the processes in accordance with the criteria.

Documented information shall be available to the extent necessary to have confidence that the processes have been carried out as planned.

The organization shall control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary.

The organization shall ensure that externally provided processes, products or services that are relevant to the information security management system are controlled.

11. New requirements for 9.1 Monitoring

ISO/IEC 27001:2013

9.1 Monitoring, measurement, analysis and evaluation

…

The organization shall retain appropriate documented information as evidence of the monitoring and measurement results.

ISO/IEC 27001:2022

9.1 Monitoring, measurement, analysis and evaluation

…

Documented information shall be available as evidence of the results.

The organization shall evaluate the information security performance and the effectiveness of the information security management system.

12. New structure of 9.2 and 9.3

ISO/IEC 27001:2013	ISO/IEC 27001:2022
9.2 Internal audit	**9.2 Internal audit**
9.3 Management review	9.2.1 General
	9.2.2 Internal audit programme
	9.3 Management review
	9.3.1 General
	9.3.2 Management review inputs
	9.3.3 Management review results

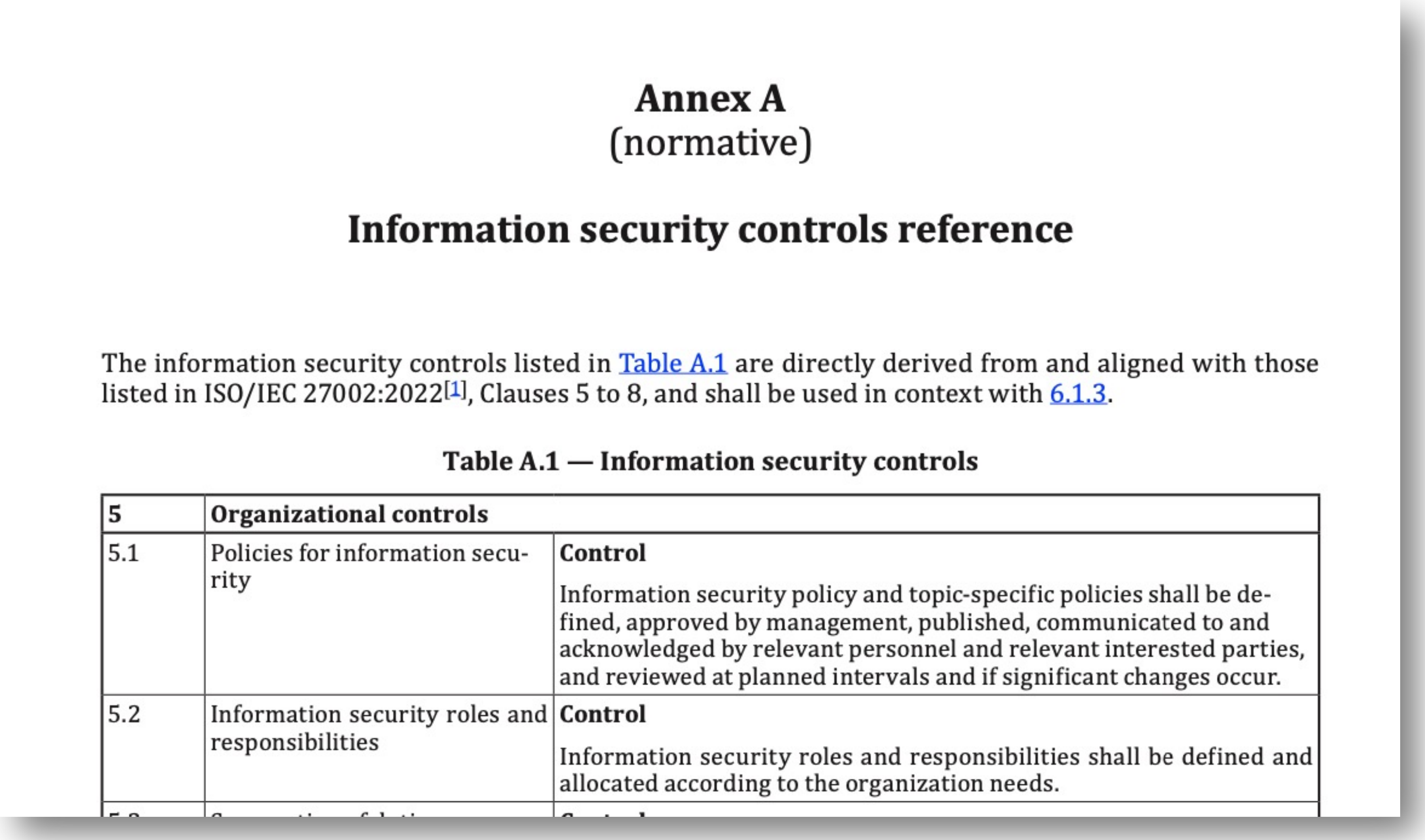
+new input for Management review:

c) changes in needs and expectations of interested parties that are relevant to the information security management system

13. New structure of 10 Improvement

ISO/IEC 27001:2013	ISO/IEC 27001:2022
10.1 Nonconformity and corrective action	**10.1 Continual improvement**
10.2 Continual improvement	**10.2 Nonconformity and corrective action**

14. NEW Annex A. IS Controls



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.

Information security controls reference (Annex A)

ISO/IEC 27001:2013

Total number of controls – 114

Domains:
A.5 Information security policies
A.6 Organisation of information security
A.7 Human resource security
A.8 Asset management
A.9 Access control
A.10 Cryptography
A.11 Physical and environmental security
A.12 Operations security
A.13 Communications security
A.14 System acquisition, development, and maintenance
A.15 Supplier relationships
A.16 Information security incident management
A.17 Information security aspects of business continuity management
A.18 Compliance

