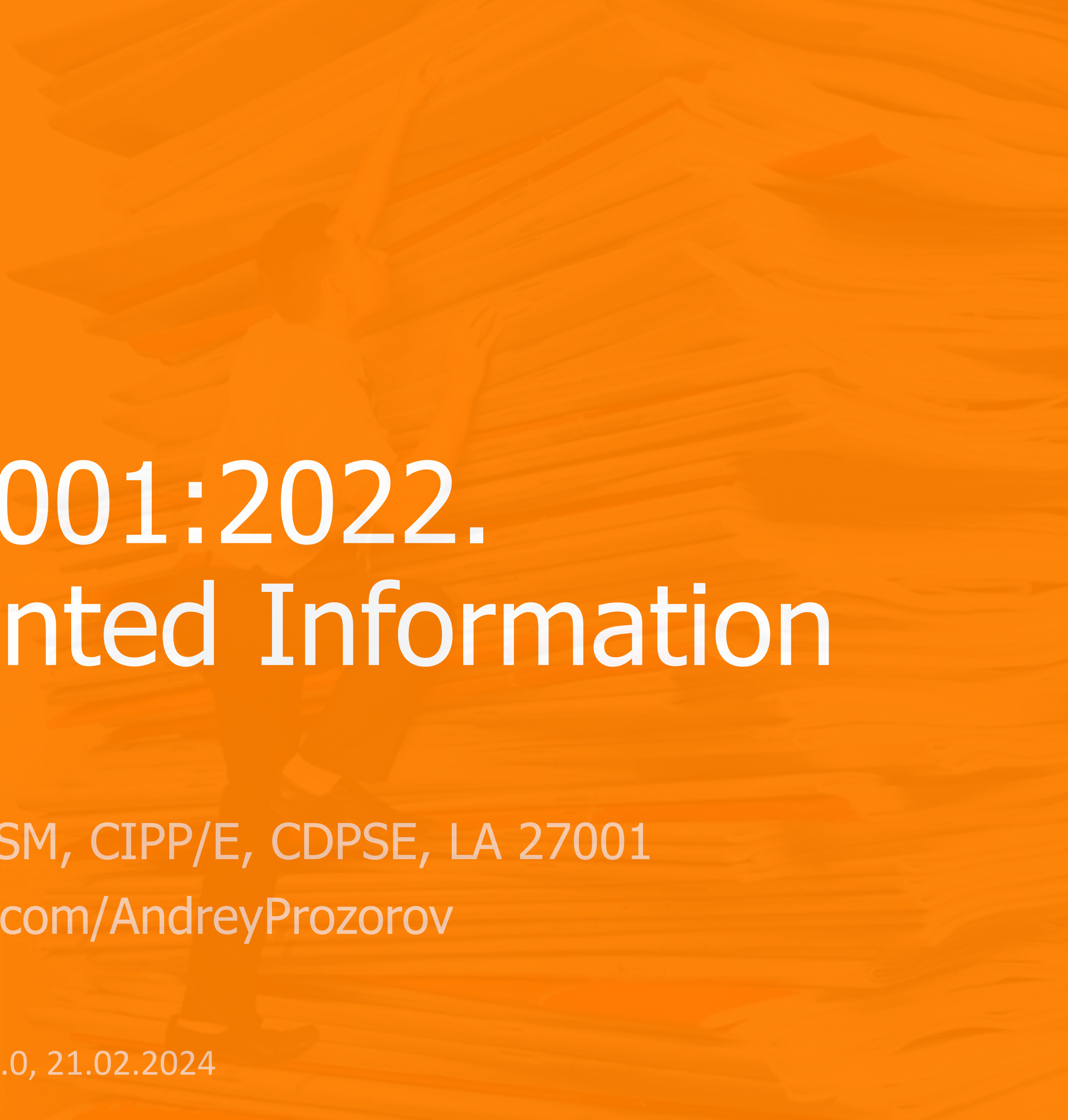


ISO 27001:2022. ISMS Documented Information

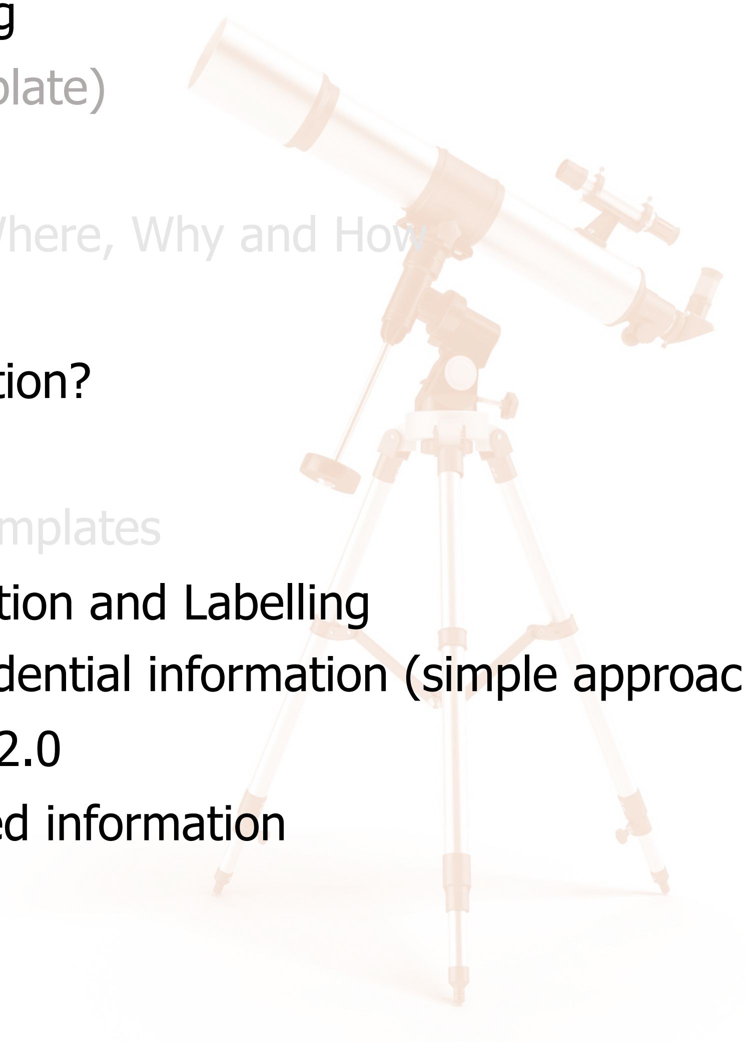
by Andrey Prozorov, CISM, CIPP/E, CDPSE, LA 27001

www.patreon.com/AndreyProzorov

lite 1.0, 21.02.2024

Agenda

1. Requirements and Recommendations
2. Documented Information (the term)
3. Required (mandatory) documented information
4. ISMS Documentation Pyramid
5. IS Policy
6. Topics mentioned in A.5.1
7. Operational procedures (A.5.37)
8. An extended list of ISMS documents
9. The shortest list of ISMS documents and some comments
10. ISMS Documents and Interested parties (example)
11. Creating and updating
12. Policy structure (template)
13. Content of policies
14. Who, What, When, Where, Why and How
15. Verbal forms
16. Where to find inspiration?
17. TOP5 ISMS toolkits
18. Examples of policy templates
19. Information classification and Labelling
20. Classification of confidential information (simple approach)
21. Traffic Light Protocol 2.0
22. Control of documented information
23. Sanity checklist



Requirements

ISO 27001 ISMS Requirements

- **7.5 Documented information**
  - 7.5.1 General
  - 7.5.2 Creating and updating
  - 7.5.3 Control of documented information
- **5.2 Policy**
- and other clauses (see further)

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

Recommendations

ISO 27002 IS Controls

- **5.1 Policies for information security**
- 5.12 Classification of information
- 5.13 Labelling of information
- 5.33 Protection of records
- **5.37 Documented operating procedures**

ISO 27003 ISMS Guidance

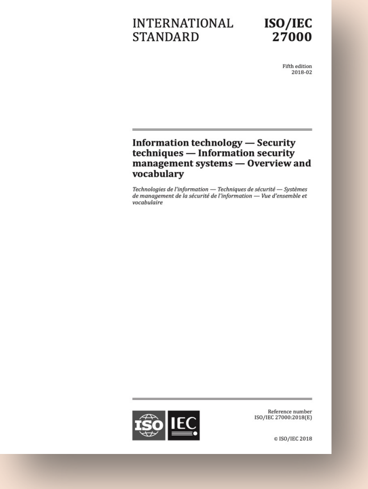
ISO 27007 Guidelines for ISMS auditing

ISO 27008 Guidelines for the assessment of information security controls

Information and documentation. Management systems for records:

- ISO 30301 Requirements
- ISO 30302 Guidelines for implementation

The term
(ISO 27000:2018)



INTERNATIONAL STANDARD

ISO/IEC 27000

Fifth edition
2018-02

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

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

Reference number
ISO/IEC 27000:2018(E)

© ISO/IEC 2018

***Documented information**: information required to be controlled and maintained by an organization and the medium on which it is contained*

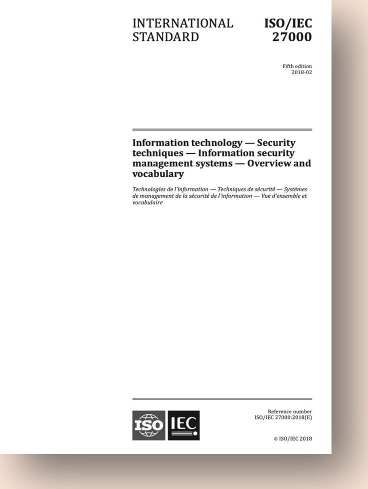
Documented information can be in any format and media and from any source.

Documented information can refer to:

- the management system, including related processes
- information created in order for the organization to operate (documentation)
- evidence of results achieved (records)

The term

(ISO 27000:2018)



INTERNATIONAL STANDARD

ISO/IEC 27000

Fifth edition
2018-02

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

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

Reference number
ISO/IEC 27000:2018(E)

© ISO/IEC 2018

***Documented information**: information required to be controlled and maintained by an organization and the medium on which it is contained*

Documented information can be in any format and media and from any source.

Documented information can refer to:

- the management system, including related processes
- information created in order for the organization to operate (documentation)
- evidence of results achieved (records)

*ISO 27007: The phrase "documented information as evidence of ..." implies the former term "**record**".*

Documented Information. General (ISO 27001:2022)

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

7.5.1 General

The organization’s ISMS shall include:

a) documented information **required** by this document; and

b) documented information **determined** by the organization **as being necessary** for the effectiveness of the ISMS.

