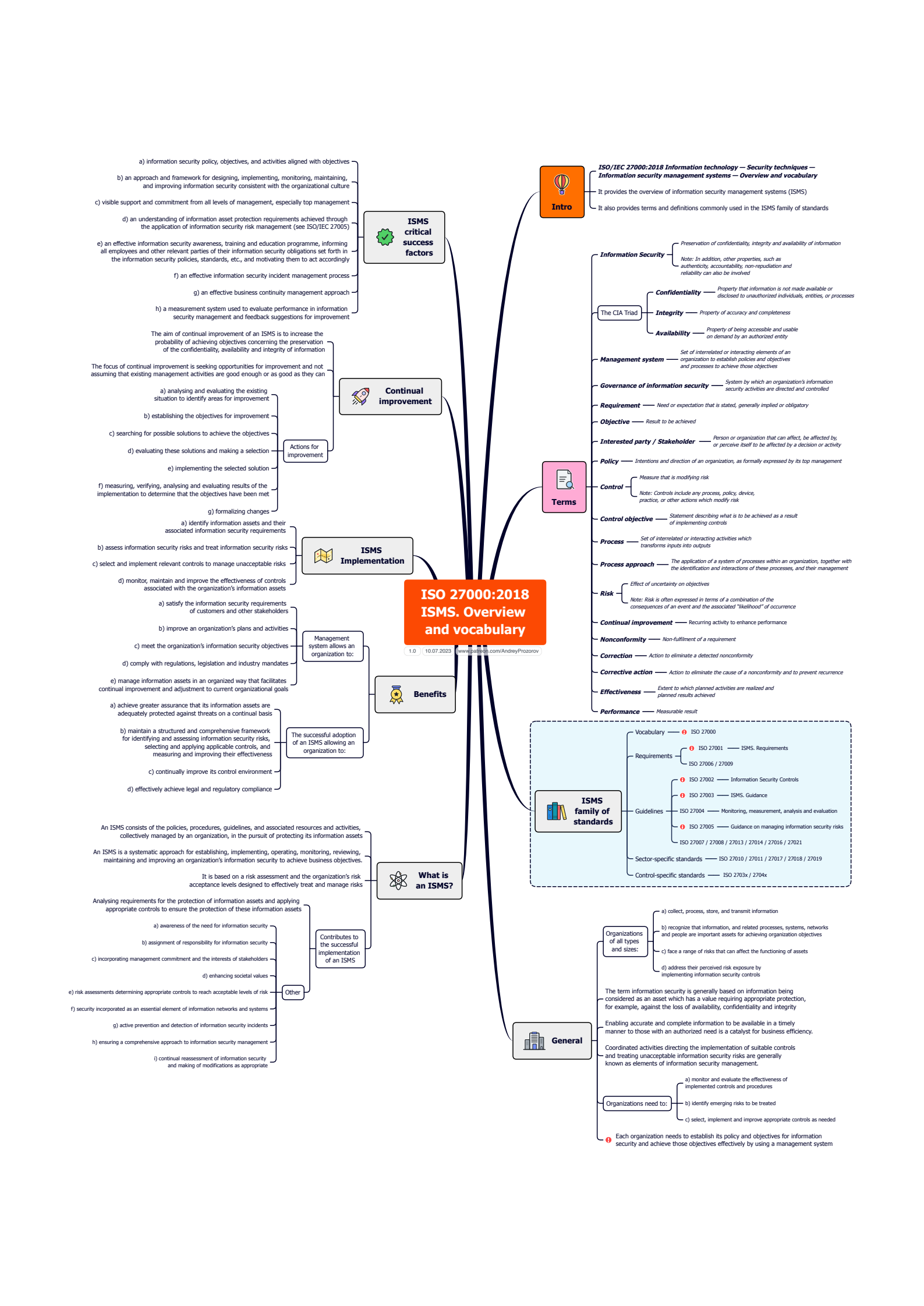
