ช่วงสุดท้ายของการเปลี่ยนผ่านเวอร์ชั่นของ ISO/IEC 27001

BSI Group (Thailand)

Discussion items

- สรุปภาพรวม ISO/IEC 27001:2022

- ภาพรวมการเปลี่ยนแปลง และเทคนิคการ implement การเปลี่ยนแปลงข้อ 4-10

- ภาพรวมการเปลี่ยนแปลง เทคนิคการ implement การเปลี่ยนแปลง control

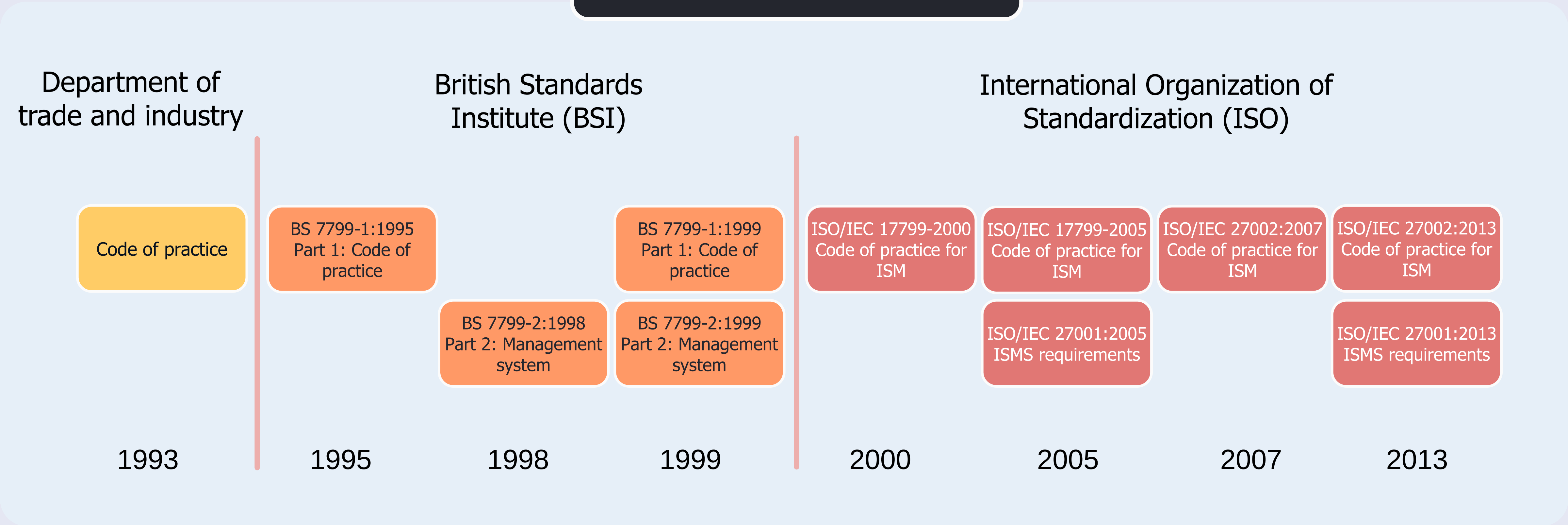
- Transitioning your ISO/IEC 27001:2013 ISMS

- สรุปภาพรวม

  ISO/IEC 27001:2022

History of ISO/IEC 27001 and ISO/IEC 27002

BS 7799 to ISO/IEC 27001



Department of trade and industry

British Standards Institute (BSI)

International Organization of Standardization (ISO)