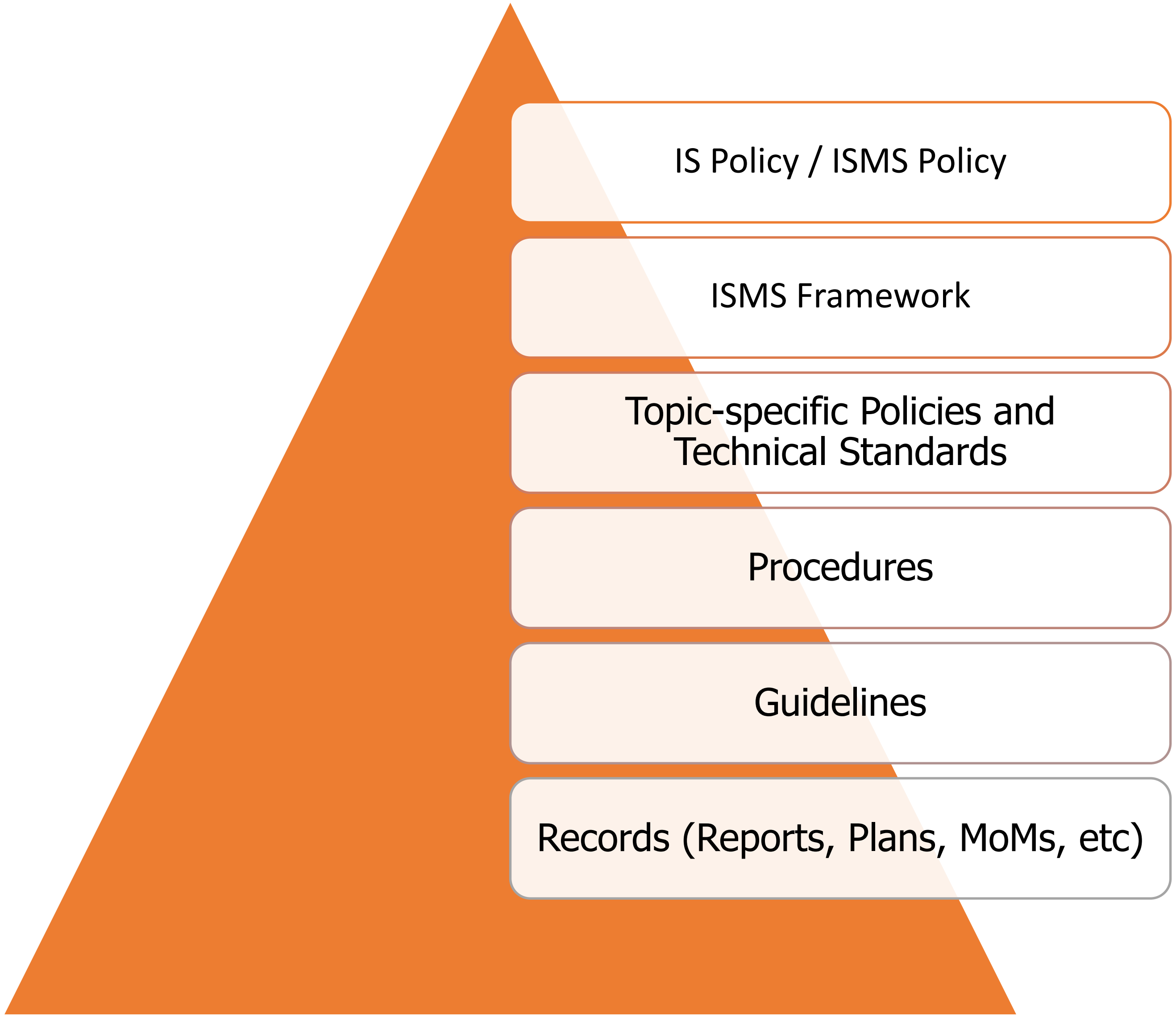
NOTE The extent of documented information for an information security management system can differ from one organization to another due to:

- the size of organization and its type of activities, processes, products and services;
- the complexity of processes and their interactions; and
- the competence of persons.

Required (mandatory) documented information

Requirements	ISO 27001:2022	My comments
1. Scope of the ISMS	4.3	Stand-alone document or appendix of the ISMS framework
2. Information security policy	5.2	Public document. Usually short, one-page
3. Information security risk assessment process	6.1.2	Information security risk management procedure and methodology, Risk Register and Reports, Risk treatment plan (RTP), MoMs
4. Information security risk treatment process	6.1.3	
5. Statement of Applicability (SoA)	6.1.3 d)	Usually Excel file / Data base
6. Information security objectives	6.2	Part of the ISMS framework / ISMS Policy + related metrics and KPIs
7. Evidence of competence	7.2 d)	Set of documents Job descriptions, CVs, Certifications, Education plan and other records
8. Documented information determined by the organization as being necessary for the effectiveness of the ISMS	7.5.1 b)	List of ISMS documents, Document management procedure Set of ISMS documents
9. Operational planning and control	8.1	Set of documents Plans, reports and MoMs, SLAs/OLAs, RACI chart and a list of ISMS processes
10. Results of the information security risk assessments	8.2	Risk Register and Reports, Risk treatment plan (RTP), KRIs, Orders, MoMs and other records
11. Results of the information security risk treatment	8.3	
12. Evidence of the monitoring and measurement results	9.1	List of metrics and KPIs, reports and MoMs
13. Evidence of the audit programme(s) and the audit results	9.2	Documented procedure, Audit Programme, Plans and Reports
14. Evidence of the results of management reviews	9.3.3	Management review Reports and MoMs
15. Evidence of the nature of the nonconformities and any subsequent actions taken	10.2 f)	Documented procedure, List of NCs, NC Reports and other records
16. Evidence of the results of any corrective action	10.2 g)	Orders, Plans, Reports and other records

ISMS Documentation Pyramid



IS Policy / ISMS Policy

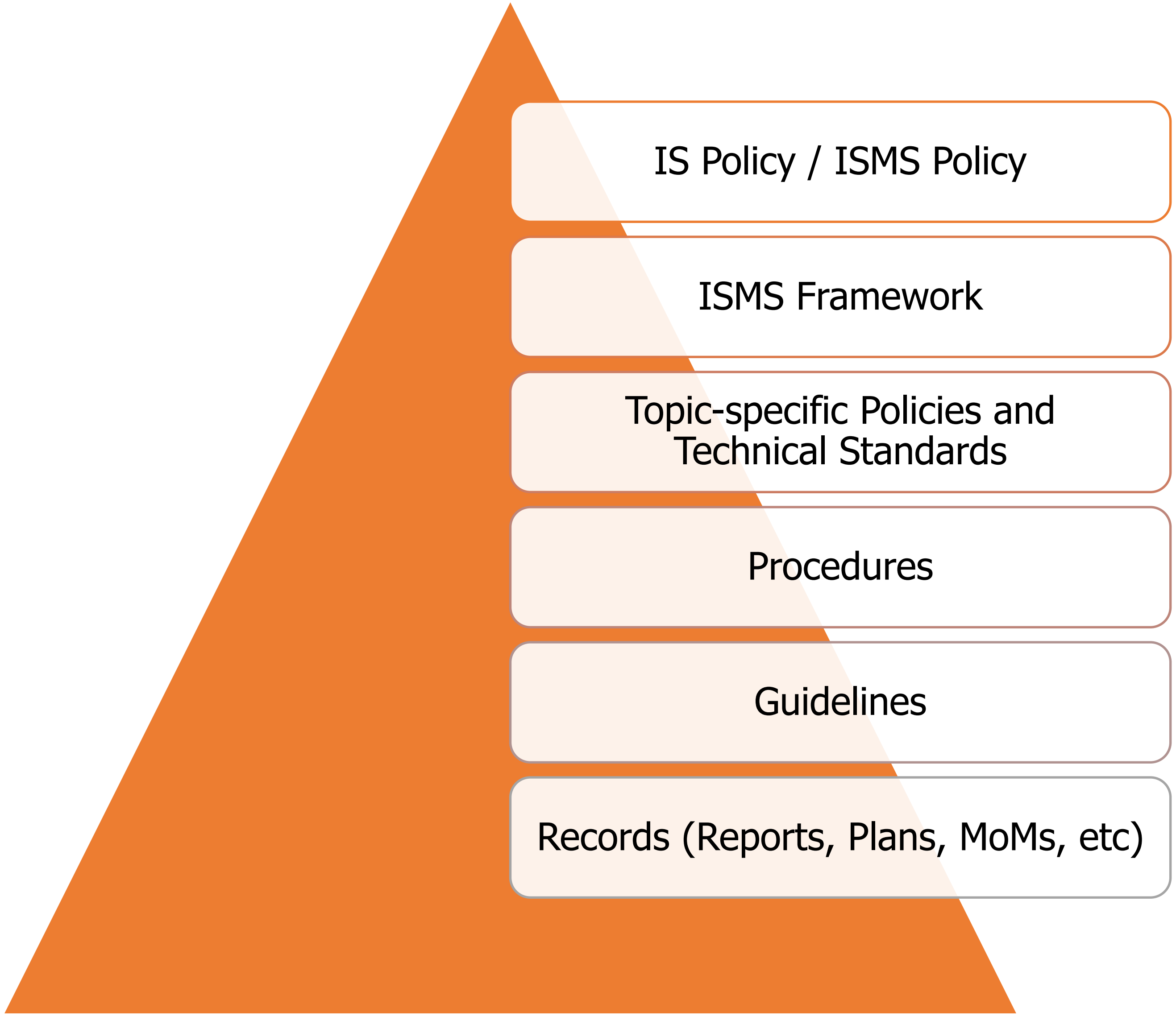
ISMS Framework

Topic-specific Policies and Technical Standards

Procedures

Guidelines

Records (Reports, Plans, MoMs, etc)


IS Policy / ISMS Policy
ISMS Framework
Topic-specific Policies and Technical Standards
Procedures
Guidelines
Records (Reports, Plans, MoMs, etc)

- **Policy**: A document that communicates required and prohibited activities and behaviors
- **Framework**: Structure of processes and specifications designed to support the accomplishment of a specific task
- **Procedure**: A document containing a detailed description of the steps necessary to perform specific operations in conformance with applicable standards. Procedures are defined as part of processes
- **Process**: Generally, a collection of activities influenced by the enterprise’s policies and procedures that takes inputs from a number of sources, (including other processes), manipulates the inputs and produces outputs.
- **Guideline**: A description of a particular way of accomplishing something that is less prescriptive than a procedure
- **Record**: Document stating results achieved or providing evidence of activities performed

IS Policy. General Requirements (ISO 27001:2022)