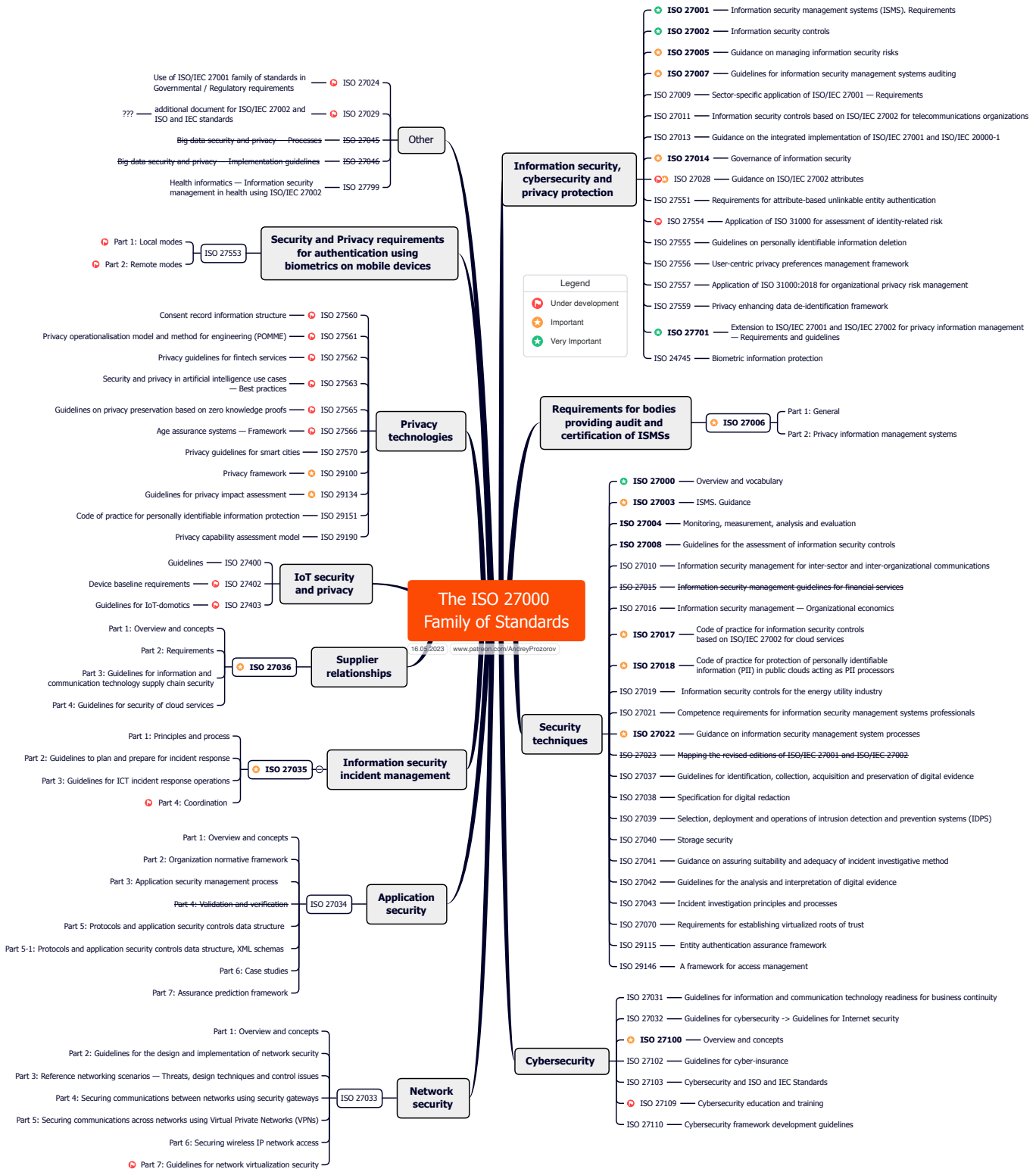