ISO/IEC 27001:2022

Total number of controls – 93, 11 new

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

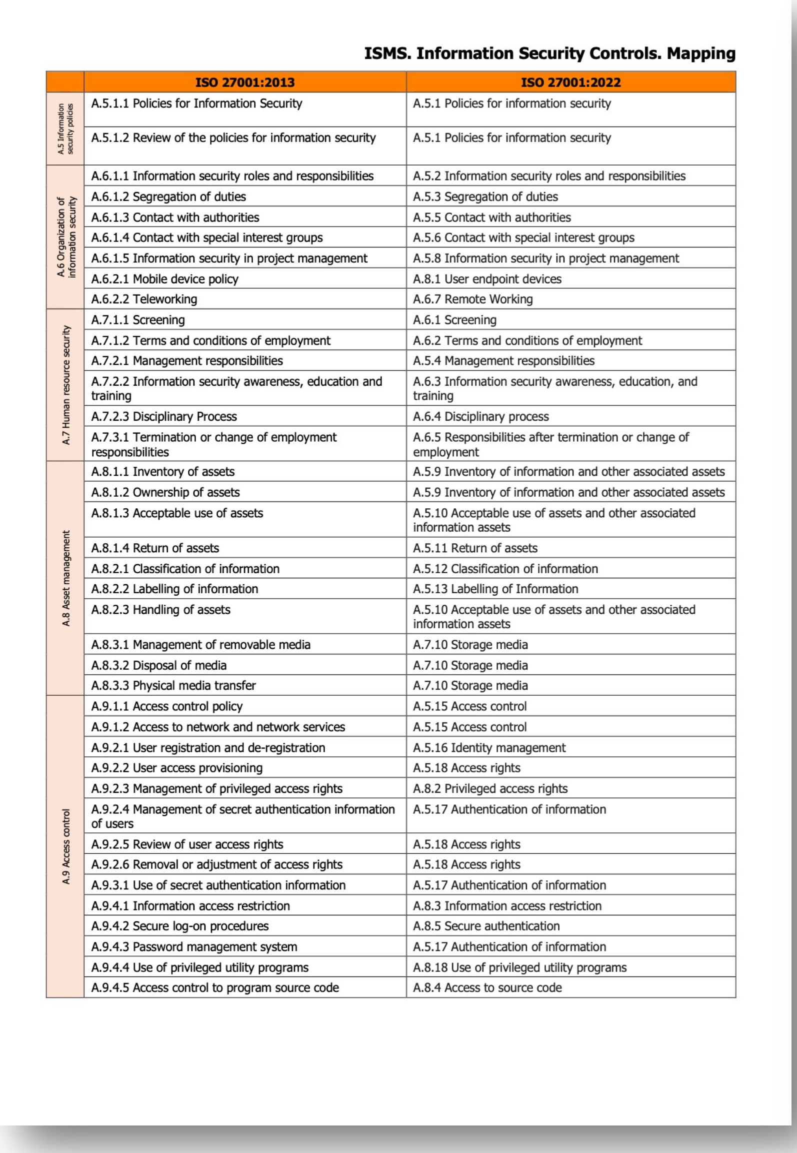
7. Physical controls

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

8. Technological controls

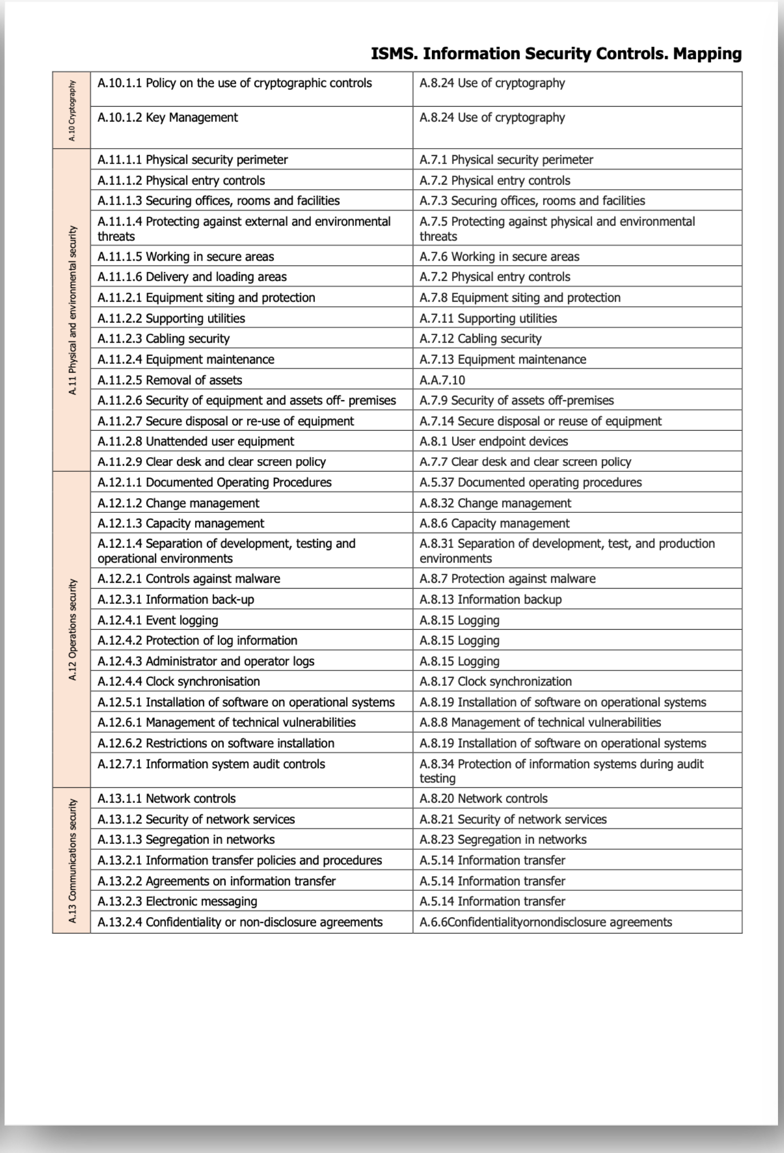
8.1. User endpoint devices
8.2. Privileged access rights
8.3. Information access restriction
8.4. Access to source code
8.5. Secure authentication
8.6. Capacity management
8.7. Protection against malware
8.8. Management of technical vulnerabilities
8.9. Configuration management
8.10. Information deletion
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



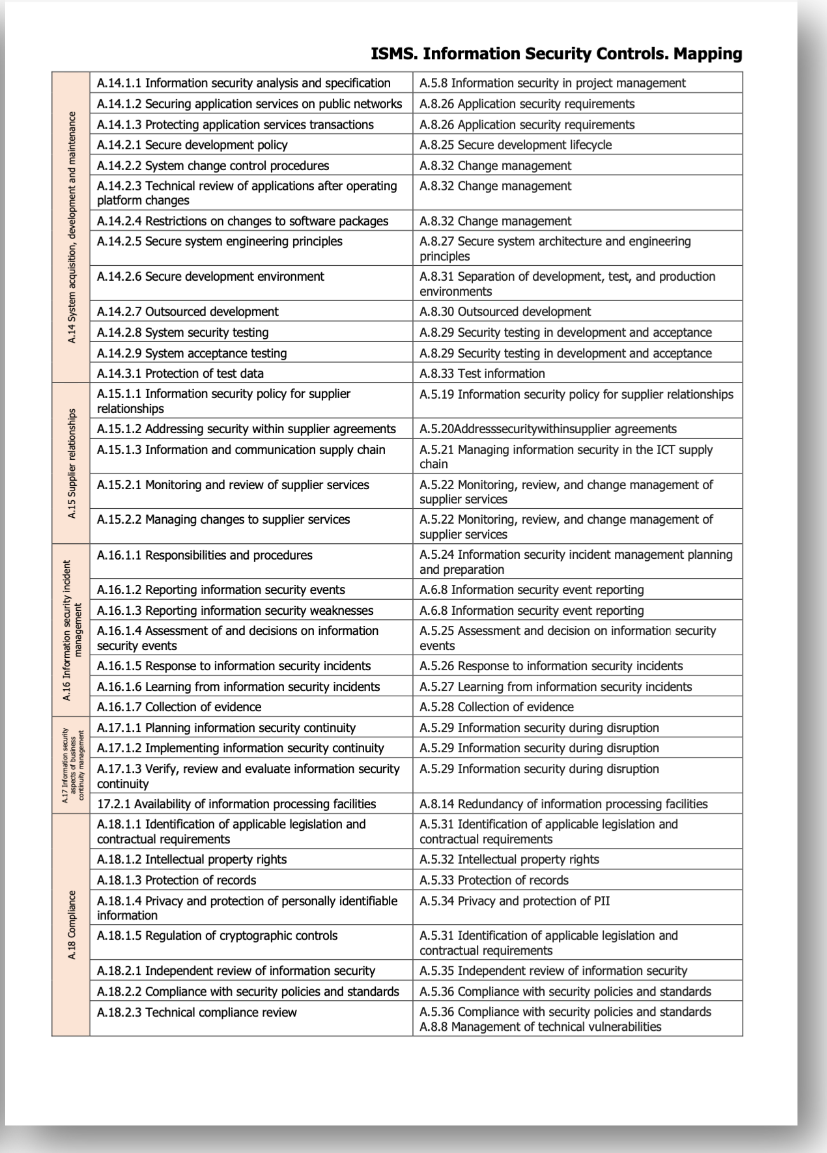
ISMS. Information Security Controls. Mapping