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

5.2 Policy

Top management shall establish an information security policy that:

a) is appropriate to the purpose of the organization

b) includes information security **objectives** or provides the framework for setting information security objectives

c) includes a commitment to **satisfy applicable requirements** related to information security

d) includes a commitment to **continual improvement** of the information security management system (ISMS)

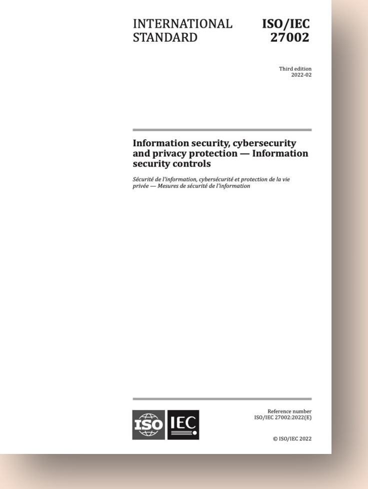
The information security policy shall:

e) be available as documented information

f) be communicated within the organization

g) be available to interested parties, as appropriate

Topics mentioned in ISO 27002: A.5.1 Policies for information security



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

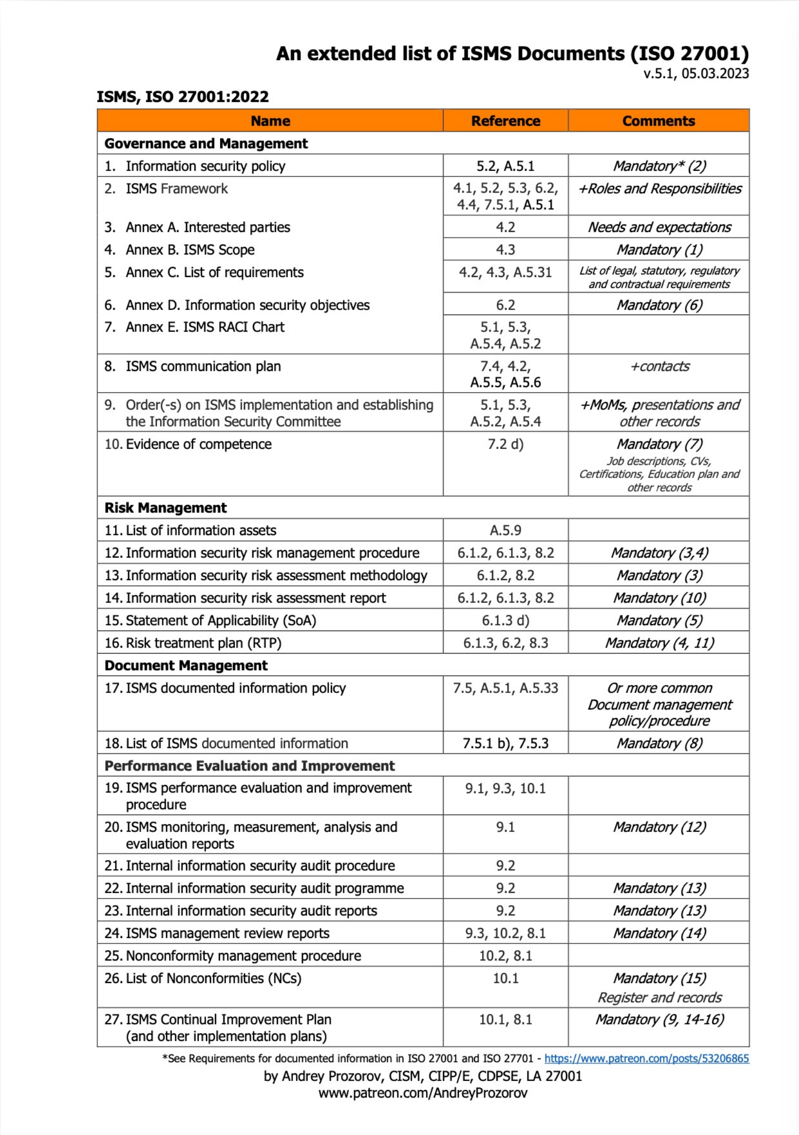
Reference number
ISO/IEC 27002:2022(E)

© ISO/IEC 2022

At a lower level, the information security policy should be supported by topic-specific policies as needed, to further mandate the implementation of information security controls. Topic-specific policies are typically structured to address the needs of certain target groups within an organization or to cover certain security areas.

Examples of such topics include:

a) Access control
b) Physical and environmental security
c) Asset management
d) Information transfer
e) Secure configuration and handling of user endpoint devices
f) Networking security
g) Information security incident management
h) Backup
i) Cryptography and key management
j) Information classification and handling
k) Management of technical vulnerabilities
l) Secure development



An extended list of ISMS Documents (ISO 27001)

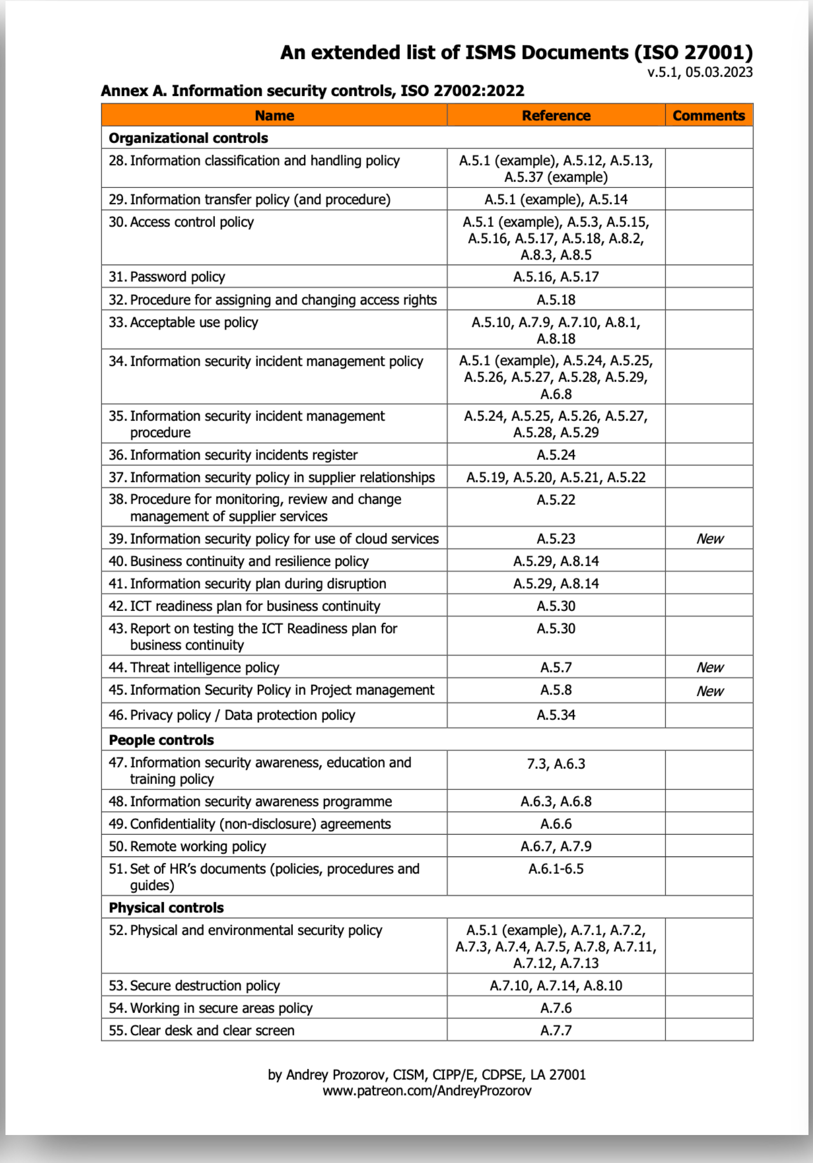
v.5.1, 05.03.2023

ISMS, ISO 27001:2022

Name	Reference	Comments
Governance and Management		
1. Information security policy	5.2, A.5.1	*Mandatory* (2)*
2. ISMS Framework	4.1, 5.2, 5.3, 6.2, 4.4, 7.5.1, A.5.1	*+Roles and Responsibilities*
3. Annex A. Interested parties	4.2	*Needs and expectations*
4. Annex B. ISMS Scope	4.3	*Mandatory (1)*
5. Annex C. List of requirements	4.2, 4.3, A.5.31	*List of legal, statutory, regulatory and contractual requirements*
6. Annex D. Information security objectives	6.2	*Mandatory (6)*
7. Annex E. ISMS RACI Chart	5.1, 5.3, A.5.4, A.5.2	
8. ISMS communication plan	7.4, 4.2, A.5.5, A.5.6	*+contacts*
9. Order(-s) on ISMS implementation and establishing the Information Security Committee	5.1, 5.3, A.5.2, A.5.4	*+MoMs, presentations and other records*
10. Evidence of competence	7.2 d)	*Mandatory (7)* *Job descriptions, CVs, Certifications, Education plan and other records*
Risk Management		
11. List of information assets	A.5.9	
12. Information security risk management procedure	6.1.2, 6.1.3, 8.2	*Mandatory (3,4)*
13. Information security risk assessment methodology	6.1.2, 8.2	*Mandatory (3)*
14. Information security risk assessment report	6.1.2, 6.1.3, 8.2	*Mandatory (10)*
15. Statement of Applicability (SoA)	6.1.3 d)	*Mandatory (5)*
16. Risk treatment plan (RTP)	6.1.3, 6.2, 8.3	*Mandatory (4, 11)*
Document Management		
17. ISMS documented information policy	7.5, A.5.1, A.5.33	*Or more common Document management policy/procedure*
18. List of ISMS documented information	7.5.1 b), 7.5.3	*Mandatory (8)*
Performance Evaluation and Improvement		
19. ISMS performance evaluation and improvement procedure	9.1, 9.3, 10.1	
20. ISMS monitoring, measurement, analysis and evaluation reports	9.1	*Mandatory (12)*
21. Internal information security audit procedure	9.2	
22. Internal information security audit programme	9.2	*Mandatory (13)*
23. Internal information security audit reports	9.2	*Mandatory (13)*
24. ISMS management review reports	9.3, 10.2, 8.1	*Mandatory (14)*
25. Nonconformity management procedure	10.2, 8.1	
26. List of Nonconformities (NCs)	10.1	*Mandatory (15)* *Register and records*
27. ISMS Continual Improvement Plan (and other implementation plans)	10.1, 8.1	*Mandatory (9, 14-16)*

*See Requirements for documented information in ISO 27001 and ISO 27701 - https://www.patreon.com/posts/53206865