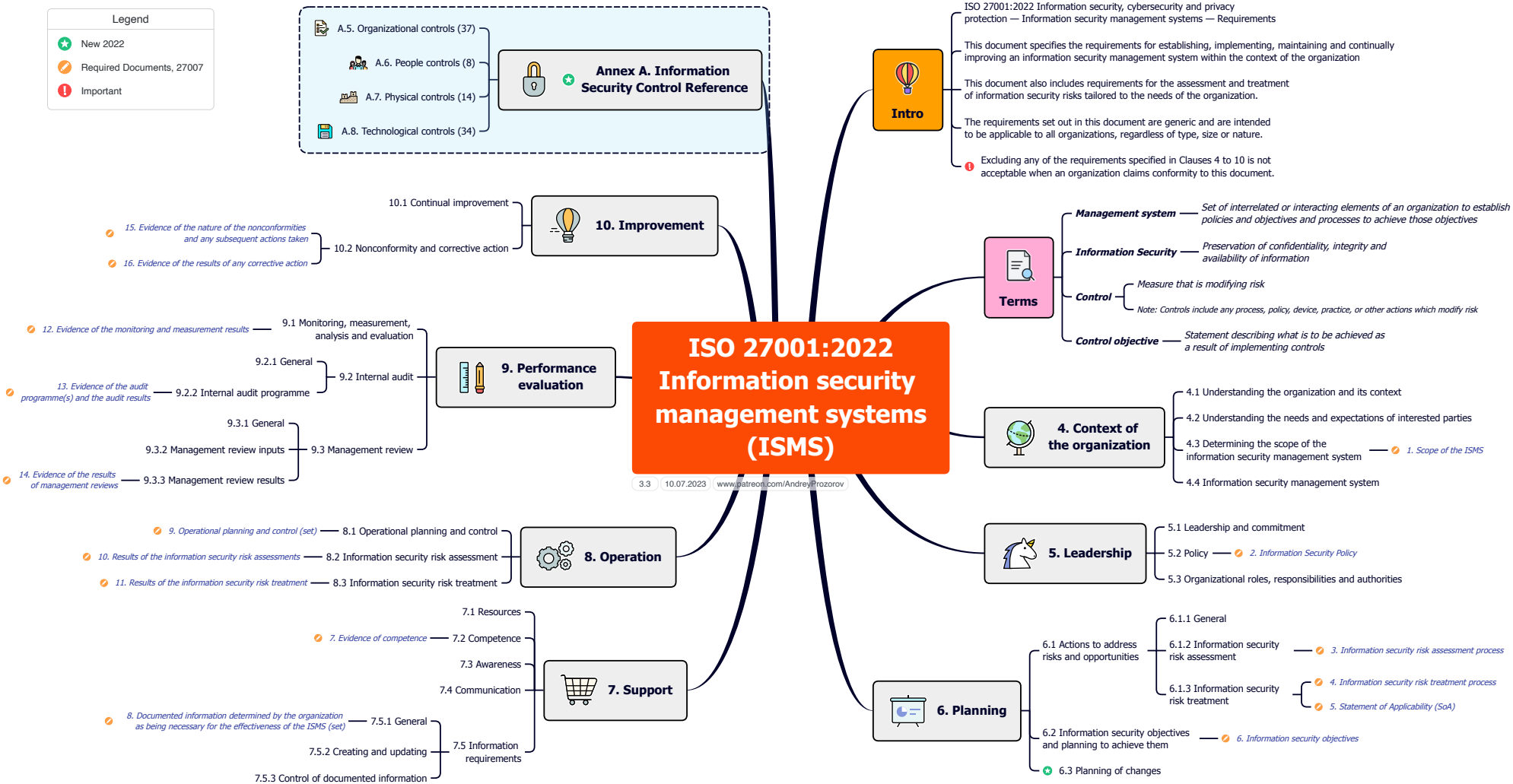