	ISO 27001:2013	ISO 27001:2022
A.5 Information security policies	A.5.1.1 Policies for Information Security	A.5.1 Policies for information security
	A.5.1.2 Review of the policies for information security	A.5.1 Policies for information security
A.6 Organization of information security	A.6.1.1 Information security roles and responsibilities	A.5.2 Information security roles and responsibilities
	A.6.1.2 Segregation of duties	A.5.3 Segregation of duties
	A.6.1.3 Contact with authorities	A.5.5 Contact with authorities
	A.6.1.4 Contact with special interest groups	A.5.6 Contact with special interest groups
	A.6.1.5 Information security in project management	A.5.8 Information security in project management
	A.6.2.1 Mobile device policy	A.8.1 User endpoint devices
	A.6.2.2 Teleworking	A.6.7 Remote Working
A.7 Human resource security	A.7.1.1 Screening	A.6.1 Screening
	A.7.1.2 Terms and conditions of employment	A.6.2 Terms and conditions of employment
	A.7.2.1 Management responsibilities	A.5.4 Management responsibilities
	A.7.2.2 Information security awareness, education and training	A.6.3 Information security awareness, education, and training
	A.7.2.3 Disciplinary Process	A.6.4 Disciplinary process
	A.7.3.1 Termination or change of employment responsibilities	A.6.5 Responsibilities after termination or change of employment
A.8 Asset management	A.8.1.1 Inventory of assets	A.5.9 Inventory of information and other associated assets
	A.8.1.2 Ownership of assets	A.5.9 Inventory of information and other associated assets
	A.8.1.3 Acceptable use of assets	A.5.10 Acceptable use of assets and other associated information assets
	A.8.1.4 Return of assets	A.5.11 Return of assets
	A.8.2.1 Classification of information	A.5.12 Classification of information
	A.8.2.2 Labelling of information	A.5.13 Labelling of Information
	A.8.2.3 Handling of assets	A.5.10 Acceptable use of assets and other associated information assets
	A.8.3.1 Management of removable media	A.7.10 Storage media
	A.8.3.2 Disposal of media	A.7.10 Storage media
	A.8.3.3 Physical media transfer	A.7.10 Storage media
A.9 Access control	A.9.1.1 Access control policy	A.5.15 Access control
	A.9.1.2 Access to network and network services	A.5.15 Access control
	A.9.2.1 User registration and de-registration	A.5.16 Identity management
	A.9.2.2 User access provisioning	A.5.18 Access rights
	A.9.2.3 Management of privileged access rights	A.8.2 Privileged access rights
	A.9.2.4 Management of secret authentication information of users	A.5.17 Authentication of information
	A.9.2.5 Review of user access rights	A.5.18 Access rights
	A.9.2.6 Removal or adjustment of access rights	A.5.18 Access rights
	A.9.3.1 Use of secret authentication information	A.5.17 Authentication of information
	A.9.4.1 Information access restriction	A.8.3 Information access restriction
	A.9.4.2 Secure log-on procedures	A.8.5 Secure authentication
	A.9.4.3 Password management system	A.5.17 Authentication of information
	A.9.4.4 Use of privileged utility programs	A.8.18 Use of privileged utility programs
	A.9.4.5 Access control to program source code	A.8.4 Access to source code



ISMS. Information Security Controls. Mapping

A.10 Cryptography	A.10.1.1 Policy on the use of cryptographic controls	A.8.24 Use of cryptography
	A.10.1.2 Key Management	A.8.24 Use of cryptography
A.11 Physical and environmental security	A.11.1.1 Physical security perimeter	A.7.1 Physical security perimeter
	A.11.1.2 Physical entry controls	A.7.2 Physical entry controls
	A.11.1.3 Securing offices, rooms and facilities	A.7.3 Securing offices, rooms and facilities
	A.11.1.4 Protecting against external and environmental threats	A.7.5 Protecting against physical and environmental threats
	A.11.1.5 Working in secure areas	A.7.6 Working in secure areas
	A.11.1.6 Delivery and loading areas	A.7.2 Physical entry controls
	A.11.2.1 Equipment siting and protection	A.7.8 Equipment siting and protection
	A.11.2.2 Supporting utilities	A.7.11 Supporting utilities
	A.11.2.3 Cabling security	A.7.12 Cabling security
	A.11.2.4 Equipment maintenance	A.7.13 Equipment maintenance
	A.11.2.5 Removal of assets	A.A.7.10
	A.11.2.6 Security of equipment and assets off- premises	A.7.9 Security of assets off-premises
	A.11.2.7 Secure disposal or re-use of equipment	A.7.14 Secure disposal or reuse of equipment
	A.11.2.8 Unattended user equipment	A.8.1 User endpoint devices
	A.11.2.9 Clear desk and clear screen policy	A.7.7 Clear desk and clear screen policy
A.12 Operations security	A.12.1.1 Documented Operating Procedures	A.5.37 Documented operating procedures
	A.12.1.2 Change management	A.8.32 Change management
	A.12.1.3 Capacity management	A.8.6 Capacity management
	A.12.1.4 Separation of development, testing and operational environments	A.8.31 Separation of development, test, and production environments
	A.12.2.1 Controls against malware	A.8.7 Protection against malware
	A.12.3.1 Information back-up	A.8.13 Information backup
	A.12.4.1 Event logging	A.8.15 Logging
	A.12.4.2 Protection of log information	A.8.15 Logging
	A.12.4.3 Administrator and operator logs	A.8.15 Logging
	A.12.4.4 Clock synchronisation	A.8.17 Clock synchronization
	A.12.5.1 Installation of software on operational systems	A.8.19 Installation of software on operational systems
	A.12.6.1 Management of technical vulnerabilities	A.8.8 Management of technical vulnerabilities
	A.12.6.2 Restrictions on software installation	A.8.19 Installation of software on operational systems
	A.12.7.1 Information system audit controls	A.8.34 Protection of information systems during audit testing
A.13 Communications security	A.13.1.1 Network controls	A.8.20 Network controls
	A.13.1.2 Security of network services	A.8.21 Security of network services
	A.13.1.3 Segregation in networks	A.8.23 Segregation in networks
	A.13.2.1 Information transfer policies and procedures	A.5.14 Information transfer
	A.13.2.2 Agreements on information transfer	A.5.14 Information transfer
	A.13.2.3 Electronic messaging	A.5.14 Information transfer
	A.13.2.4 Confidentiality or non-disclosure agreements	A.6.6Confidentialityornondisclosure agreements