1993

Code of practice

1995

BS 7799-1:1995 Part 1: Code of practice

1998

BS 7799-2:1998 Part 2: Management system

1999

BS 7799-1:1999 Part 1: Code of practice

BS 7799-2:1999 Part 2: Management system

2000

ISO/IEC 17799-2000 Code of practice for ISM

2005

ISO/IEC 17799-2005 Code of practice for ISM

ISO/IEC 27001:2005 ISMS requirements

2007

ISO/IEC 27002:2007 Code of practice for ISM

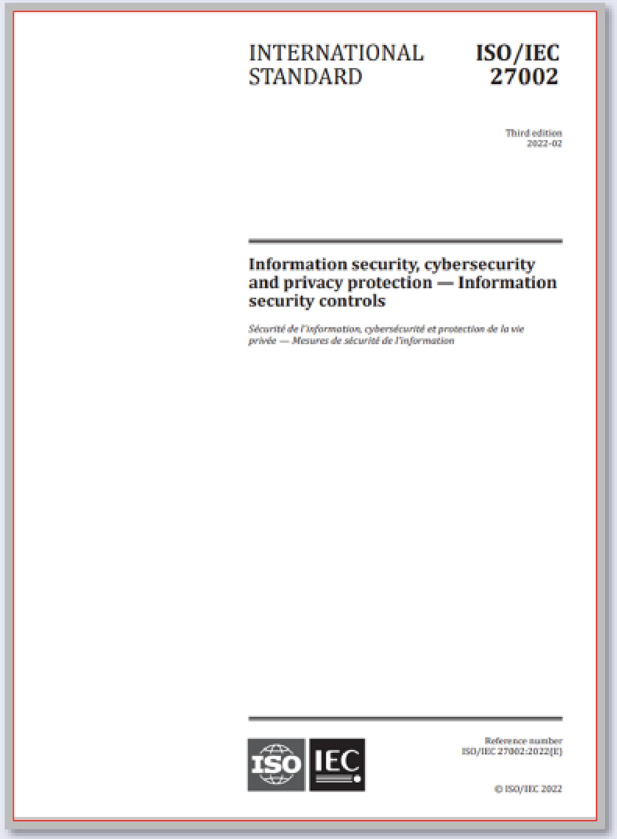
2013

ISO/IEC 27002:2013 Code of practice for ISM

ISO/IEC 27001:2013 ISMS requirements

New Chapter of ISO/IEC 27001:2022 and ISO/IEC 27002:2022

February 2022



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

October 2022

INTERNATIONAL STANDARD

ISO/IEC 27001

Third edition
2022-10

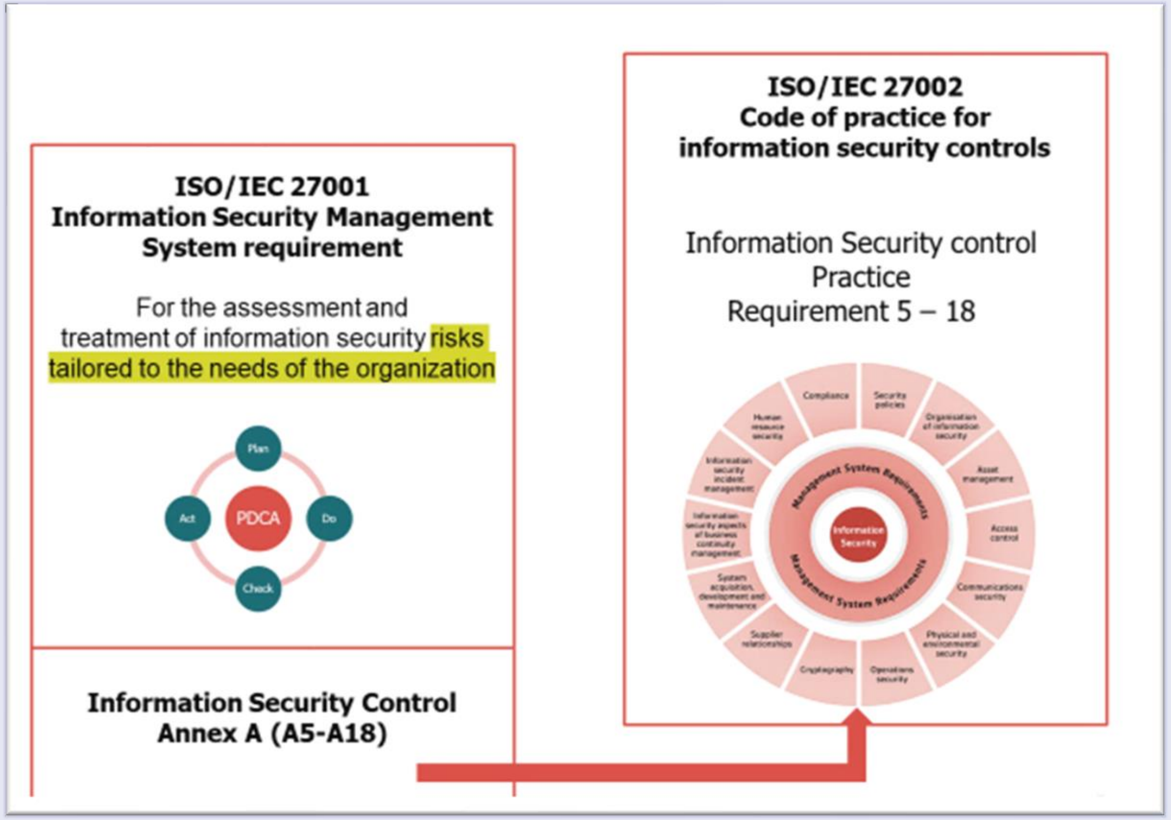
Information security, cybersecurity and privacy protection — Information security management systems — Requirements

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

ผลกระทบของการเปลี่ยนแปลง ISO/IEC 27002 ต่อ ISO/IEC 27001



ISO/IEC 27001
Information Security Management System requirement

For the assessment and treatment of information security risks tailored to the needs of the organization

Information Security Control
Annex A (A5-A18)

ISO/IEC 27002
Code of practice for information security controls

Information Security control
Practice
Requirement 5 – 18

Compliance
Security policies
Organisation of information security
Asset management
Access control
Communications security
Physical and environmental security
Operations security
Cryptography
Supplier relationships
System acquisition, development and maintenance
Information security aspects of business continuity management
Information security incident management
Human resource security
Management System Requirements
Management System Requirements
Information Security

Changed

ISO/IEC 27002

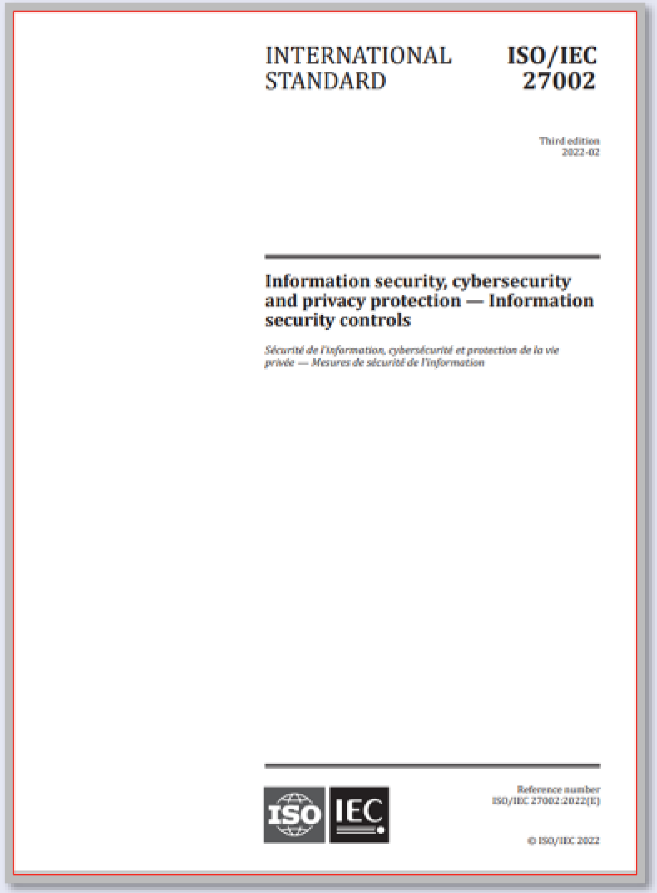
Information security, cybersecurity and privacy protection — Information security controls

Version 2022

Changed in Security control

New Chapter of ISO/IEC 27001:2022 and ISO/IEC 27002:2022

February 2022



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

October 2022

INTERNATIONAL STANDARD

ISO/IEC 27001

Third edition
2022-10

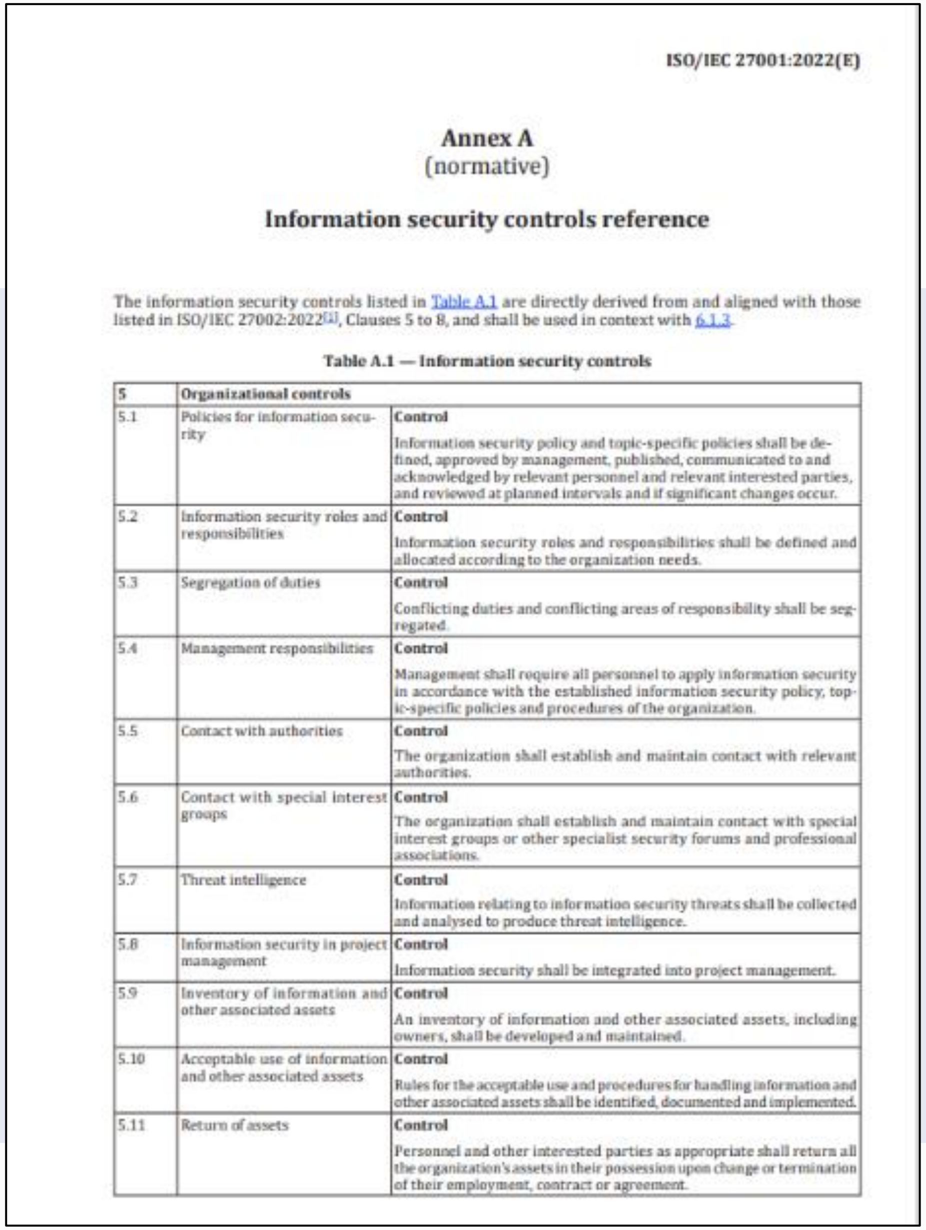
Information security, cybersecurity and privacy protection — Information security management systems — Requirements