ISO 27000:2018 ISMS. Overview and vocabulary
1.0
10.07.2023
www.patreon.com/AndreyProzorov
Intro
ISO/IEC 27000:2018 Information technology — Security techniques — Information security management systems — Overview and vocabulary
It provides the overview of information security management systems (ISMS)
It also provides terms and definitions commonly used in the ISMS family of standards
Terms
Information Security
Preservation of confidentiality, integrity and availability of information
Note: In addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved
The CIA Triad
Confidentiality
Property that information is not made available or disclosed to unauthorized individuals, entities, or processes
Integrity
Property of accuracy and completeness
Availability
Property of being accessible and usable on demand by an authorized entity
Management system
Set of interrelated or interacting elements of an organization to establish policies and objectives and processes to achieve those objectives
Governance of information security
System by which an organization's information security activities are directed and controlled
Requirement
Need or expectation that is stated, generally implied or obligatory
Objective
Result to be achieved
Interested party / Stakeholder
Person or organization that can affect, be affected by, or perceive itself to be affected by a decision or activity
Policy
Intentions and direction of an organization, as formally expressed by its top management
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
Process
Set of interrelated or interacting activities which transforms inputs into outputs
Process approach
The application of a system of processes within an organization, together with the identification and interactions of these processes, and their management
Risk
Effect of uncertainty on objectives
Note: Risk is often expressed in terms of a combination of the consequences of an event and the associated "likelihood" of occurrence
Continual improvement
Recurring activity to enhance performance
Nonconformity
Non-fulfilment of a requirement
Correction
Action to eliminate a detected nonconformity
Corrective action
Action to eliminate the cause of a nonconformity and to prevent recurrence
Effectiveness
Extent to which planned activities are realized and planned results achieved
Performance
Measurable result
ISMS family of standards
Vocabulary
ISO 27000
Requirements
ISO 27001
ISMS. Requirements
ISO 27006 / 27009
Guidelines
ISO 27002
Information Security Controls
ISO 27003
ISMS. Guidance
ISO 27004
Monitoring, measurement, analysis and evaluation
ISO 27005
Guidance on managing information security risks
ISO 27007 / 27008 / 27013 / 27014 / 27016 / 27021
Sector-specific standards
ISO 27010 / 27011 / 27017 / 27018 / 27019
Control-specific standards
ISO 2703x / 2704x
General
Organizations of all types and sizes:
a) collect, process, store, and transmit information
b) recognize that information, and related processes, systems, networks and people are important assets for achieving organization objectives
c) face a range of risks that can affect the functioning of assets
d) address their perceived risk exposure by implementing information security controls
The term information security is generally based on information being considered as an asset which has a value requiring appropriate protection, for example, against the loss of availability, confidentiality and integrity
Enabling accurate and complete information to be available in a timely manner to those with an authorized need is a catalyst for business efficiency.
Coordinated activities directing the implementation of suitable controls and treating unacceptable information security risks are generally known as elements of information security management.
Organizations need to:
a) monitor and evaluate the effectiveness of implemented controls and procedures
b) identify emerging risks to be treated
c) select, implement and improve appropriate controls as needed
Each organization needs to establish its policy and objectives for information security and achieve those objectives effectively by using a management system
What is an ISMS?
An ISMS consists of the policies, procedures, guidelines, and associated resources and activities, collectively managed by an organization, in the pursuit of protecting its information assets