ISMS. Information Security Controls. Mapping

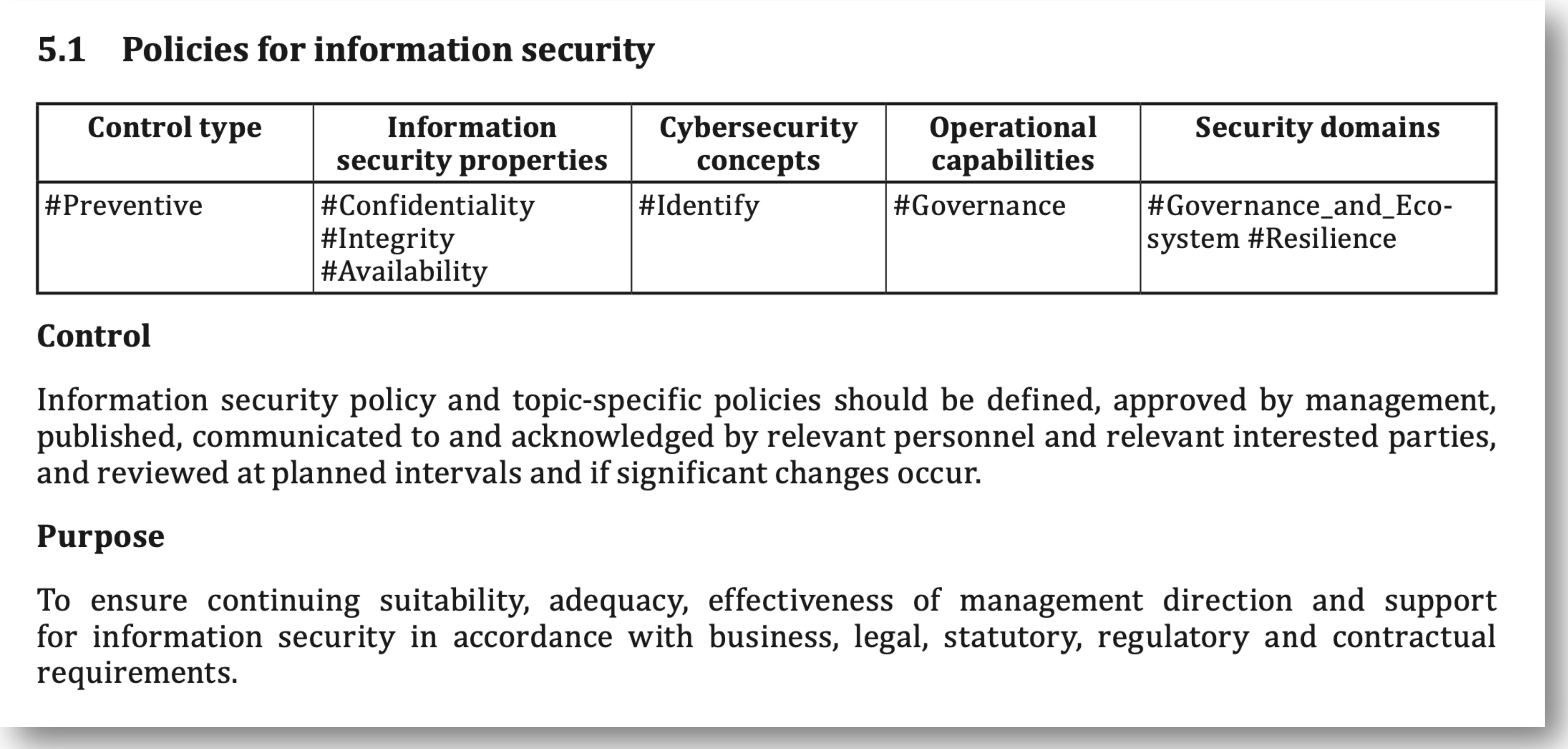
A.14 System acquisition, development and maintenance	A.14.1.1 Information security analysis and specification	A.5.8 Information security in project management
	A.14.1.2 Securing application services on public networks	A.8.26 Application security requirements
	A.14.1.3 Protecting application services transactions	A.8.26 Application security requirements
	A.14.2.1 Secure development policy	A.8.25 Secure development lifecycle
	A.14.2.2 System change control procedures	A.8.32 Change management
	A.14.2.3 Technical review of applications after operating platform changes	A.8.32 Change management
	A.14.2.4 Restrictions on changes to software packages	A.8.32 Change management
	A.14.2.5 Secure system engineering principles	A.8.27 Secure system architecture and engineering principles
	A.14.2.6 Secure development environment	A.8.31 Separation of development, test, and production environments
	A.14.2.7 Outsourced development	A.8.30 Outsourced development
	A.14.2.8 System security testing	A.8.29 Security testing in development and acceptance
	A.14.2.9 System acceptance testing	A.8.29 Security testing in development and acceptance
	A.14.3.1 Protection of test data	A.8.33 Test information
A.15 Supplier relationships	A.15.1.1 Information security policy for supplier relationships	A.5.19 Information security policy for supplier relationships
	A.15.1.2 Addressing security within supplier agreements	A.5.20Addresssecuritywithinsupplier agreements
	A.15.1.3 Information and communication supply chain	A.5.21 Managing information security in the ICT supply chain
	A.15.2.1 Monitoring and review of supplier services	A.5.22 Monitoring, review, and change management of supplier services
	A.15.2.2 Managing changes to supplier services	A.5.22 Monitoring, review, and change management of supplier services
A.16 Information security incident management	A.16.1.1 Responsibilities and procedures	A.5.24 Information security incident management planning and preparation
	A.16.1.2 Reporting information security events	A.6.8 Information security event reporting
	A.16.1.3 Reporting information security weaknesses	A.6.8 Information security event reporting
	A.16.1.4 Assessment of and decisions on information security events	A.5.25 Assessment and decision on information security events
	A.16.1.5 Response to information security incidents	A.5.26 Response to information security incidents
	A.16.1.6 Learning from information security incidents	A.5.27 Learning from information security incidents
	A.16.1.7 Collection of evidence	A.5.28 Collection of evidence
A.17 Information security aspects of business continuity management	A.17.1.1 Planning information security continuity	A.5.29 Information security during disruption
	A.17.1.2 Implementing information security continuity	A.5.29 Information security during disruption
	A.17.1.3 Verify, review and evaluate information security continuity	A.5.29 Information security during disruption
	17.2.1 Availability of information processing facilities	A.8.14 Redundancy of information processing facilities
A.18 Compliance	A.18.1.1 Identification of applicable legislation and contractual requirements	A.5.31 Identification of applicable legislation and contractual requirements
	A.18.1.2 Intellectual property rights	A.5.32 Intellectual property rights
	A.18.1.3 Protection of records	A.5.33 Protection of records
	A.18.1.4 Privacy and protection of personally identifiable information	A.5.34 Privacy and protection of PII
	A.18.1.5 Regulation of cryptographic controls	A.5.31 Identification of applicable legislation and contractual requirements
	A.18.2.1 Independent review of information security	A.5.35 Independent review of information security
	A.18.2.2 Compliance with security policies and standards	A.5.36 Compliance with security policies and standards
	A.18.2.3 Technical compliance review	A.5.36 Compliance with security policies and standards A.8.8 Management of technical vulnerabilities

NEW 2022:

A.5.7 Threat intelligence
A.5.23 Information security for use of cloud services
A.5.30 ICT readiness for business continuity
A.7.4 Physical security monitoring
A.8.9 Configuration management
A.8.10 Information deletion
A.8.11 Data masking
A.8.12 Data leakage prevention
A.8.16 Monitoring activities
A.8.23 Web filtering
A.8.28 Secure coding

www.patreon.com/posts/iso-27001-2013-73584456

ISO 27002:2022. Example of Attributes



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_Ecosystem #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.

If you have the ISMS, you will need to do:

1. Review the Risk Treatment Plan (RTP), align it with the new structure and numbering of controls.
2. Review and update the Statement of Applicability (SoA). I recommend using 2 spreadsheets (2013 and 2022) in the next 1-2 years.
3. Review and update the ISMS Management review procedure (inputs).
4. Review and update IS objectives and the Monitoring, measurement, analysis and evaluation procedure.
5. Review and update the ISMS Communication Plan.
6. Review and update other policies, standards and procedures (if necessary).