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

Example of Annex A



ISO/IEC 27001:2022(E)

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.
5.3	Segregation of duties	**Control** Conflicting duties and conflicting areas of responsibility shall be segregated.
5.4	Management responsibilities	**Control** Management shall require all personnel to apply information security in accordance with the established information security policy, topic-specific policies and procedures of the organization.
5.5	Contact with authorities	**Control** The organization shall establish and maintain contact with relevant authorities.
5.6	Contact with special interest groups	**Control** The organization shall establish and maintain contact with special interest groups or other specialist security forums and professional associations.
5.7	Threat intelligence	**Control** Information relating to information security threats shall be collected and analysed to produce threat intelligence.
5.8	Information security in project management	**Control** Information security shall be integrated into project management.
5.9	Inventory of information and other associated assets	**Control** An inventory of information and other associated assets, including owners, shall be developed and maintained.
5.10	Acceptable use of information and other associated assets	**Control** Rules for the acceptable use and procedures for handling information and other associated assets shall be identified, documented and implemented.
5.11	Return of assets	**Control** Personnel and other interested parties as appropriate shall return all the organization's assets in their possession upon change or termination of their employment, contract or agreement.

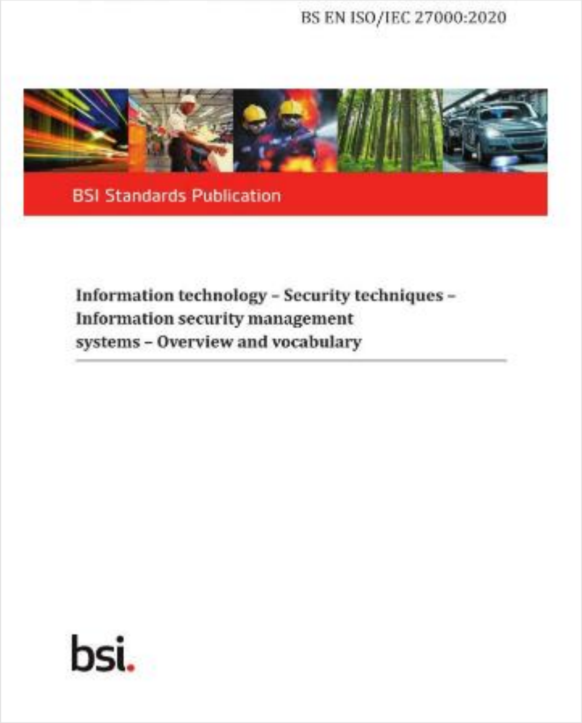
Who was involved in its development?

International Organization for Standardization

International Electrotechnical Commission

Joint technical committee ISO/IEC JTC 1

ISO standards for information security management

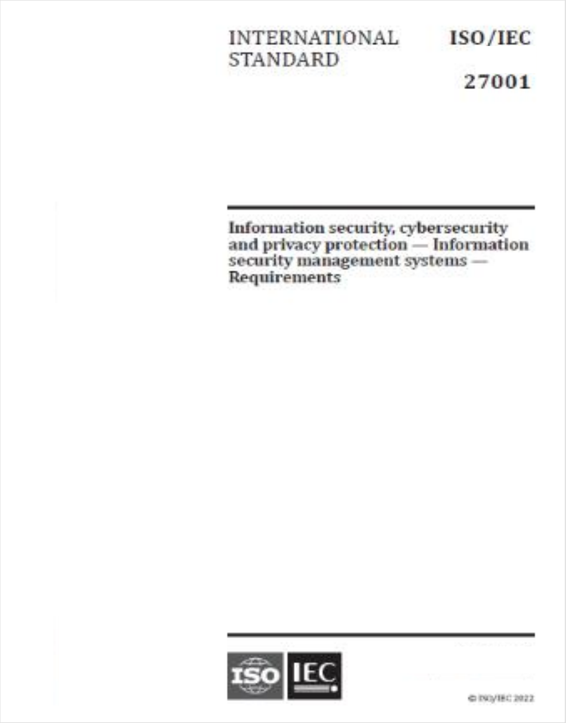


BS EN ISO/IEC 27000:2020

BSI Standards Publication

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

bsi.