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



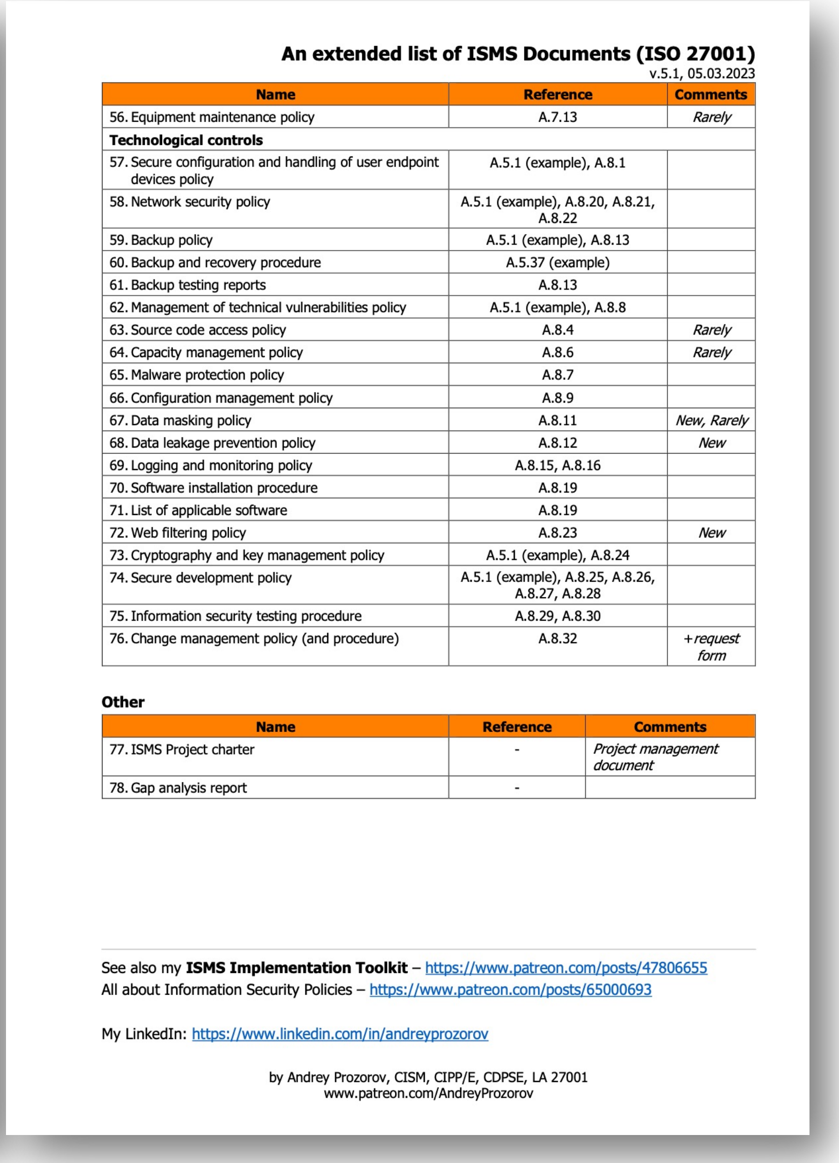
An extended list of ISMS Documents (ISO 27001)

v.5.1, 05.03.2023

Annex A. Information security controls, ISO 27002:2022

Name	Reference	Comments
Organizational controls		
28. Information classification and handling policy	A.5.1 (example), A.5.12, A.5.13, A.5.37 (example)	
29. Information transfer policy (and procedure)	A.5.1 (example), A.5.14	
30. Access control policy	A.5.1 (example), A.5.3, A.5.15, A.5.16, A.5.17, A.5.18, A.8.2, A.8.3, A.8.5	
31. Password policy	A.5.16, A.5.17	
32. Procedure for assigning and changing access rights	A.5.18	
33. Acceptable use policy	A.5.10, A.7.9, A.7.10, A.8.1, A.8.18	
34. Information security incident management policy	A.5.1 (example), A.5.24, A.5.25, A.5.26, A.5.27, A.5.28, A.5.29, A.6.8	
35. Information security incident management procedure	A.5.24, A.5.25, A.5.26, A.5.27, A.5.28, A.5.29	
36. Information security incidents register	A.5.24	
37. Information security policy in supplier relationships	A.5.19, A.5.20, A.5.21, A.5.22	
38. Procedure for monitoring, review and change management of supplier services	A.5.22	
39. Information security policy for use of cloud services	A.5.23	*New*
40. Business continuity and resilience policy	A.5.29, A.8.14	
41. Information security plan during disruption	A.5.29, A.8.14	
42. ICT readiness plan for business continuity	A.5.30	
43. Report on testing the ICT Readiness plan for business continuity	A.5.30	
44. Threat intelligence policy	A.5.7	*New*
45. Information Security Policy in Project management	A.5.8	*New*
46. Privacy policy / Data protection policy	A.5.34	
People controls		
47. Information security awareness, education and training policy	7.3, A.6.3	
48. Information security awareness programme	A.6.3, A.6.8	
49. Confidentiality (non-disclosure) agreements	A.6.6	
50. Remote working policy	A.6.7, A.7.9	
51. Set of HR's documents (policies, procedures and guides)	A.6.1-6.5	
Physical controls		
52. Physical and environmental security policy	A.5.1 (example), A.7.1, A.7.2, A.7.3, A.7.4, A.7.5, A.7.8, A.7.11, A.7.12, A.7.13	
53. Secure destruction policy	A.7.10, A.7.14, A.8.10	
54. Working in secure areas policy	A.7.6	
55. Clear desk and clear screen	A.7.7	

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



An extended list of ISMS Documents (ISO 27001)

v.5.1, 05.03.2023

Name	Reference	Comments
56. Equipment maintenance policy	A.7.13	*Rarely*
Technological controls		
57. Secure configuration and handling of user endpoint devices policy	A.5.1 (example), A.8.1	
58. Network security policy	A.5.1 (example), A.8.20, A.8.21, A.8.22	
59. Backup policy	A.5.1 (example), A.8.13	
60. Backup and recovery procedure	A.5.37 (example)	
61. Backup testing reports	A.8.13	
62. Management of technical vulnerabilities policy	A.5.1 (example), A.8.8	
63. Source code access policy	A.8.4	*Rarely*
64. Capacity management policy	A.8.6	*Rarely*
65. Malware protection policy	A.8.7	
66. Configuration management policy	A.8.9	
67. Data masking policy	A.8.11	*New, Rarely*
68. Data leakage prevention policy	A.8.12	*New*
69. Logging and monitoring policy	A.8.15, A.8.16	
70. Software installation procedure	A.8.19	
71. List of applicable software	A.8.19	
72. Web filtering policy	A.8.23	*New*
73. Cryptography and key management policy	A.5.1 (example), A.8.24	
74. Secure development policy	A.5.1 (example), A.8.25, A.8.26, A.8.27, A.8.28	
75. Information security testing procedure	A.8.29, A.8.30	
76. Change management policy (and procedure)	A.8.32	*+request form*

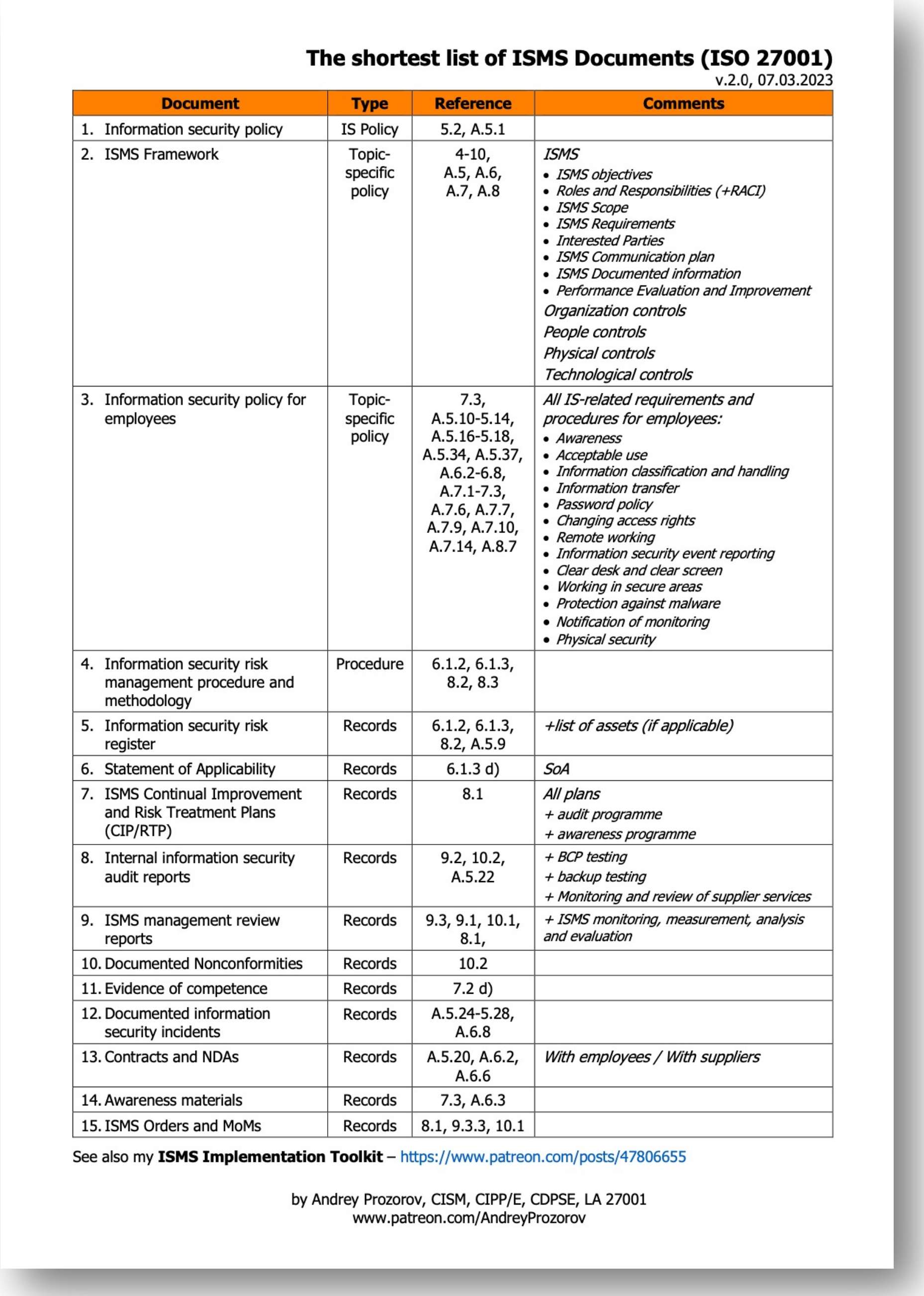
Other

Name	Reference	Comments
77. ISMS Project charter	-	*Project management document*
78. Gap analysis report	-	