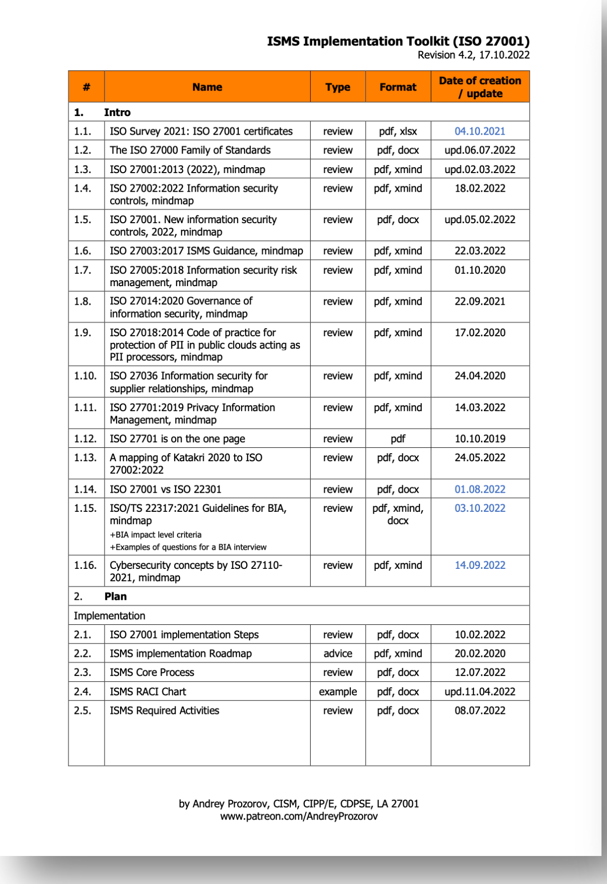
7. Review and update checklists and questionnaires used for audits (internal and external).
8. Evaluate and possibly adapt third-party security tools (e.g., GRC, SIEM, VM) to ensure the records you are using to demonstrate compliance support the new requirements.

Thanks!

www.linkedin.com/in/andreyprozorov

www.patreon.com/AndreyProzorov

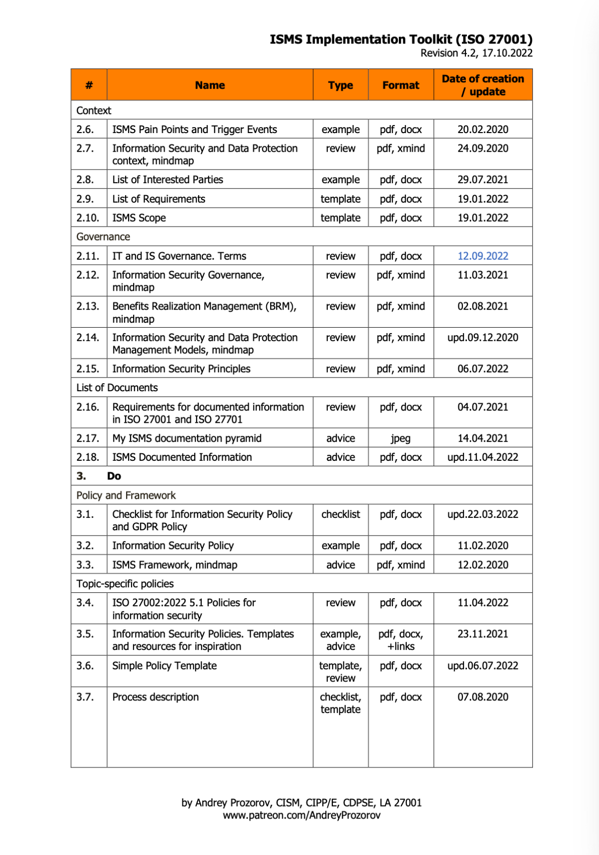
My ISMS Implementation Toolkit (ISO 27001)



ISMS Implementation Toolkit (ISO 27001)
Revision 4.2, 17.10.2022

#	Name	Type	Format	Date of creation / update
1.	**Intro**			
1.1.	ISO Survey 2021: ISO 27001 certificates	review	pdf, xlsx	04.10.2021
1.2.	The ISO 27000 Family of Standards	review	pdf, docx	upd.06.07.2022
1.3.	ISO 27001:2013 (2022), mindmap	review	pdf, xmind	upd.02.03.2022
1.4.	ISO 27002:2022 Information security controls, mindmap	review	pdf, xmind	18.02.2022
1.5.	ISO 27001. New information security controls, 2022, mindmap	review	pdf, docx	upd.05.02.2022
1.6.	ISO 27003:2017 ISMS Guidance, mindmap	review	pdf, xmind	22.03.2022
1.7.	ISO 27005:2018 Information security risk management, mindmap	review	pdf, xmind	01.10.2020
1.8.	ISO 27014:2020 Governance of information security, mindmap	review	pdf, xmind	22.09.2021
1.9.	ISO 27018:2014 Code of practice for protection of PII in public clouds acting as PII processors, mindmap	review	pdf, xmind	17.02.2020
1.10.	ISO 27036 Information security for supplier relationships, mindmap	review	pdf, xmind	24.04.2020
1.11.	ISO 27701:2019 Privacy Information Management, mindmap	review	pdf, xmind	14.03.2022
1.12.	ISO 27701 is on the one page	review	pdf	10.10.2019
1.13.	A mapping of Katakri 2020 to ISO 27002:2022	review	pdf, docx	24.05.2022
1.14.	ISO 27001 vs ISO 22301	review	pdf, docx	01.08.2022
1.15.	ISO/TS 22317:2021 Guidelines for BIA, mindmap +BIA impact level criteria +Examples of questions for a BIA interview	review	pdf, xmind, docx	03.10.2022
1.16.	Cybersecurity concepts by ISO 27110-2021, mindmap	review	pdf, xmind	14.09.2022
2.	**Plan**			
Implementation				
2.1.	ISO 27001 implementation Steps	review	pdf, docx	10.02.2022
2.2.	ISMS implementation Roadmap	advice	pdf, xmind	20.02.2020
2.3.	ISMS Core Process	review	pdf, docx	12.07.2022
2.4.	ISMS RACI Chart	example	pdf, docx	upd.11.04.2022
2.5.	ISMS Required Activities	review	pdf, docx	08.07.2022

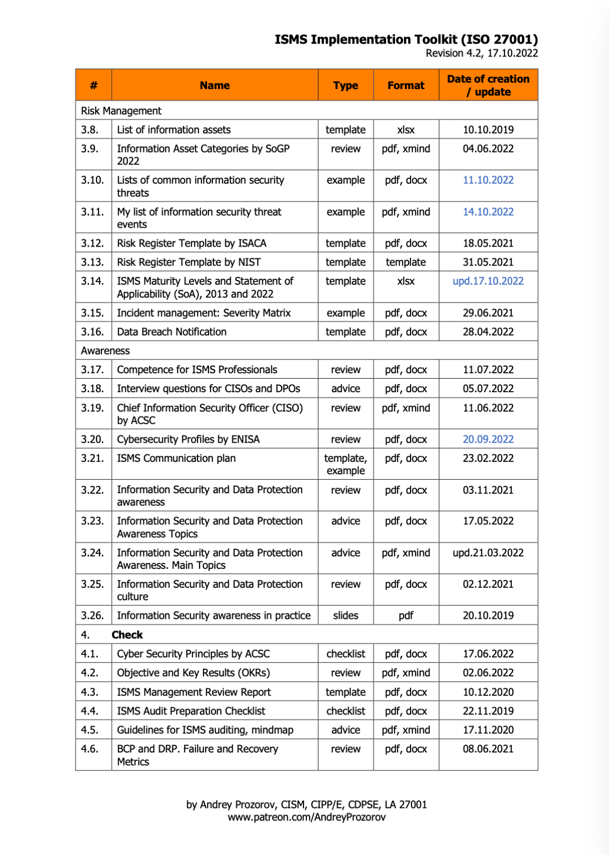
by Andrey Prozorov, CISM, CIPP/E, CDPSE, LA 27001
www.patreon.com/AndreyProzorov