INTERNATIONAL STANDARD

ISO/IEC 27001

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

© ISO/IEC 2022

INTERNATIONAL STANDARD

ISO/IEC 27002

Third edition 2022-02

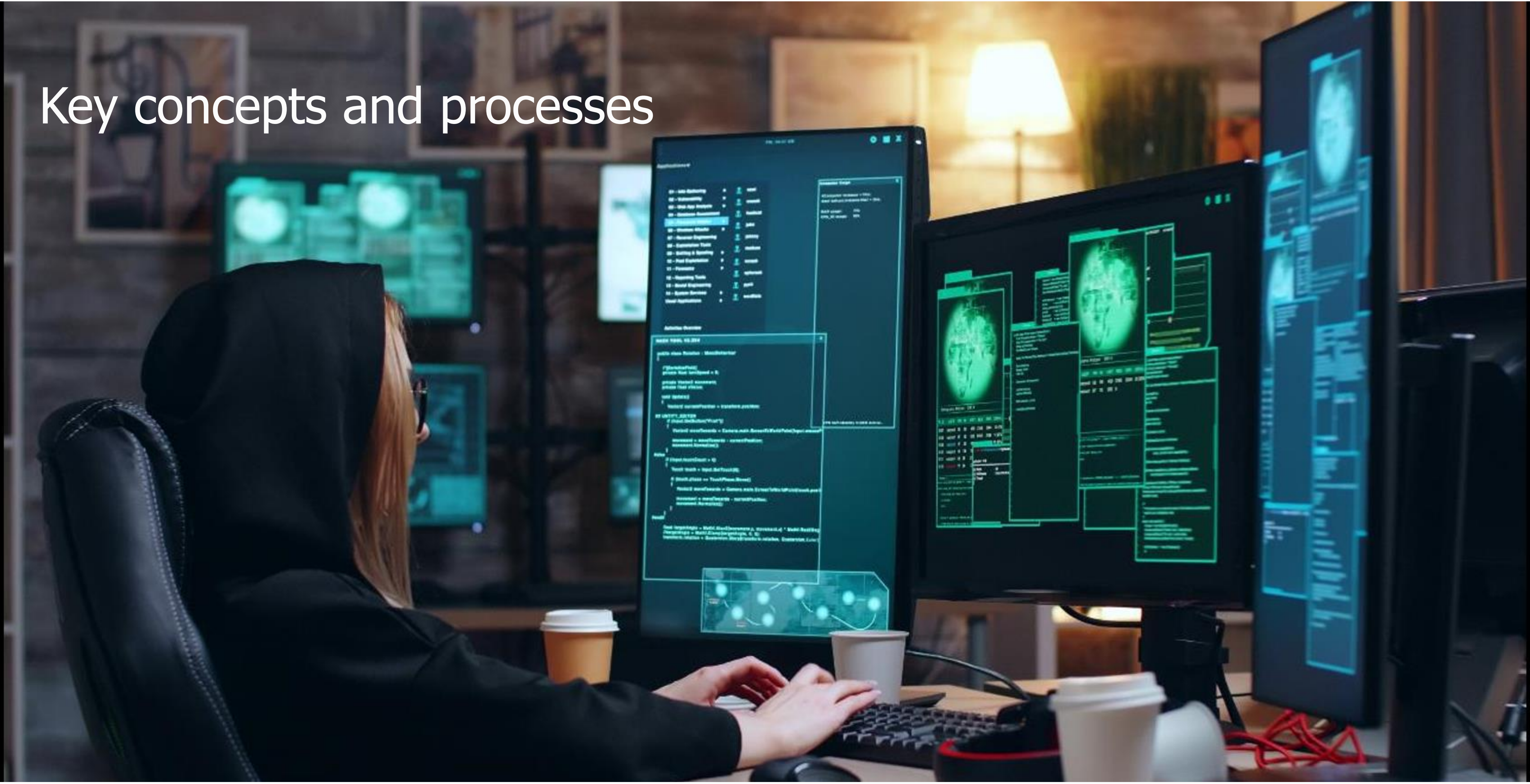
Information security, cybersecurity and privacy protection — Information security controls

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

Reference number ISO/IEC 27002:2022(E)