An ISMS is a systematic approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organization's information security to achieve business objectives.
It is based on a risk assessment and the organization's risk acceptance levels designed to effectively treat and manage risks
Contributes to the successful implementation of an ISMS
Analysing requirements for the protection of information assets and applying appropriate controls to ensure the protection of these information assets
Other
a) awareness of the need for information security
b) assignment of responsibility for information security
c) incorporating management commitment and the interests of stakeholders
d) enhancing societal values
e) risk assessments determining appropriate controls to reach acceptable levels of risk
f) security incorporated as an essential element of information networks and systems
g) active prevention and detection of information security incidents
h) ensuring a comprehensive approach to information security management
i) continual reassessment of information security and making of modifications as appropriate
Benefits
Management system allows an organization to:
a) satisfy the information security requirements of customers and other stakeholders
b) improve an organization's plans and activities
c) meet the organization's information security objectives
d) comply with regulations, legislation and industry mandates
e) manage information assets in an organized way that facilitates continual improvement and adjustment to current organizational goals
The successful adoption of an ISMS allowing an organization to:
a) achieve greater assurance that its information assets are adequately protected against threats on a continual basis
b) maintain a structured and comprehensive framework for identifying and assessing information security risks, selecting and applying applicable controls, and measuring and improving their effectiveness
c) continually improve its control environment
d) effectively achieve legal and regulatory compliance
ISMS Implementation
a) identify information assets and their associated information security requirements
b) assess information security risks and treat information security risks
c) select and implement relevant controls to manage unacceptable risks
d) monitor, maintain and improve the effectiveness of controls associated with the organization's information assets
Continual improvement
The aim of continual improvement of an ISMS is to increase the probability of achieving objectives concerning the preservation of the confidentiality, availability and integrity of information
The focus of continual improvement is seeking opportunities for improvement and not assuming that existing management activities are good enough or as good as they can
Actions for improvement
a) analysing and evaluating the existing situation to identify areas for improvement
b) establishing the objectives for improvement
c) searching for possible solutions to achieve the objectives
d) evaluating these solutions and making a selection
e) implementing the selected solution
f) measuring, verifying, analysing and evaluating results of the implementation to determine that the objectives have been met
g) formalizing changes
ISMS critical success factors
a) information security policy, objectives, and activities aligned with objectives
b) an approach and framework for designing, implementing, monitoring, maintaining, and improving information security consistent with the organizational culture
c) visible support and commitment from all levels of management, especially top management
d) an understanding of information asset protection requirements achieved through the application of information security risk management (see ISO/IEC 27005)
e) an effective information security awareness, training and education programme, informing all employees and other relevant parties of their information security obligations set forth in the information security policies, standards, etc., and motivating them to act accordingly
f) an effective information security incident management process
g) an effective business continuity management approach
h) a measurement system used to evaluate performance in information security management and feedback suggestions for improvement