ISMS Implementation Toolkit (ISO 27001)
Revision 4.2, 17.10.2022

#	Name	Type	Format	Date of creation / update
Context				
2.6.	ISMS Pain Points and Trigger Events	example	pdf, docx	20.02.2020
2.7.	Information Security and Data Protection context, mindmap	review	pdf, xmind	24.09.2020
2.8.	List of Interested Parties	example	pdf, docx	29.07.2021
2.9.	List of Requirements	template	pdf, docx	19.01.2022
2.10.	ISMS Scope	template	pdf, docx	19.01.2022
Governance				
2.11.	IT and IS Governance. Terms	review	pdf, docx	12.09.2022
2.12.	Information Security Governance, mindmap	review	pdf, xmind	11.03.2021
2.13.	Benefits Realization Management (BRM), mindmap	review	pdf, xmind	02.08.2021
2.14.	Information Security and Data Protection Management Models, mindmap	review	pdf, xmind	upd.09.12.2020
2.15.	Information Security Principles	review	pdf, xmind	06.07.2022
List of Documents				
2.16.	Requirements for documented information in ISO 27001 and ISO 27701	review	pdf, docx	04.07.2021
2.17.	My ISMS documentation pyramid	advice	jpeg	14.04.2021
2.18.	ISMS Documented Information	advice	pdf, docx	upd.11.04.2022
3.	**Do**			
Policy and Framework				
3.1.	Checklist for Information Security Policy and GDPR Policy	checklist	pdf, docx	upd.22.03.2022
3.2.	Information Security Policy	example	pdf, docx	11.02.2020
3.3.	ISMS Framework, mindmap	advice	pdf, xmind	12.02.2020
Topic-specific policies				
3.4.	ISO 27002:2022 5.1 Policies for information security	review	pdf, docx	11.04.2022
3.5.	Information Security Policies. Templates and resources for inspiration	example, advice	pdf, docx, +links	23.11.2021
3.6.	Simple Policy Template	template, review	pdf, docx	upd.06.07.2022
3.7.	Process description	checklist, template	pdf, docx	07.08.2020

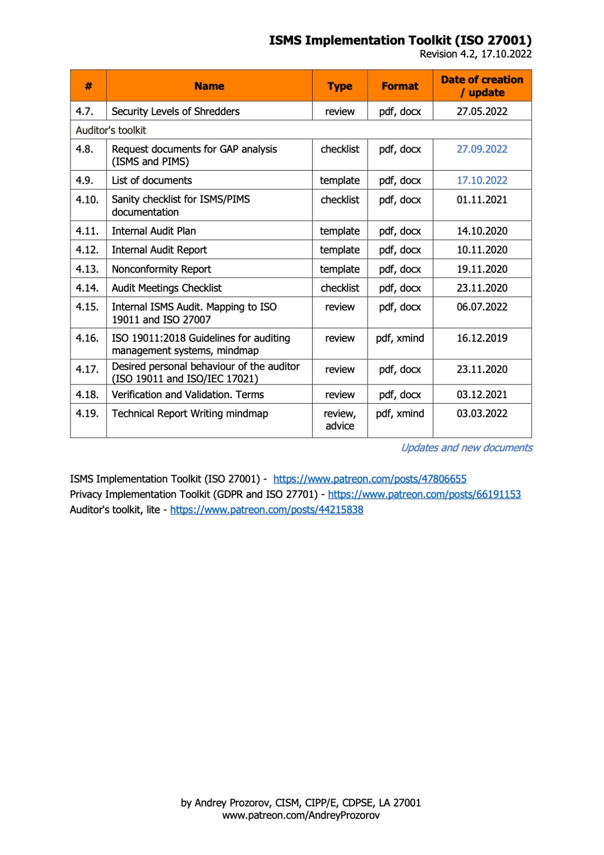
by Andrey Prozorov, CISM, CIPP/E, CDPSE, LA 27001
www.patreon.com/AndreyProzorov



ISMS Implementation Toolkit (ISO 27001)
Revision 4.2, 17.10.2022

#	Name	Type	Format	Date of creation / update
Risk Management				
3.8.	List of information assets	template	xlsx	10.10.2019
3.9.	Information Asset Categories by SoGP 2022	review	pdf, xmind	04.06.2022
3.10.	Lists of common information security threats	example	pdf, docx	11.10.2022
3.11.	My list of information security threat events	example	pdf, xmind	14.10.2022
3.12.	Risk Register Template by ISACA	template	pdf, docx	18.05.2021
3.13.	Risk Register Template by NIST	template	template	31.05.2021
3.14.	ISMS Maturity Levels and Statement of Applicability (SoA), 2013 and 2022	template	xlsx	upd.17.10.2022
3.15.	Incident management: Severity Matrix	example	pdf, docx	29.06.2021
3.16.	Data Breach Notification	template	pdf, docx	28.04.2022
Awareness				
3.17.	Competence for ISMS Professionals	review	pdf, docx	11.07.2022
3.18.	Interview questions for CISOs and DPOs	advice	pdf, docx	05.07.2022
3.19.	Chief Information Security Officer (CISO) by ACSC	review	pdf, xmind	11.06.2022
3.20.	Cybersecurity Profiles by ENISA	review	pdf, docx	20.09.2022
3.21.	ISMS Communication plan	template, example	pdf, docx	23.02.2022
3.22.	Information Security and Data Protection awareness	review	pdf, docx	03.11.2021
3.23.	Information Security and Data Protection Awareness Topics	advice	pdf, docx	17.05.2022
3.24.	Information Security and Data Protection Awareness. Main Topics	advice	pdf, xmind	upd.21.03.2022
3.25.	Information Security and Data Protection culture	review	pdf, docx	02.12.2021
3.26.	Information Security awareness in practice	slides	pdf	20.10.2019
4.	**Check**			
4.1.	Cyber Security Principles by ACSC	checklist	pdf, docx	17.06.2022
4.2.	Objective and Key Results (OKRs)	review	pdf, xmind	02.06.2022
4.3.	ISMS Management Review Report	template	pdf, docx	10.12.2020
4.4.	ISMS Audit Preparation Checklist	checklist	pdf, docx	22.11.2019
4.5.	Guidelines for ISMS auditing, mindmap	advice	pdf, xmind	17.11.2020
4.6.	BCP and DRP. Failure and Recovery Metrics	review	pdf, docx	08.06.2021

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



ISMS Implementation Toolkit (ISO 27001)
Revision 4.2, 17.10.2022

#	Name	Type	Format	Date of creation / update
4.7.	Security Levels of Shredders	review	pdf, docx	27.05.2022
Auditor's toolkit				
4.8.	Request documents for GAP analysis (ISMS and PIMS)	checklist	pdf, docx	27.09.2022
4.9.	List of documents	template	pdf, docx	17.10.2022
4.10.	Sanity checklist for ISMS/PIMS documentation	checklist	pdf, docx	01.11.2021
4.11.	Internal Audit Plan	template	pdf, docx	14.10.2020
4.12.	Internal Audit Report	template	pdf, docx	10.11.2020
4.13.	Nonconformity Report	template	pdf, docx	19.11.2020
4.14.	Audit Meetings Checklist	checklist	pdf, docx	23.11.2020
4.15.	Internal ISMS Audit. Mapping to ISO 19011 and ISO 27007	review	pdf, docx	06.07.2022
4.16.	ISO 19011:2018 Guidelines for auditing management systems, mindmap	review	pdf, xmind	16.12.2019
4.17.	Desired personal behaviour of the auditor (ISO 19011 and ISO/IEC 17021)	review	pdf, docx	23.11.2020
4.18.	Verification and Validation. Terms	review	pdf, docx	03.12.2021
4.19.	Technical Report Writing mindmap	review, advice	pdf, xmind	03.03.2022