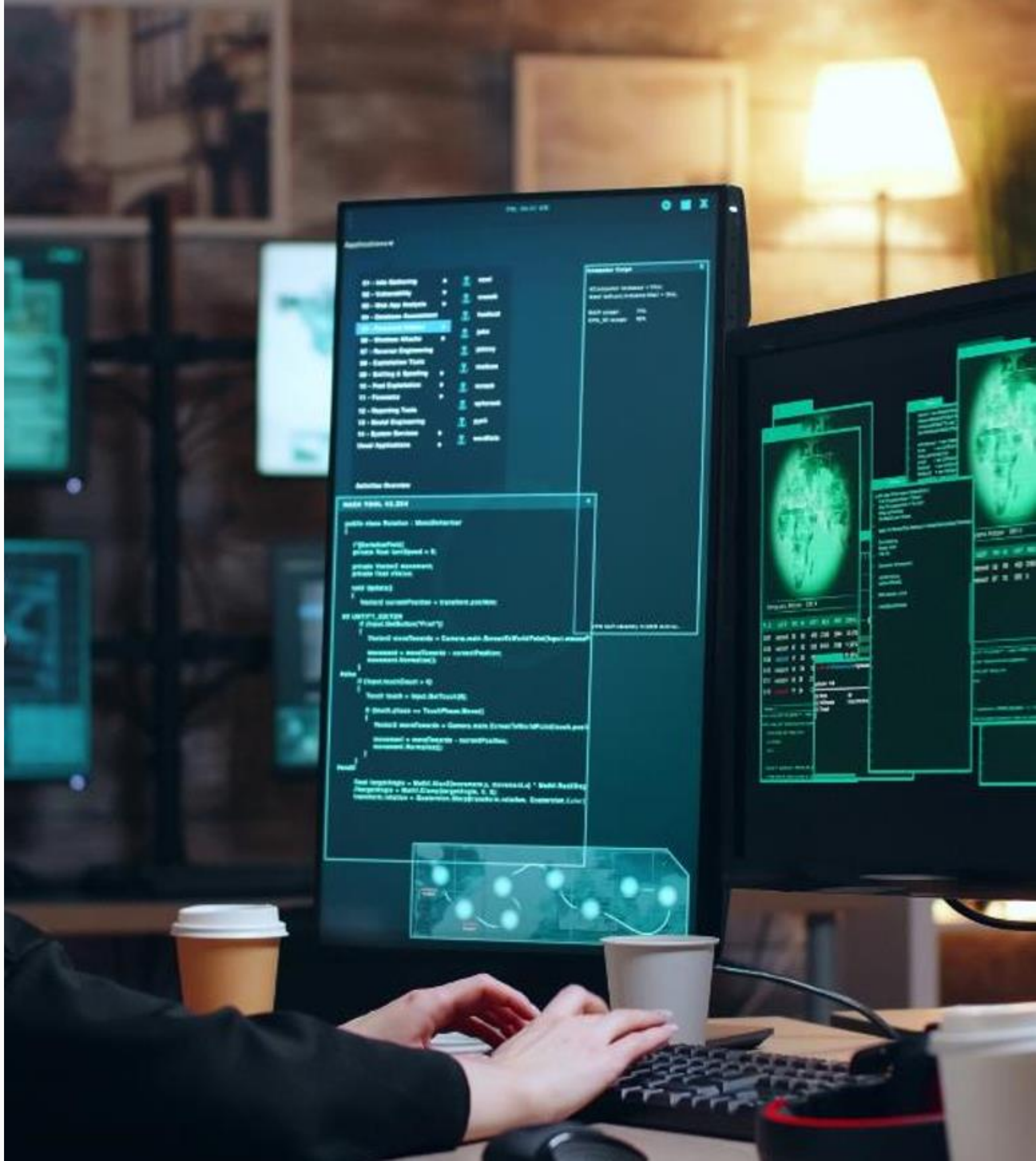
© ISO/IEC 2022

Key concepts and processes



Key concepts: Risk-based thinking

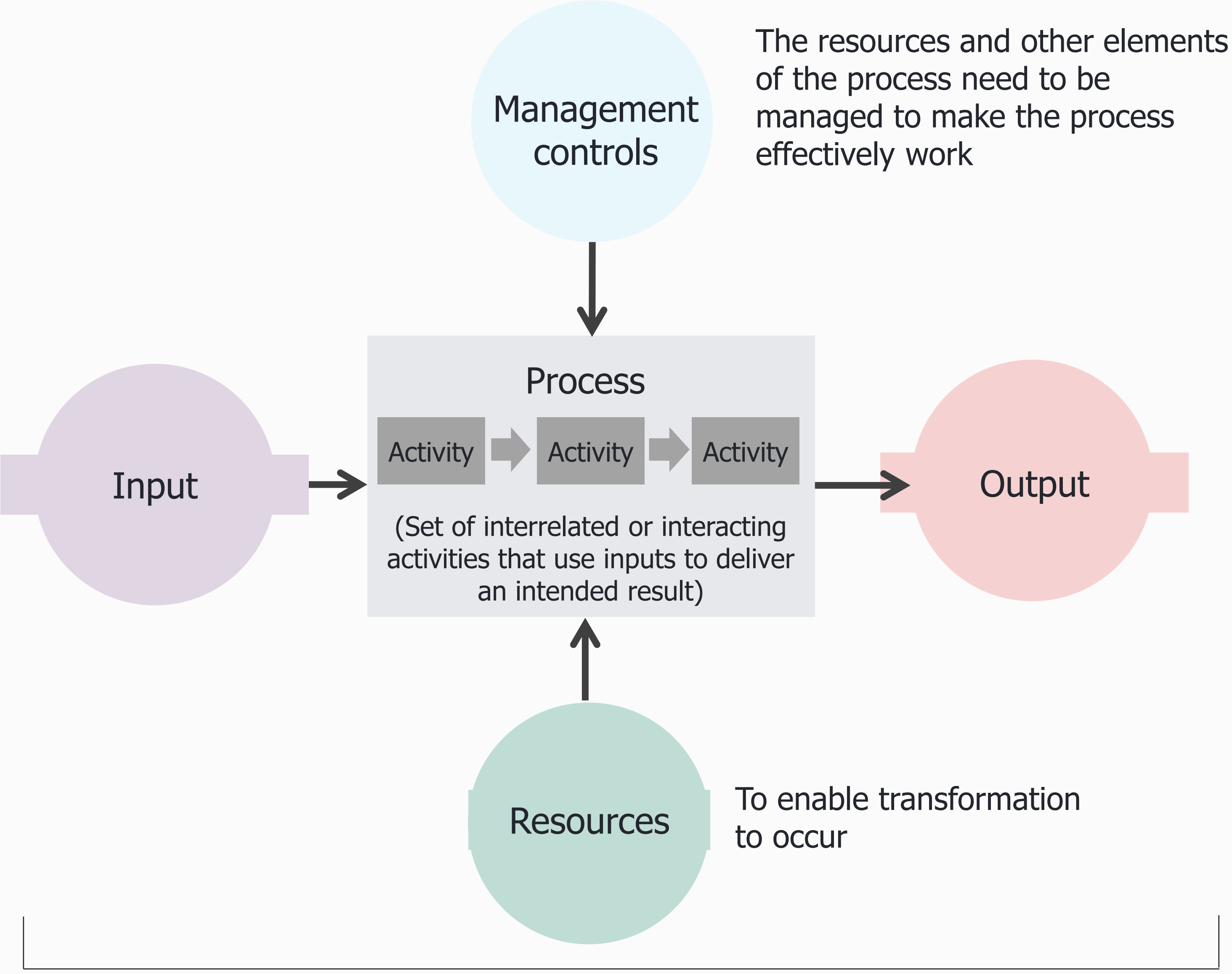
- Risk is the '**effect** of **uncertainty on objectives**'
- One of the purposes of an ISMS is to act as a preventive tool



What is a process?

MARIO Model: A process approach

- **M** for Management
- **A** for Activity
- **R** for Resources
- **I** for Inputs and
- **O** for Outputs



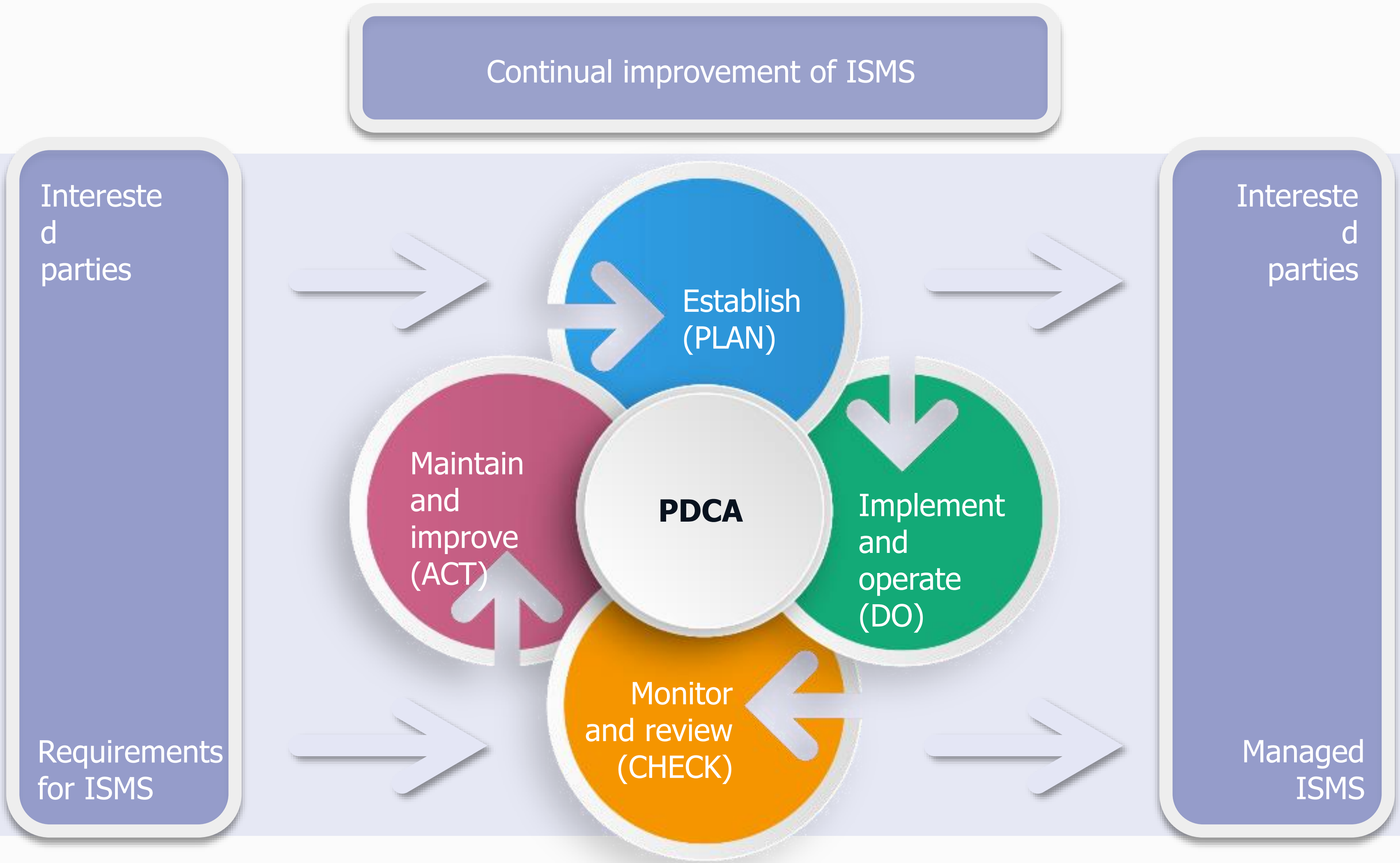
The resources and other elements of the process need to be managed to make the process effectively work