The ISO 27000 Family of Standards
16.08.2023
www.patreon.com/AndreyProzorov
Legend
Under development
Important
Very Important
Information security, cybersecurity and privacy protection
ISO 27001 — Information security management systems (ISMS). Requirements
ISO 27002 — Information security controls
ISO 27005 — Guidance on managing information security risks
ISO 27007 — Guidelines for information security management systems auditing
ISO 27009 — Sector-specific application of ISO/IEC 27001 — Requirements
ISO 27011 — Information security controls based on ISO/IEC 27002 for telecommunications organizations
ISO 27013 — Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1
ISO 27014 — Governance of information security
ISO 27028 — Guidance on ISO/IEC 27002 attributes
ISO 27551 — Requirements for attribute-based unlinkable entity authentication
ISO 27554 — Application of ISO 31000 for assessment of identity-related risk
ISO 27555 — Guidelines on personally identifiable information deletion
ISO 27556 — User-centric privacy preferences management framework
ISO 27557 — Application of ISO 31000:2018 for organizational privacy risk management
ISO 27559 — Privacy enhancing data de-identification framework
ISO 27701 — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines
ISO 24745 — Biometric information protection
Requirements for bodies providing audit and certification of ISMSs
ISO 27006
Part 1: General
Part 2: Privacy information management systems
Security techniques
ISO 27000 — Overview and vocabulary
ISO 27003 — ISMS. Guidance
ISO 27004 — Monitoring, measurement, analysis and evaluation
ISO 27008 — Guidelines for the assessment of information security controls
ISO 27010 — Information security management for inter-sector and inter-organizational communications
~~ISO 27015 — Information security management guidelines for financial services~~
ISO 27016 — Information security management — Organizational economics
ISO 27017 — Code of practice for information security controls based on ISO/IEC 27002 for cloud services
ISO 27018 — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
ISO 27019 — Information security controls for the energy utility industry
ISO 27021 — Competence requirements for information security management systems professionals
ISO 27022 — Guidance on information security management system processes
~~ISO 27023 — Mapping the revised editions of ISO/IEC 27001 and ISO/IEC 27002~~
ISO 27037 — Guidelines for identification, collection, acquisition and preservation of digital evidence
ISO 27038 — Specification for digital redaction
ISO 27039 — Selection, deployment and operations of intrusion detection and prevention systems (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 27070 — Requirements for establishing virtualized roots of trust
ISO 29115 — Entity authentication assurance framework
ISO 29146 — A framework for access management
Cybersecurity
ISO 27031 — Guidelines for information and communication technology readiness for business continuity
ISO 27032 — Guidelines for cybersecurity -> Guidelines for Internet security
ISO 27100 — Overview and concepts
ISO 27102 — Guidelines for cyber-insurance
ISO 27103 — Cybersecurity and ISO and IEC Standards
ISO 27109 — Cybersecurity education and training
ISO 27110 — Cybersecurity framework development guidelines
Network security
ISO 27033
Part 1: Overview and concepts
Part 2: Guidelines for the design and implementation of network security
Part 3: Reference networking scenarios — Threats, design techniques and control issues
Part 4: Securing communications between networks using security gateways
Part 5: Securing communications across networks using Virtual Private Networks (VPNs)
Part 6: Securing wireless IP network access
Part 7: Guidelines for network virtualization security
Application security
ISO 27034
Part 1: Overview and concepts
Part 2: Organization normative framework
Part 3: Application security management process
~~Part 4: Validation and verification~~
Part 5: Protocols and application security controls data structure
Part 5-1: Protocols and application security controls data structure, XML schemas
Part 6: Case studies
Part 7: Assurance prediction framework
Information security incident management
ISO 27035
Part 1: Principles and process
Part 2: Guidelines to plan and prepare for incident response
Part 3: Guidelines for ICT incident response operations
Part 4: Coordination
Supplier relationships
ISO 27036
Part 1: Overview and concepts
Part 2: Requirements
Part 3: Guidelines for information and communication technology supply chain security
Part 4: Guidelines for security of cloud services
IoT security and privacy
Guidelines — ISO 27400
Device baseline requirements — ISO 27402
Guidelines for IoT-domotics — ISO 27403
Privacy technologies
Consent record information structure — ISO 27560
Privacy operationalisation model and method for engineering (POMME) — ISO 27561
Privacy guidelines for fintech services — ISO 27562
Security and privacy in artificial intelligence use cases — Best practices — ISO 27563
Guidelines on privacy preservation based on zero knowledge proofs — ISO 27565
Age assurance systems — Framework — ISO 27566
Privacy guidelines for smart cities — ISO 27570
Privacy framework — ISO 29100
Guidelines for privacy impact assessment — ISO 29134
Code of practice for personally identifiable information protection — ISO 29151
Privacy capability assessment model — ISO 29190
Security and Privacy requirements for authentication using biometrics on mobile devices
ISO 27553
Part 1: Local modes
Part 2: Remote modes
Other
Use of ISO/IEC 27001 family of standards in Governmental / Regulatory requirements — ISO 27024
??? — additional document for ISO/IEC 27002 and ISO and IEC standards — ISO 27029
~~Big data security and privacy — Processes — ISO 27045~~
~~Big data security and privacy — Implementation guidelines — ISO 27046~~
Health informatics — Information security management in health using ISO/IEC 27002 — ISO 27799