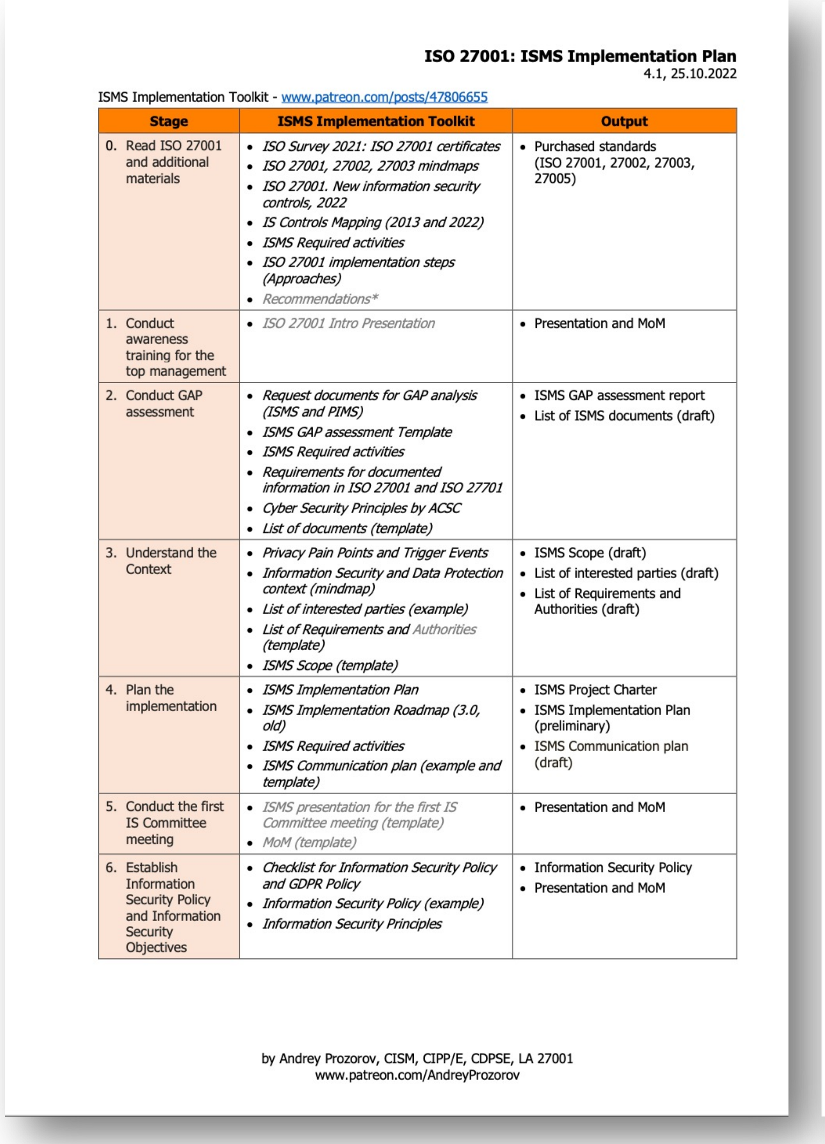
Updates and new documents

ISMS Implementation Toolkit (ISO 27001) - https://www.patreon.com/posts/47806655
Privacy Implementation Toolkit (GDPR and ISO 27701) - https://www.patreon.com/posts/66191153
Auditor's toolkit, lite - https://www.patreon.com/posts/44215838

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

www.patreon.com/posts/47806655

My ISMS Implemantation Plan

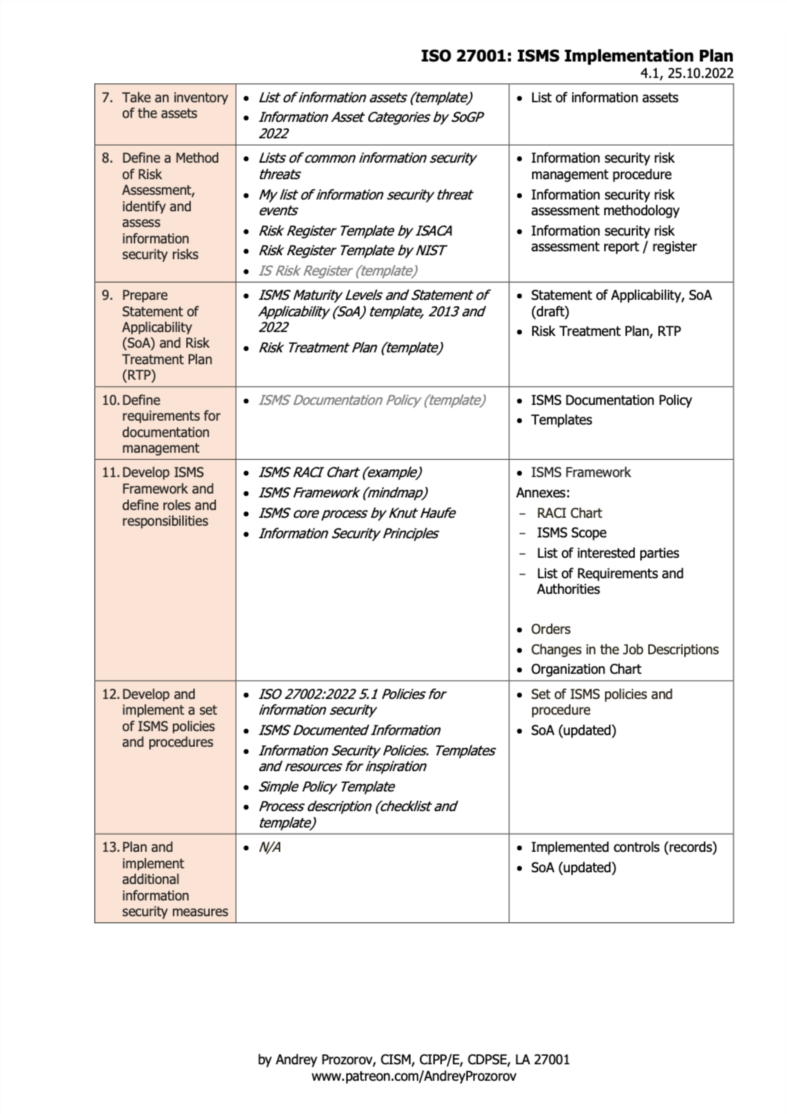


ISO 27001: ISMS Implementation Plan
4.1, 25.10.2022

ISMS Implementation Toolkit - www.patreon.com/posts/47806655

Stage	ISMS Implementation Toolkit	Output
0. Read ISO 27001 and additional materials	*ISO Survey 2021: ISO 27001 certificates* *ISO 27001, 27002, 27003 mindmaps* *ISO 27001. New information security controls, 2022* *IS Controls Mapping (2013 and 2022)* *ISMS Required activities* *ISO 27001 implementation steps (Approaches)* *Recommendations**	Purchased standards (ISO 27001, 27002, 27003, 27005)
1. Conduct awareness training for the top management	*ISO 27001 Intro Presentation*	Presentation and MoM
2. Conduct GAP assessment	*Request documents for GAP analysis (ISMS and PIMS)* *ISMS GAP assessment Template* *ISMS Required activities* *Requirements for documented information in ISO 27001 and ISO 27701* *Cyber Security Principles by ACSC* *List of documents (template)*	ISMS GAP assessment report List of ISMS documents (draft)
3. Understand the Context	*Privacy Pain Points and Trigger Events* *Information Security and Data Protection context (mindmap)* *List of interested parties (example)* *List of Requirements and Authorities (template)* *ISMS Scope (template)*	ISMS Scope (draft) List of interested parties (draft) List of Requirements and Authorities (draft)
4. Plan the implementation	*ISMS Implementation Plan* *ISMS Implementation Roadmap (3.0, old)* *ISMS Required activities* *ISMS Communication plan (example and template)*	ISMS Project Charter ISMS Implementation Plan (preliminary) ISMS Communication plan (draft)
5. Conduct the first IS Committee meeting	*ISMS presentation for the first IS Committee meeting (template)* *MoM (template)*	Presentation and MoM
6. Establish Information Security Policy and Information Security Objectives	*Checklist for Information Security Policy and GDPR Policy* *Information Security Policy (example)* *Information Security Principles*	Information Security Policy Presentation and MoM