(Set of interrelated or interacting activities that use inputs to deliver an intended result)

To enable transformation to occur

Monitoring and measurement opportunities (Before, during, and after the process)

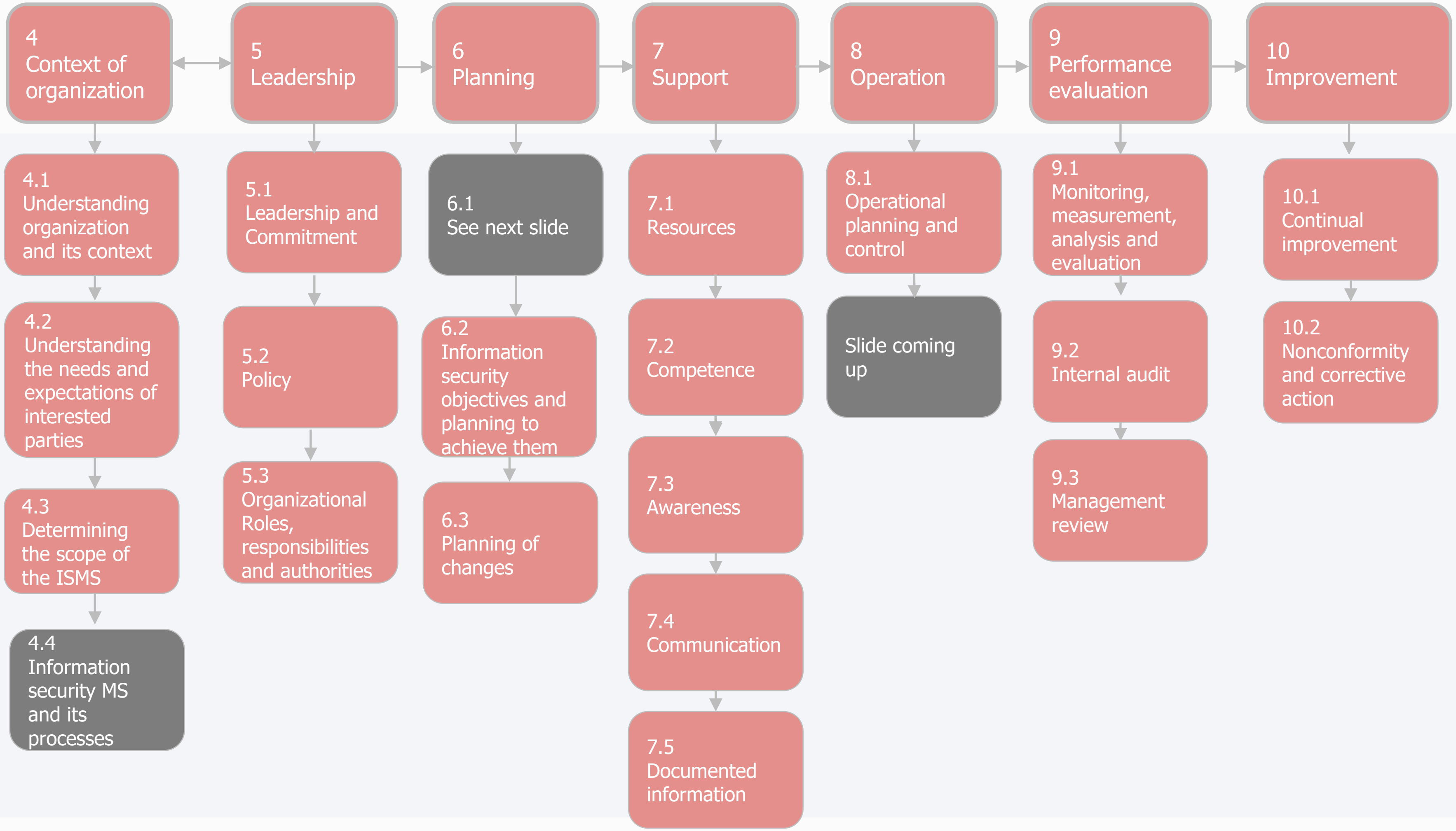
PDCA and ISMS



Key concepts: Harmonized approach

- The belief is that this will enhance consistency, make standards more generic and more easily applicable to service industries
- The harmonized approach forms the core of ISO management system standards, including ISO/IEC 27001