See also my **ISMS Implementation Toolkit** – https://www.patreon.com/posts/47806655
All about Information Security Policies – https://www.patreon.com/posts/65000693

My LinkedIn: https://www.linkedin.com/in/andreyprozorov

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



The shortest list of ISMS Documents (ISO 27001)

v.2.0, 07.03.2023

Document	Type	Reference	Comments
1. Information security policy	IS Policy	5.2, A.5.1	
2. ISMS Framework	Topic-specific policy	4-10, A.5, A.6, A.7, A.8	*ISMS* • *ISMS objectives* • *Roles and Responsibilities (+RACI)* • *ISMS Scope* • *ISMS Requirements* • *Interested Parties* • *ISMS Communication plan* • *ISMS Documented information* • *Performance Evaluation and Improvement* *Organization controls* *People controls* *Physical controls* *Technological controls*
3. Information security policy for employees	Topic-specific policy	7.3, A.5.10-5.14, A.5.16-5.18, A.5.34, A.5.37, A.6.2-6.8, A.7.1-7.3, A.7.6, A.7.7, A.7.9, A.7.10, A.7.14, A.8.7	*All IS-related requirements and procedures for employees:* • *Awareness* • *Acceptable use* • *Information classification and handling* • *Information transfer* • *Password policy* • *Changing access rights* • *Remote working* • *Information security event reporting* • *Clear desk and clear screen* • *Working in secure areas* • *Protection against malware* • *Notification of monitoring* • *Physical security*
4. Information security risk management procedure and methodology	Procedure	6.1.2, 6.1.3, 8.2, 8.3	
5. Information security risk register	Records	6.1.2, 6.1.3, 8.2, A.5.9	*+list of assets (if applicable)*
6. Statement of Applicability	Records	6.1.3 d)	*SoA*
7. ISMS Continual Improvement and Risk Treatment Plans (CIP/RTP)	Records	8.1	*All plans* *+ audit programme* *+ awareness programme*
8. Internal information security audit reports	Records	9.2, 10.2, A.5.22	*+ BCP testing* *+ backup testing* *+ Monitoring and review of supplier services*
9. ISMS management review reports	Records	9.3, 9.1, 10.1, 8.1,	*+ ISMS monitoring, measurement, analysis and evaluation*
10. Documented Nonconformities	Records	10.2	
11. Evidence of competence	Records	7.2 d)	
12. Documented information security incidents	Records	A.5.24-5.28, A.6.8	
13. Contracts and NDAs	Records	A.5.20, A.6.2, A.6.6	*With employees / With suppliers*
14. Awareness materials	Records	7.3, A.6.3	
15. ISMS Orders and MoMs	Records	8.1, 9.3.3, 10.1	

See also my **ISMS Implementation Toolkit** – https://www.patreon.com/posts/47806655

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

Some comments:

1. The list of documents and their titles depend on the overall approach of the organisation, its size, and the expectations of interested parties (internal and external)
2. Some of the topic-specific policies might be combined in one document (e.g. ISMS Framework, IT Security Policy, Physical Security Policy, Acceptable Use Policy…)
3. Mandatory documents must be provided in order to certify an ISMS
4. ISMS Documented Information Policy is valuable if you don’t have a General Document Management Policy / Procedure
5. Document and regularly update the list of ISMS documents

Documented Information. Creating and updating (ISO 27001:2022)

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

7.5.2 Creating and updating

When creating and updating documented information the organization shall ensure appropriate:

a) Identification and description (e.g. a title, date, author, or reference number);

b) Format (e.g. language, software version, graphics) and media (e.g. paper, electronic); and

c) Review and approval for suitability and adequacy.

Documented Information. Creating and updating (ISO 27001:2022)

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

7.5.2 Creating and updating

When creating and updating documented information the organization shall ensure appropriate:

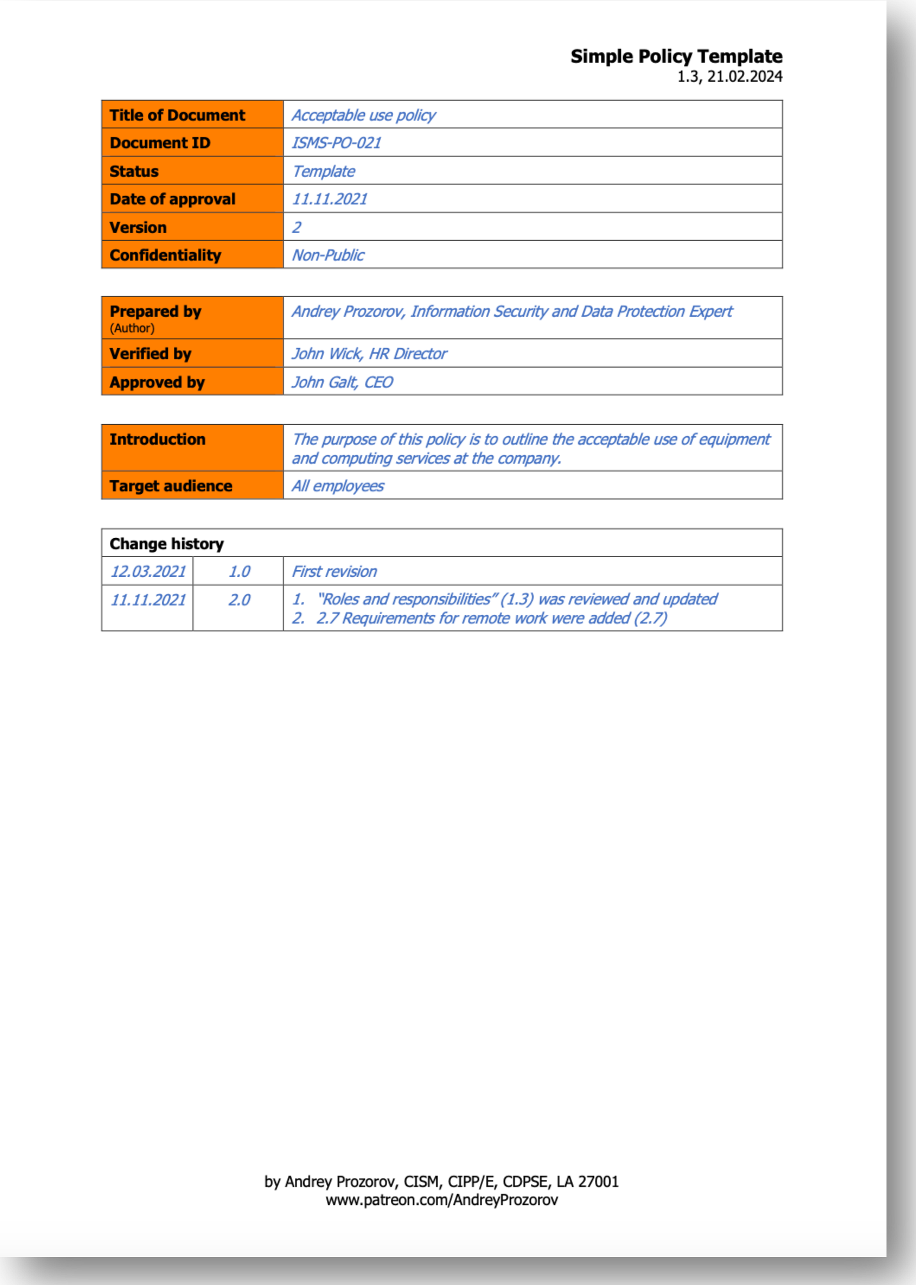
a) Identification and description (e.g. a title, date, author, or reference number);

b) Format (e.g. language, software version, graphics) and media (e.g. paper, electronic); and

c) Review and approval for suitability and adequacy.

My comment. Auditors also review:

- history of changes
- identity of reviewer and approver



Simple Policy Template
1.3, 21.02.2024

Title of Document	*Acceptable use policy*
Document ID	*ISMS-PO-021*
Status	*Template*
Date of approval	*11.11.2021*
Version	*2*
Confidentiality	*Non-Public*

Prepared by (Author)	*Andrey Prozorov, Information Security and Data Protection Expert*
Verified by	*John Wick, HR Director*
Approved by	*John Galt, CEO*

Introduction	*The purpose of this policy is to outline the acceptable use of equipment and computing services at the company.*
Target audience	*All employees*

Change history		
12.03.2021	*1.0*	*First revision*
11.11.2021	*2.0*	*1. "Roles and responsibilities" (1.3) was reviewed and updated* *2. 2.7 Requirements for remote work were added (2.7)*

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

Title page:

1. Title of Document
2. Document ID
3. Status
4. Date of approval
5. Version
6. Confidentiality

7. Prepared by (Author)
8. Verified by
9. Approved by

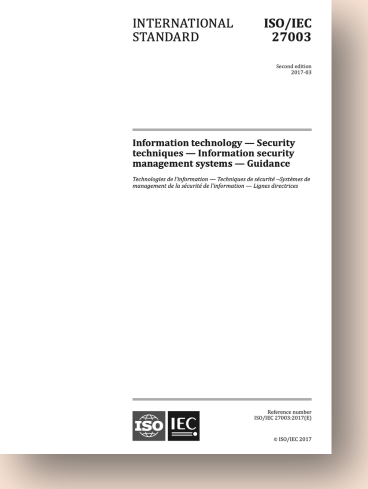
10. Introduction
11. Target audience
12. Change history

The main body:

1. Acronyms and abbreviations
2. Terms and definitions
3. Introduction
   - Purpose and objectives
   - Scope
   - Roles and Responsibilities

4. General Provisions
5. Main points of the document / Policy requirements
6. Document revision (Provisions for document revision)
7. References / Related Policies
8. Annexes (if applicable)

Content of policies
(ISO 27003)



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

The content of policies is based on the context in which an organization operates. Specifically, the following should be considered when developing any policy within the policy framework:

1. The aims and objectives of the organization
2. Strategies adopted to achieve the organization's objectives
3. The structure and processes adopted by the organization
4. Aims and objectives associated with the topic of the policy
5. The requirements of related higher level policies
6. The target group to be directed by the policy

Statements and writing style should be tailored to the **audience** and **scope** of the documentation

Verbal Forms

- “**Shall**” indicates a requirement
- “**Should**” indicates a recommendation
- “**May**” indicates a permission
- “**Can**” indicates a possibility or a capability

Where to find inspiration?