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 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

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

#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

Attributes

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

a) Control type

When and how the control modifies the risk with regard to the occurrence of an information security incident

- #Preventive — the control that is intended to prevent the occurrence of an information security incident
- #Detective — the control acts when an information security incident occurs
- #Corrective — the control acts after an information security incident occurs

b) Information security properties

Characteristic of information the control will contribute to preserving

- #Confidentiality
- #Integrity
- #Availability

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

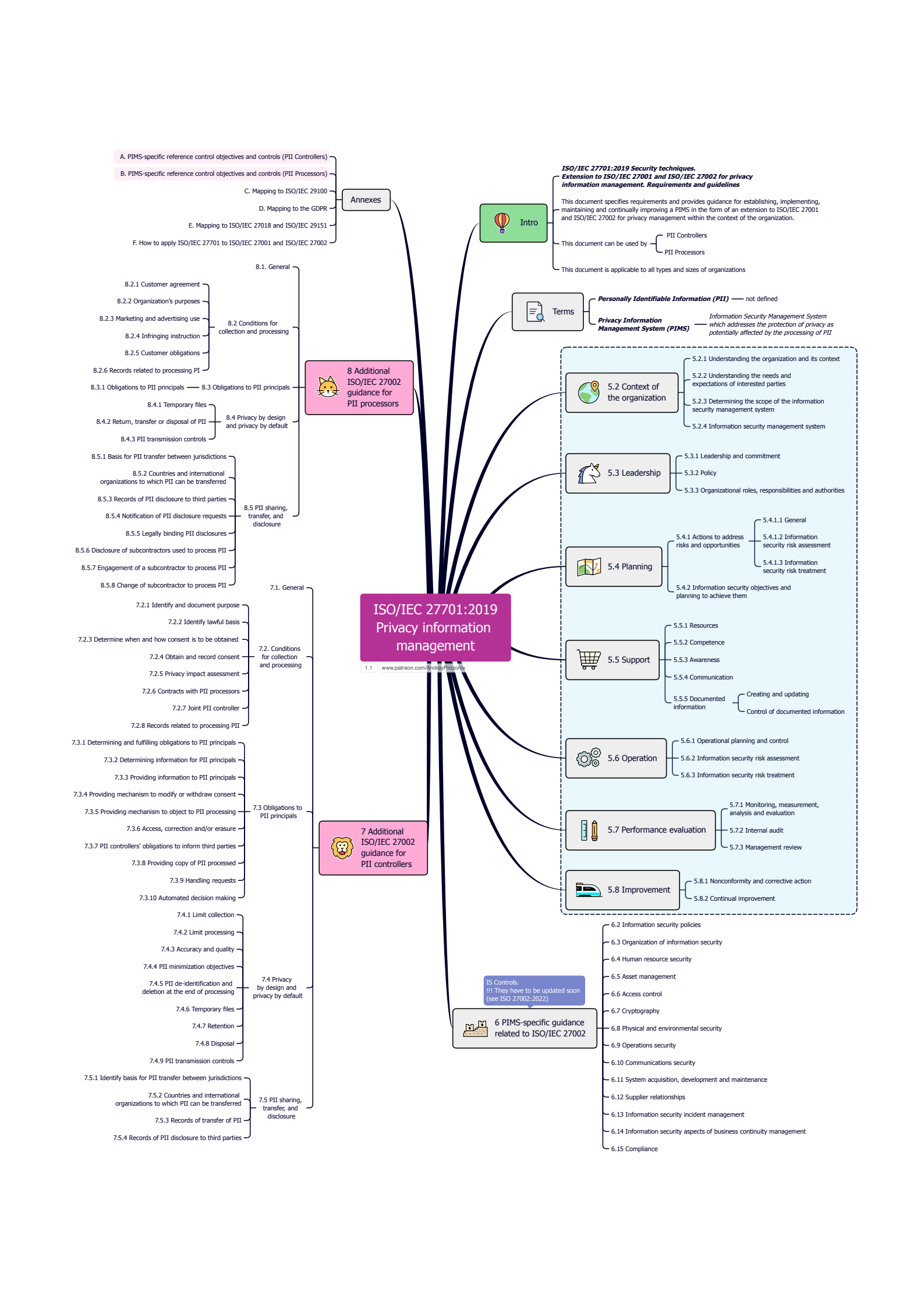
d) Operational capabilities

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

e) Security domains

- #Governance_and_Ecosystem
- #Protection
- #Defence
- #Resilience


ISO/IEC 27701:2019 Privacy information management
1.1
www.patreon.com/AndriyPrzorov
Intro
ISO/IEC 27701:2019 Security techniques. Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management. Requirements and guidelines
This document specifies requirements and provides guidance for establishing, implementing, maintaining and continually improving a 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 can be used by
PII Controllers
PII Processors
This document is applicable to all types and sizes of organizations
Terms
Personally Identifiable Information (PII) — not defined
Privacy Information Management System (PIMS) — Information Security Management System which addresses the protection of privacy as potentially affected by the processing of PII
5.2 Context of the organization
5.2.1 Understanding the organization and its context
5.2.2 Understanding the needs and expectations of interested parties
5.2.3 Determining the scope of the information security management system
5.2.4 Information security management system
5.3 Leadership
5.3.1 Leadership and commitment
5.3.2 Policy
5.3.3 Organizational roles, responsibilities and authorities
5.4 Planning
5.4.1 Actions to address risks and opportunities
5.4.1.1 General
5.4.1.2 Information security risk assessment
5.4.1.3 Information security risk treatment
5.4.2 Information security objectives and planning to achieve them
5.5 Support
5.5.1 Resources
5.5.2 Competence
5.5.3 Awareness
5.5.4 Communication
5.5.5 Documented information
Creating and updating
Control of documented information
5.6 Operation
5.6.1 Operational planning and control
5.6.2 Information security risk assessment
5.6.3 Information security risk treatment
5.7 Performance evaluation
5.7.1 Monitoring, measurement, analysis and evaluation
5.7.2 Internal audit
5.7.3 Management review
5.8 Improvement
5.8.1 Nonconformity and corrective action
5.8.2 Continual improvement
6 PIMS-specific guidance related to ISO/IEC 27002
IS Controls.
!!! They have to be updated soon (see ISO 27002:2022)
6.2 Information security policies
6.3 Organization of information security
6.4 Human resource security
6.5 Asset management