The harmonized approach with ISMS additions



4 Context of organization

4.1 Understanding organization and its context

4.2 Understanding the needs and expectations of interested parties

4.3 Determining the scope of the ISMS

4.4 Information security MS and its processes

5 Leadership

5.1 Leadership and Commitment

5.2 Policy

5.3 Organizational Roles, responsibilities and authorities

6 Planning

6.1 See next slide

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

Slide coming up

9 Performance evaluation

9.1 Monitoring, measurement, analysis and evaluation

9.2 Internal audit

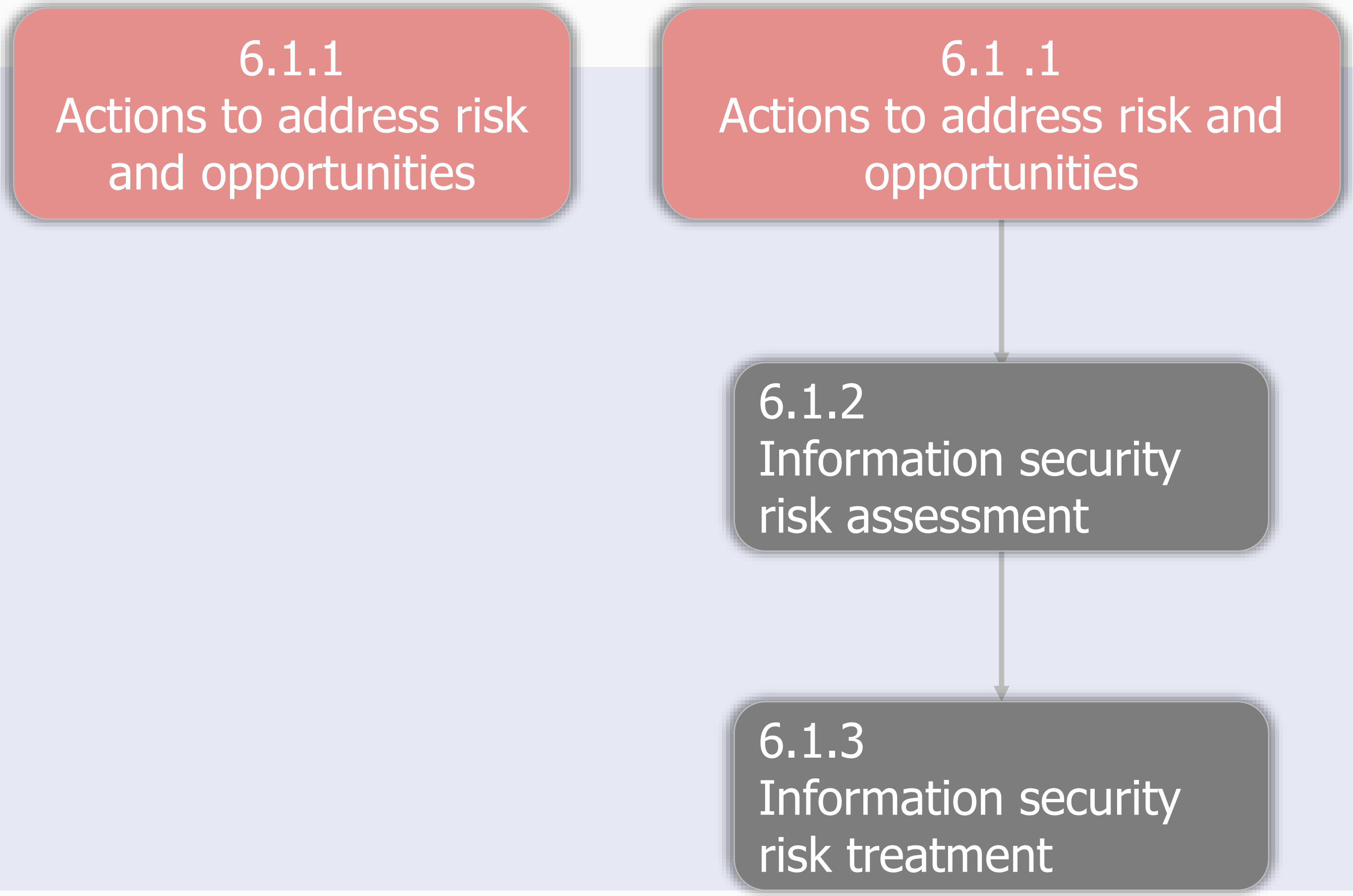
9.3 Management review

10 Improvement

10.1 Continual improvement

10.2 Nonconformity and corrective action

The harmonized approach with ISMS additions Clause 6.1



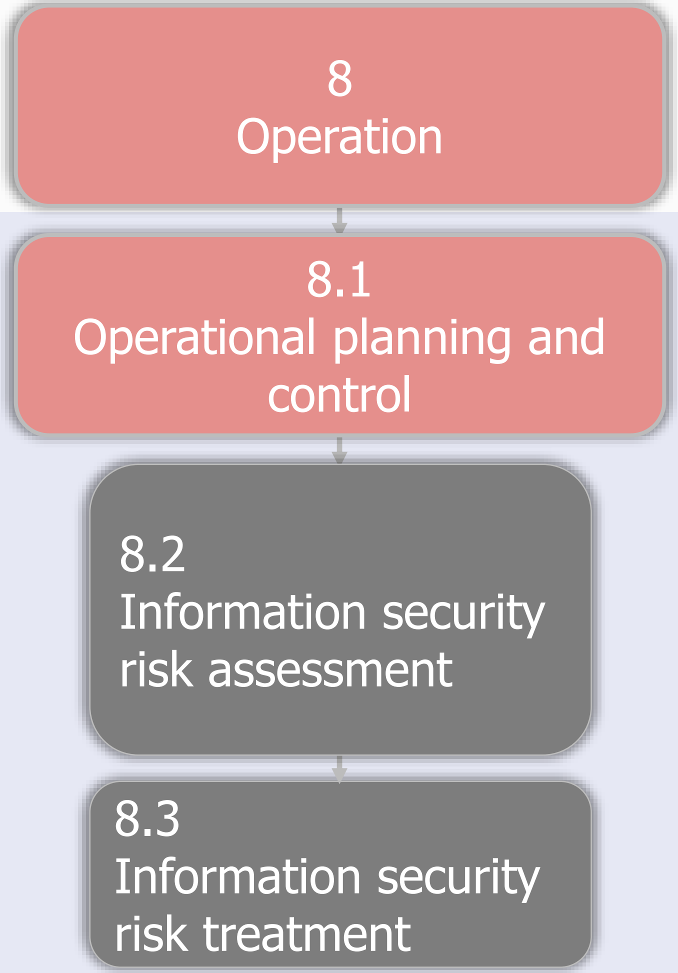
6.1.1
Actions to address risk and opportunities

6.1 .1
Actions to address risk and opportunities

6.1.2
Information security risk assessment

6.1.3
Information security risk treatment

The harmonized approach with ISMS additions Clause 8


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

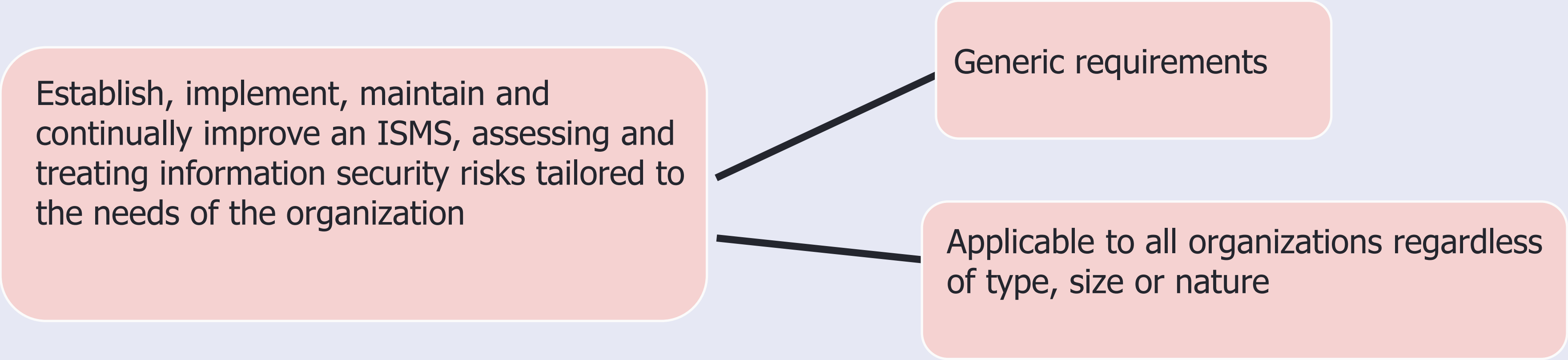
Introduction to ISO/IEC 27001

Introduction

1 Scope

2 Normative references

3 Terms and definitions



Establish, implement, maintain and continually improve an ISMS, assessing and treating information security risks tailored to the needs of the organization