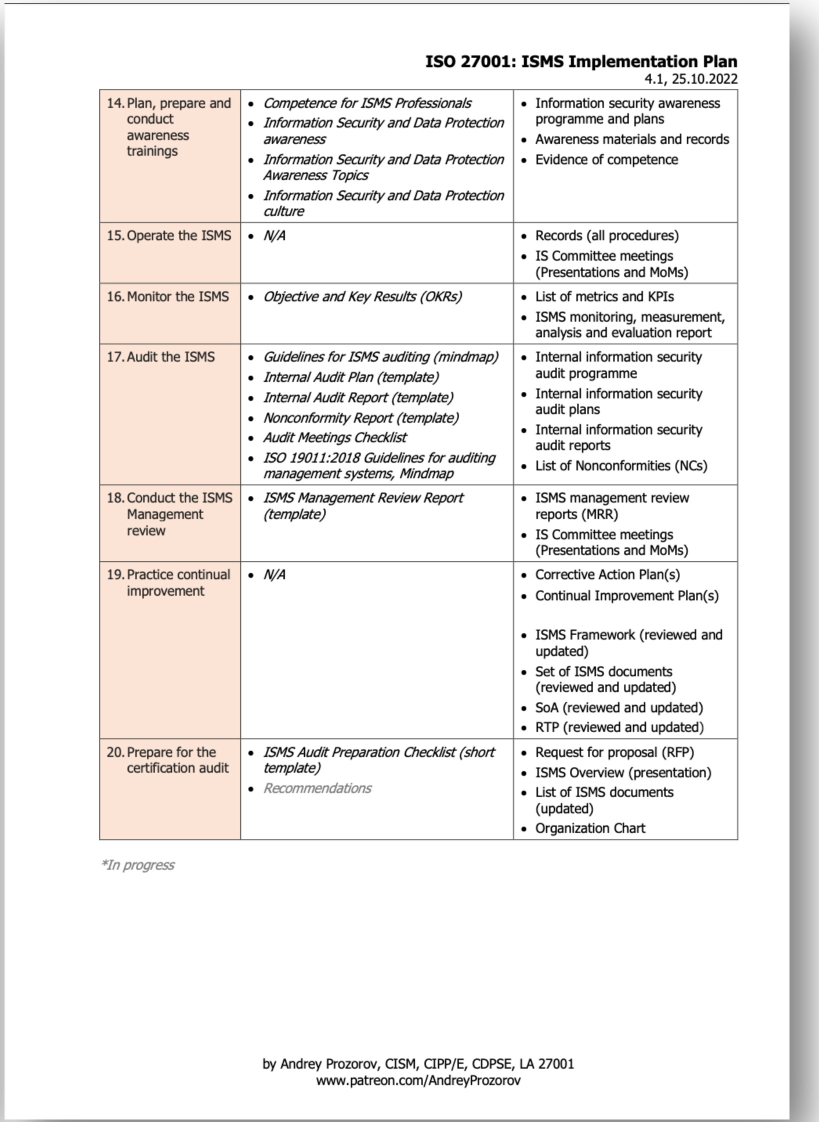
by Andrey Prozorov, CISM, CIPP/E, CDPSE, LA 27001
www.patreon.com/AndreyProzorov



ISO 27001: ISMS Implementation Plan
4.1, 25.10.2022

7. Take an inventory of the assets	*List of information assets (template)* *Information Asset Categories by SoGP 2022*	List of information assets
8. Define a Method of Risk Assessment, identify and assess information security risks	*Lists of common information security threats* *My list of information security threat events* *Risk Register Template by ISACA* *Risk Register Template by NIST* *IS Risk Register (template)*	Information security risk management procedure Information security risk assessment methodology Information security risk assessment report / register
9. Prepare Statement of Applicability (SoA) and Risk Treatment Plan (RTP)	*ISMS Maturity Levels and Statement of Applicability (SoA) template, 2013 and 2022* *Risk Treatment Plan (template)*	Statement of Applicability, SoA (draft) Risk Treatment Plan, RTP
10. Define requirements for documentation management	*ISMS Documentation Policy (template)*	ISMS Documentation Policy Templates
11. Develop ISMS Framework and define roles and responsibilities	*ISMS RACI Chart (example)* *ISMS Framework (mindmap)* *ISMS core process by Knut Haufe* *Information Security Principles*	ISMS Framework Annexes: – RACI Chart – ISMS Scope – List of interested parties – List of Requirements and Authorities Orders Changes in the Job Descriptions Organization Chart
12. Develop and implement a set of ISMS policies and procedures	*ISO 27002:2022 5.1 Policies for information security* *ISMS Documented Information* *Information Security Policies. Templates and resources for inspiration* *Simple Policy Template* *Process description (checklist and template)*	Set of ISMS policies and procedure SoA (updated)
13. Plan and implement additional information security measures	*N/A*	Implemented controls (records) SoA (updated)

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



ISO 27001: ISMS Implementation Plan
4.1, 25.10.2022

14. Plan, prepare and conduct awareness trainings	*Competence for ISMS Professionals* *Information Security and Data Protection awareness* *Information Security and Data Protection Awareness Topics* *Information Security and Data Protection culture*	Information security awareness programme and plans Awareness materials and records Evidence of competence
15. Operate the ISMS	*N/A*	Records (all procedures) IS Committee meetings (Presentations and MoMs)
16. Monitor the ISMS	*Objective and Key Results (OKRs)*	List of metrics and KPIs ISMS monitoring, measurement, analysis and evaluation report
17. Audit the ISMS	*Guidelines for ISMS auditing (mindmap)* *Internal Audit Plan (template)* *Internal Audit Report (template)* *Nonconformity Report (template)* *Audit Meetings Checklist* *ISO 19011:2018 Guidelines for auditing management systems, Mindmap*	Internal information security audit programme Internal information security audit plans Internal information security audit reports List of Nonconformities (NCs)
18. Conduct the ISMS Management review	*ISMS Management Review Report (template)*	ISMS management review reports (MRR) IS Committee meetings (Presentations and MoMs)
19. Practice continual improvement	*N/A*	Corrective Action Plan(s) Continual Improvement Plan(s) ISMS Framework (reviewed and updated) Set of ISMS documents (reviewed and updated) SoA (reviewed and updated) RTP (reviewed and updated)
20. Prepare for the certification audit	*ISMS Audit Preparation Checklist (short template)* *Recommendations*	Request for proposal (RFP) ISMS Overview (presentation) List of ISMS documents (updated) Organization Chart

**In progress*

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