6.6 Access control
6.7 Cryptography
6.8 Physical and environmental security
6.9 Operations security
6.10 Communications security
6.11 System acquisition, development and maintenance
6.12 Supplier relationships
6.13 Information security incident management
6.14 Information security aspects of business continuity management
6.15 Compliance
7 Additional ISO/IEC 27002 guidance for PII controllers
7.1. General
7.2. Conditions for collection and processing
7.2.1 Identify and document purpose
7.2.2 Identify lawful basis
7.2.3 Determine when and how consent is to be obtained
7.2.4 Obtain and record consent
7.2.5 Privacy impact assessment
7.2.6 Contracts with PII processors
7.2.7 Joint PII controller
7.2.8 Records related to processing PII
7.3 Obligations to PII principals
7.3.1 Determining and fulfilling obligations to PII principals
7.3.2 Determining information for PII principals
7.3.3 Providing information to PII principals
7.3.4 Providing mechanism to modify or withdraw consent
7.3.5 Providing mechanism to object to PII processing
7.3.6 Access, correction and/or erasure
7.3.7 PII controllers' obligations to inform third parties
7.3.8 Providing copy of PII processed
7.3.9 Handling requests
7.3.10 Automated decision making
7.4 Privacy by design and privacy by default
7.4.1 Limit collection
7.4.2 Limit processing
7.4.3 Accuracy and quality
7.4.4 PII minimization objectives
7.4.5 PII de-identification and deletion at the end of processing
7.4.6 Temporary files
7.4.7 Retention
7.4.8 Disposal
7.4.9 PII transmission controls
7.5 PII sharing, transfer, and disclosure
7.5.1 Identify basis for PII transfer between jurisdictions
7.5.2 Countries and international organizations to which PII can be transferred
7.5.3 Records of transfer of PII
7.5.4 Records of PII disclosure to third parties
8 Additional ISO/IEC 27002 guidance for PII processors
8.1. General
8.2 Conditions for collection and processing
8.2.1 Customer agreement
8.2.2 Organization's purposes
8.2.3 Marketing and advertising use
8.2.4 Infringing instruction
8.2.5 Customer obligations
8.2.6 Records related to processing PI
8.3 Obligations to PII principals
8.3.1 Obligations to PII principals
8.4 Privacy by design and privacy by default
8.4.1 Temporary files
8.4.2 Return, transfer or disposal of PII
8.4.3 PII transmission controls
8.5 PII sharing, transfer, and disclosure
8.5.1 Basis for PII transfer between jurisdictions
8.5.2 Countries and international organizations to which PII can be transferred
8.5.3 Records of PII disclosure to third parties
8.5.4 Notification of PII disclosure requests
8.5.5 Legally binding PII disclosures
8.5.6 Disclosure of subcontractors used to process PII
8.5.7 Engagement of a subcontractor to process PII
8.5.8 Change of subcontractor to process PII
Annexes
A. PIMS-specific reference control objectives and controls (PII Controllers)
B. PIMS-specific reference control objectives and controls (PII Processors)
C. Mapping to ISO/IEC 29100
D. Mapping to the GDPR
E. Mapping to ISO/IEC 27018 and ISO/IEC 29151
F. How to apply ISO/IEC 27701 to ISO/IEC 27001 and ISO/IEC 27002

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

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

Control: measure that maintains and/or modifies risk