1. Copy-paste from standards and good practices or retell them. I prefer ISO 27001/27002/27003, ISF SoGP, COBIT and CIS Controls
2. Use ISO 27001 Toolkits
3. Ask ChatGPT, Notion AI or other AI
4. Google it (“filetype:pdf policy name”)

TOP 5
ISMS Toolkits
(ISO 27001)

1. ISO27k Toolkit by ISO27k Forum (Free) - https://lnkd.in/eC5Kh5d6
2. **ISMS Implementation Toolkit by Andrey Prozorov** - https://lnkd.in/enzZdZ9
3. ISO 27001 Documentation Toolkit by Advisera - https://lnkd.in/euYBc-SW
4. ISO 27001 Toolkit by CertiKit -https://lnkd.in/ePxZUjHe
5. ISO 27001 Toolkit by IT Governance - https://lnkd.in/eAwTcuE6

Information Classification and Labelling

A. 5.12 Classification of information

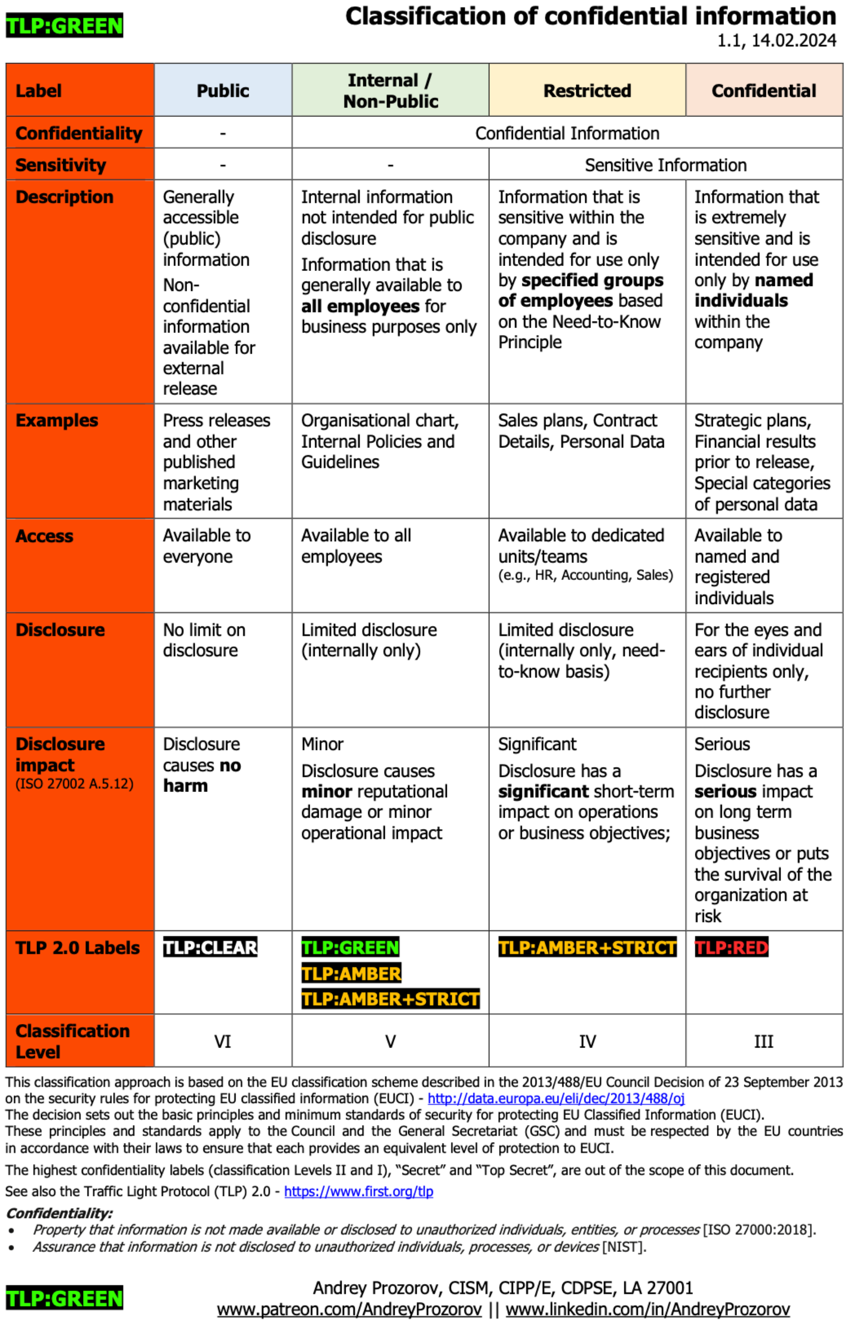
Information shall be classified according to the information security needs of the organization based on confidentiality, integrity, availability and relevant interested party requirements.

A. 5.13 Labelling of information

An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization.

Owners of information should be accountable for their classification...

Classification of confidential information (simple approach)



TLP:GREEN

Classification of confidential information

1.1, 14.02.2024

Label	Public	Internal / Non-Public	Restricted	Confidential
Confidentiality	-	Confidential Information		
Sensitivity	-	-	Sensitive Information	
Description	Generally accessible (public) information Non-confidential information available for external release	Internal information not intended for public disclosure Information that is generally available to **all employees** for business purposes only	Information that is sensitive within the company and is intended for use only by **specified groups of employees** based on the Need-to-Know Principle	Information that is extremely sensitive and is intended for use only by **named individuals** within the company
Examples	Press releases and other published marketing materials	Organisational chart, Internal Policies and Guidelines	Sales plans, Contract Details, Personal Data	Strategic plans, Financial results prior to release, Special categories of personal data
Access	Available to everyone	Available to all employees	Available to dedicated units/teams (e.g., HR, Accounting, Sales)	Available to named and registered individuals
Disclosure	No limit on disclosure	Limited disclosure (internally only)	Limited disclosure (internally only, need-to-know basis)	For the eyes and ears of individual recipients only, no further disclosure
Disclosure impact (ISO 27002 A.5.12)	Disclosure causes **no harm**	Minor Disclosure causes **minor** reputational damage or minor operational impact	Significant Disclosure has a **significant** short-term impact on operations or business objectives;	Serious Disclosure has a **serious** impact on long term business objectives or puts the survival of the organization at risk
TLP 2.0 Labels	TLP:CLEAR	TLP:GREEN TLP:AMBER TLP:AMBER+STRICT	TLP:AMBER+STRICT	TLP:RED
Classification Level	VI	V	IV	III

This classification approach is based on the EU classification scheme described in the 2013/488/EU Council Decision of 23 September 2013 on the security rules for protecting EU classified information (EUCI) - http://data.europa.eu/eli/dec/2013/488/oj
The decision sets out the basic principles and minimum standards of security for protecting EU Classified Information (EUCI).
These principles and standards apply to the Council and the General Secretariat (GSC) and must be respected by the EU countries in accordance with their laws to ensure that each provides an equivalent level of protection to EUCI.

The highest confidentiality labels (classification Levels II and I), "Secret" and "Top Secret", are out of the scope of this document.

See also the Traffic Light Protocol (TLP) 2.0 - https://www.first.org/tlp

Confidentiality:

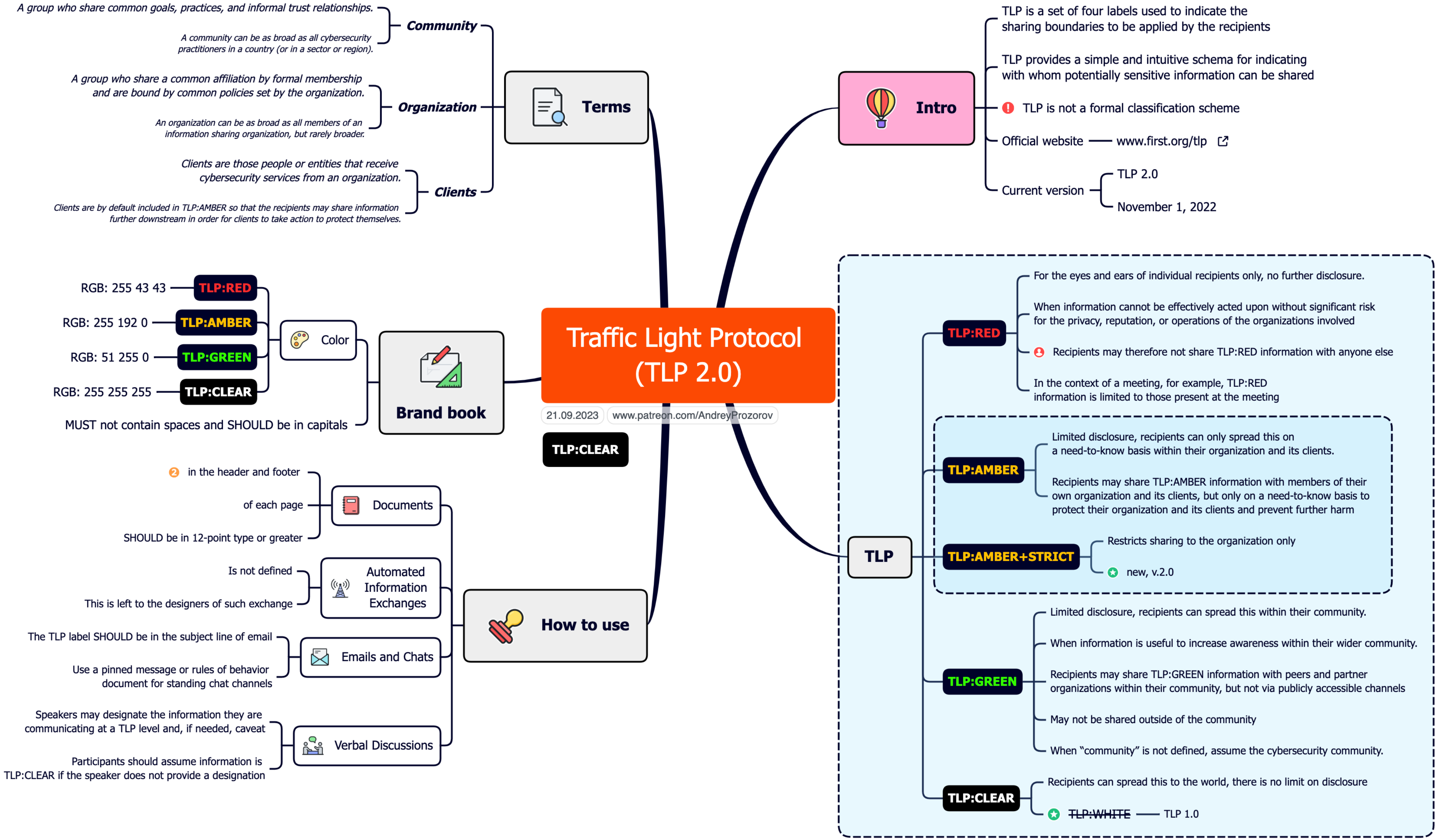
- *Property that information is not made available or disclosed to unauthorized individuals, entities, or processes* [ISO 27000:2018].
- *Assurance that information is not disclosed to unauthorized individuals, processes, or devices* [NIST].

TLP:GREEN

Andrey Prozorov, CISM, CIPP/E, CDPSE, LA 27001
www.patreon.com/AndreyProzorov || www.linkedin.com/in/AndreyProzorov

Examples of labelling techniques include:

a) physical labels
b) headers and footers
c) metadata
d) watermarking
e) rubber-stamps



Traffic Light Protocol (TLP 2.0)

21.09.2023 www.patreon.com/AndreyProzorov

TLP:CLEAR

- **Terms**
  - ***Community***
    - *A group who share common goals, practices, and informal trust relationships.*
    - *A community can be as broad as all cybersecurity practitioners in a country (or in a sector or region).*
  - ***Organization***
    - *A group who share a common affiliation by formal membership and are bound by common policies set by the organization.*
    - *An organization can be as broad as all members of an information sharing organization, but rarely broader.*
  - ***Clients***
    - *Clients are those people or entities that receive cybersecurity services from an organization.*
    - *Clients are by default included in TLP:AMBER so that the recipients may share information further downstream in order for clients to take action to protect themselves.*
- **Brand book**
  - Color
    - TLP:RED — RGB: 255 43 43
    - TLP:AMBER — RGB: 255 192 0
    - TLP:GREEN — RGB: 51 255 0
    - TLP:CLEAR — RGB: 255 255 255
  - MUST not contain spaces and SHOULD be in capitals
- **How to use**
  - Documents
    - ❷ in the header and footer
    - of each page
    - SHOULD be in 12-point type or greater
  - Automated Information Exchanges
    - Is not defined
    - This is left to the designers of such exchange
  - Emails and Chats
    - The TLP label SHOULD be in the subject line of email
    - Use a pinned message or rules of behavior document for standing chat channels
  - Verbal Discussions
    - Speakers may designate the information they are communicating at a TLP level and, if needed, caveat
    - Participants should assume information is TLP:CLEAR if the speaker does not provide a designation
- **Intro**
  - TLP is a set of four labels used to indicate the sharing boundaries to be applied by the recipients
  - TLP provides a simple and intuitive schema for indicating with whom potentially sensitive information can be shared
  - ! TLP is not a formal classification scheme
  - Official website — www.first.org/tlp
  - Current version
    - TLP 2.0
    - November 1, 2022
- **TLP**
  - **TLP:RED**
    - For the eyes and ears of individual recipients only, no further disclosure.
    - When information cannot be effectively acted upon without significant risk for the privacy, reputation, or operations of the organizations involved
    - Recipients may therefore not share TLP:RED information with anyone else
    - In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting
  - **TLP:AMBER**
    - Limited disclosure, recipients can only spread this on a need-to-know basis within their organization and its clients.
    - Recipients may share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm
  - **TLP:AMBER+STRICT**
    - Restricts sharing to the organization only
    - new, v.2.0
  - **TLP:GREEN**
    - Limited disclosure, recipients can spread this within their community.
    - When information is useful to increase awareness within their wider community.
    - Recipients may share TLP:GREEN information with peers and partner organizations within their community, but not via publicly accessible channels
    - May not be shared outside of the community
    - When "community" is not defined, assume the cybersecurity community.
  - **TLP:CLEAR**
    - Recipients can spread this to the world, there is no limit on disclosure
    - ~~TLP:WHITE~~ — TLP 1.0

Documented Information. Control (ISO 27001:2022)

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

7.5.3 Control of documented information

Documented information required by the ISMS and by this

a) it is available and suitable for use, where and when it is needed; and

b) it is adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity).

For the control of documented information, the organization shall address the following activities, as applicable:

c) distribution, access, retrieval and use;

d) storage and preservation, including the preservation of legibility;

e) control of changes (e.g. version control); and

f) retention and disposition.

Documented information of external origin, determined by the organization to be necessary for the planning and operation of the information security management system, shall be identified as appropriate, and controlled.

NOTE Access can imply a decision regarding the permission to view the documented information only, or the permission and authority to view and change the documented information, etc.

Thanks, and good luck!

www.linkedin.com/in/andreyprozorov

www.patreon.com/AndreyProzorov

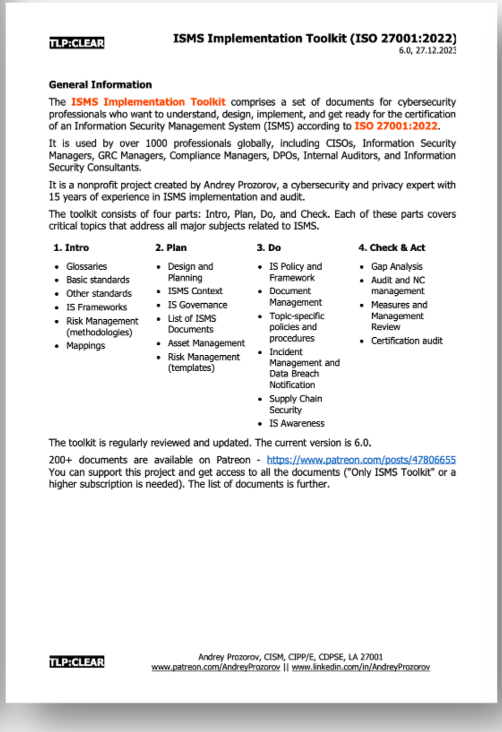
ISMS Implementation Toolkit by Andrey Prozorov

www.patreon.com/posts/47806655

ISMS IMPLEMENTATION TOOLKIT (ISO 27001:2022)

TLP:CLEAR

Andrey Prozorov, CISM, CIPP/E, CDPSE, LA 27001
www.patreon.com/AndreyProzorov || www.linkedin.com/in/AndreyProzorov



TLP:CLEAR

ISMS Implementation Toolkit (ISO 27001:2022)
6.0, 27.12.2023

General Information

The **ISMS Implementation Toolkit** comprises a set of documents for cybersecurity professionals who want to understand, design, implement, and get ready for the certification of an Information Security Management System (ISMS) according to **ISO 27001:2022**.

It is used by over 1000 professionals globally, including CISOs, Information Security Managers, GRC Managers, Compliance Managers, DPOs, Internal Auditors, and Information Security Consultants.

It is a nonprofit project created by Andrey Prozorov, a cybersecurity and privacy expert with 15 years of experience in ISMS implementation and audit.

The toolkit consists of four parts: Intro, Plan, Do, and Check. Each of these parts covers critical topics that address all major subjects related to ISMS.

1. Intro

- Glossaries
- Basic standards
- Other standards
- IS Frameworks
- Risk Management (methodologies)
- Mappings

2. Plan

- Design and Planning
- ISMS Context
- IS Governance
- List of ISMS Documents
- Asset Management
- Risk Management (templates)

3. Do

- IS Policy and Framework
- Document Management
- Topic-specific policies and procedures
- Incident Management and Data Breach Notification
- Supply Chain Security
- IS Awareness

4. Check & Act

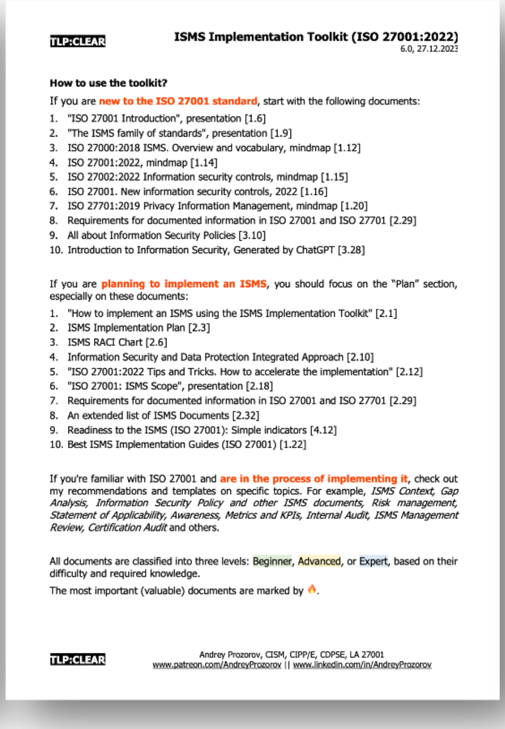
- Gap Analysis
- Audit and NC management
- Measures and Management Review
- Certification audit

The toolkit is regularly reviewed and updated. The current version is 6.0.

200+ documents are available on Patreon - https://www.patreon.com/posts/47806655
You can support this project and get access to all the documents ("Only ISMS Toolkit" or a higher subscription is needed). The list of documents is further.

TLP:CLEAR

Andrey Prozorov, CISM, CIPP/E, CDPSE, LA 27001
www.patreon.com/AndreyProzorov || www.linkedin.com/in/AndreyProzorov



TLP:CLEAR

ISMS Implementation Toolkit (ISO 27001:2022)
6.0, 27.12.2023

How to use the toolkit?

If you are **new to the ISO 27001 standard**, start with the following documents:

1. "ISO 27001 Introduction", presentation [1.6]
2. "The ISMS family of standards", presentation [1.9]
3. ISO 27000:2018 ISMS. Overview and vocabulary, mindmap [1.12]
4. ISO 27001:2022, mindmap [1.14]
5. ISO 27002:2022 Information security controls, mindmap [1.15]
6. ISO 27001. New information security controls, 2022 [1.16]
7. ISO 27701:2019 Privacy Information Management, mindmap [1.20]
8. Requirements for documented information in ISO 27001 and ISO 27701 [2.29]
9. All about Information Security Policies [3.10]
10. Introduction to Information Security, Generated by ChatGPT [3.28]

If you are **planning to implement an ISMS**, you should focus on the "Plan" section, especially on these documents:

1. "How to implement an ISMS using the ISMS Implementation Toolkit" [2.1]
2. ISMS Implementation Plan [2.3]
3. ISMS RACI Chart [2.6]
4. Information Security and Data Protection Integrated Approach [2.10]
5. "ISO 27001:2022 Tips and Tricks. How to accelerate the implementation" [2.12]
6. "ISO 27001: ISMS Scope", presentation [2.18]
7. Requirements for documented information in ISO 27001 and ISO 27701 [2.29]
8. An extended list of ISMS Documents [2.32]
9. Readiness to the ISMS (ISO 27001): Simple indicators [4.12]
10. Best ISMS Implementation Guides (ISO 27001) [1.22]

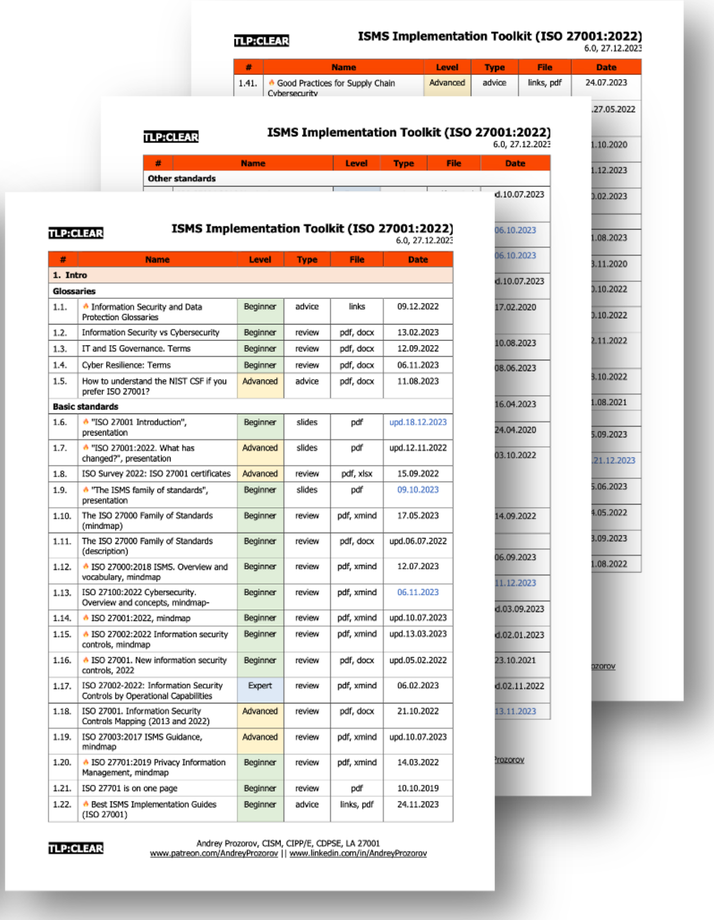
If you're familiar with ISO 27001 and **are in the process of implementing it**, check out my recommendations and templates on specific topics. For example, *ISMS Context, Gap Analysis, Information Security Policy and other ISMS documents, Risk management, Statement of Applicability, Awareness, Metrics and KPIs, Internal Audit, ISMS Management Review, Certification Audit* and others.

All documents are classified into three levels: Beginner, Advanced, or Expert, based on their difficulty and required knowledge.

The most important (valuable) documents are marked by 🔥.

TLP:CLEAR

Andrey Prozorov, CISM, CIPP/E, CDPSE, LA 27001
www.patreon.com/AndreyProzorov || www.linkedin.com/in/AndreyProzorov



TLP:CLEAR

ISMS Implementation Toolkit (ISO 27001:2022)
6.0, 27.12.2023

#	Name	Level	Type	File	Date
1.41.	🔥 Good Practices for Supply Chain Cybersecurity	Advanced	advice	links, pdf	24.07.2023

TLP:CLEAR

ISMS Implementation Toolkit (ISO 27001:2022)
6.0, 27.12.2023

#	Name	Level	Type	File	Date
Other standards					

TLP:CLEAR

ISMS Implementation Toolkit (ISO 27001:2022)
6.0, 27.12.2023

#	Name	Level	Type	File	Date
1. Intro					
Glossaries					
1.1.	🔥 Information Security and Data Protection Glossaries	Beginner	advice	links	09.12.2022
1.2.	Information Security vs Cybersecurity	Beginner	review	pdf, docx	13.02.2023
1.3.	IT and IS Governance. Terms	Beginner	review	pdf, docx	12.09.2022
1.4.	Cyber Resilience: Terms	Beginner	review	pdf, docx	06.11.2023
1.5.	How to understand the NIST CSF if you prefer ISO 27001?	Advanced	advice	pdf, docx	11.08.2023
Basic standards					
1.6.	🔥 "ISO 27001 Introduction", presentation	Beginner	slides	pdf	upd.18.12.2023
1.7.	🔥 "ISO 27001:2022. What has changed?", presentation	Advanced	slides	pdf	upd.12.11.2022
1.8.	ISO Survey 2022: ISO 27001 certificates	Advanced	review	pdf, xlsx	15.09.2022
1.9.	🔥 "The ISMS family of standards", presentation	Beginner	slides	pdf	09.10.2023
1.10.	The ISO 27000 Family of Standards (mindmap)	Beginner	review	pdf, xmind	17.05.2023
1.11.	The ISO 27000 Family of Standards (description)	Beginner	review	pdf, docx	upd.06.07.2022
1.12.	🔥 ISO 27000:2018 ISMS. Overview and vocabulary, mindmap	Beginner	review	pdf, xmind	12.07.2023
1.13.	ISO 27100:2022 Cybersecurity. Overview and concepts, mindmap-	Beginner	review	pdf, xmind	06.11.2023
1.14.	🔥 ISO 27001:2022, mindmap	Beginner	review	pdf, xmind	upd.10.07.2023
1.15.	🔥 ISO 27002:2022 Information security controls, mindmap	Beginner	review	pdf, xmind	upd.13.03.2023
1.16.	🔥 ISO 27001. New information security controls, 2022	Beginner	review	pdf, docx	upd.05.02.2022
1.17.	ISO 27002-2022: Information Security Controls by Operational Capabilities	Expert	review	pdf, xmind	06.02.2023
1.18.	ISO 27001. Information Security Controls Mapping (2013 and 2022)	Advanced	review	pdf, docx	21.10.2022
1.19.	ISO 27003:2017 ISMS Guidance, mindmap	Advanced	review	pdf, xmind	upd.10.07.2023
1.20.	🔥 ISO 27701:2019 Privacy Information Management, mindmap	Beginner	review	pdf, xmind	14.03.2022
1.21.	ISO 27701 is on one page	Beginner	review	pdf	10.10.2019
1.22.	🔥 Best ISMS Implementation Guides (ISO 27001)	Beginner	advice	links, pdf	24.11.2023

TLP:CLEAR

Andrey Prozorov, CISM, CIPP/E, CDPSE, LA 27001
www.patreon.com/AndreyProzorov || www.linkedin.com/in/AndreyProzorov

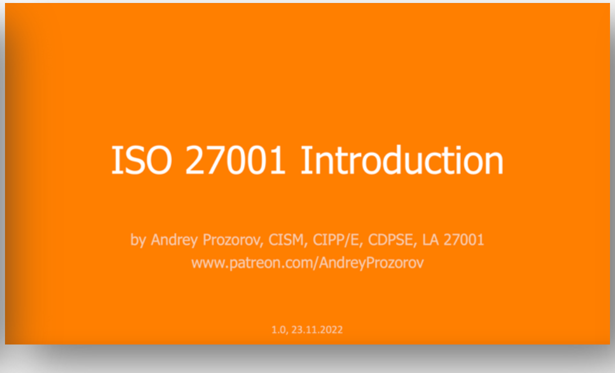
ISO Survey 2022:
ISO 27001 certificates

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

ISO 27001:2022.
What has changed?

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

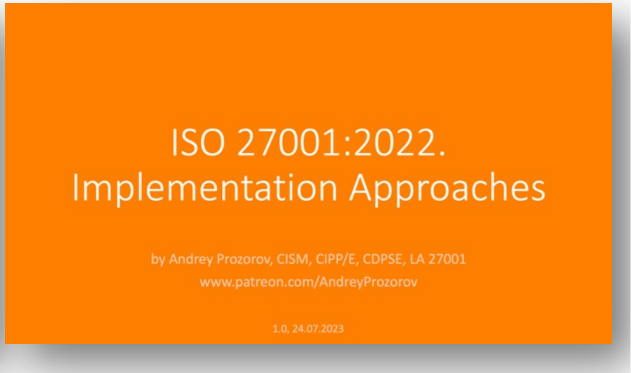
1.0, 25.10.2022



ISO 27001 Introduction

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

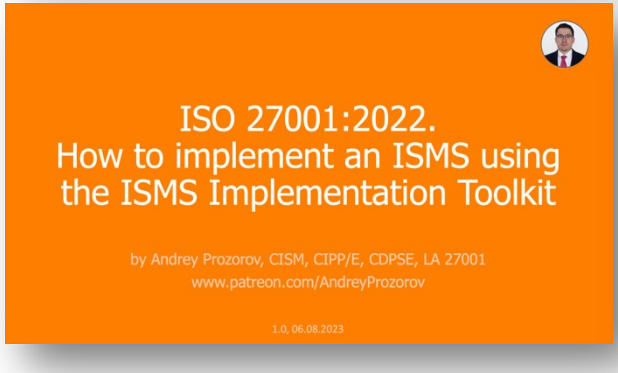
1.0, 23.11.2022



ISO 27001:2022.
Implementation Approaches

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

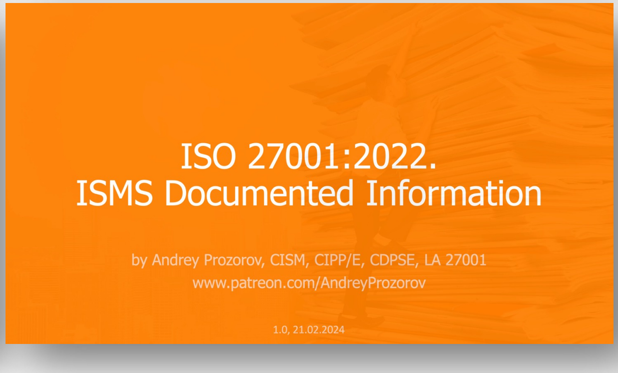
1.0, 24.07.2023



ISO 27001:2022.
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.
ISMS Documented Information

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

1.0, 21.02.2024

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

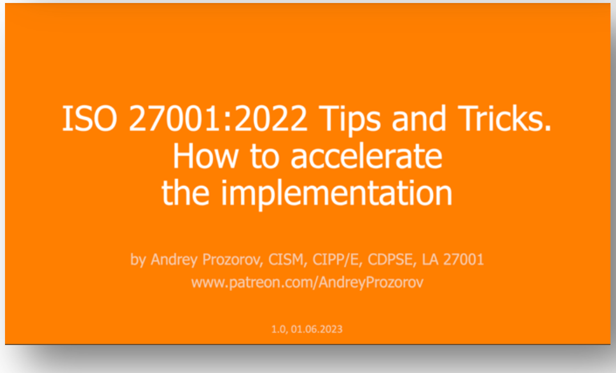
by Andrey Prozorov, CISM, CIPP/E, CDPSE, LA 27001
www.patreon.com/AndreyProzorov

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