Generic requirements

Applicable to all organizations regardless of type, size or nature

All requirements in Clauses 4 to 10 are to be implemented to claim conformity

Introduction to ISO/IEC 27001

Introduction

1 Scope

2 Normative references

3 Terms and definitions

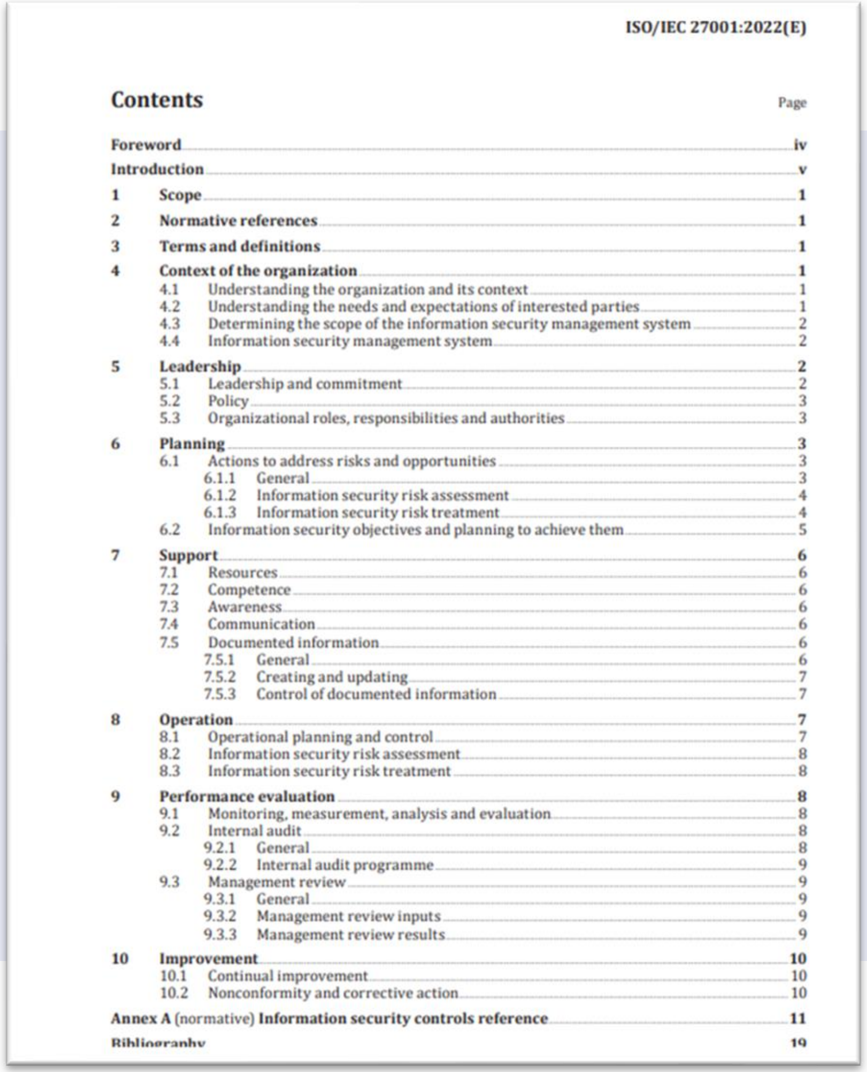
Normative references cites ISO/IEC 27000:2018 as indispensable for its application

Introduction to ISO/IEC 27001

Introduction 1 Scope 2 Normative references **3 Terms and definitions**

Terms, definitions and concepts used in ISO/IEC 27000

Introduction to ISO/IEC 27001

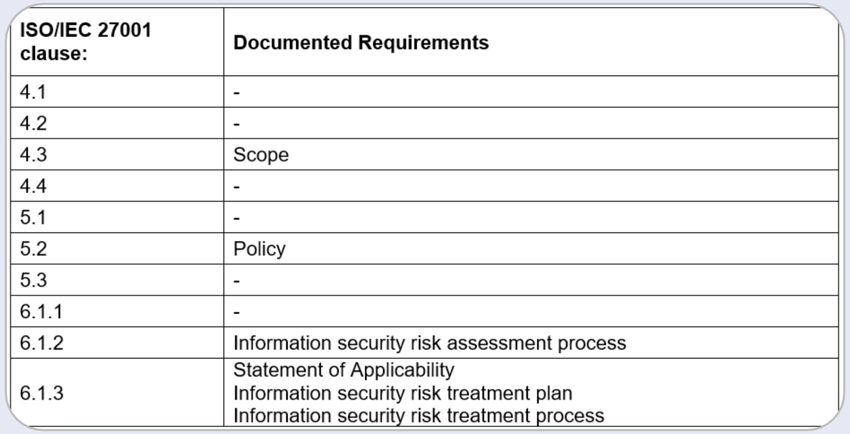


ISO/IEC 27001:2022(E)

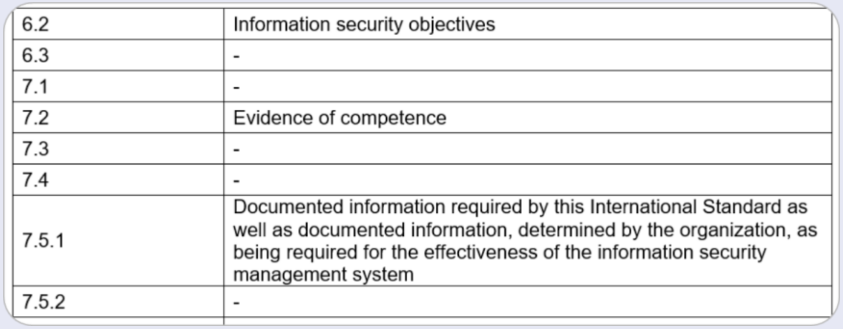
Contents

Page

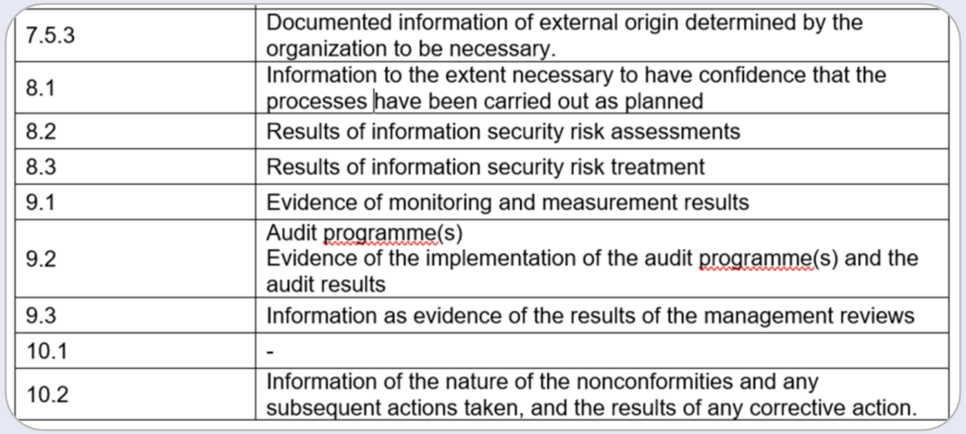
Minimum Document Requirement in ISO/IEC 27001:2022



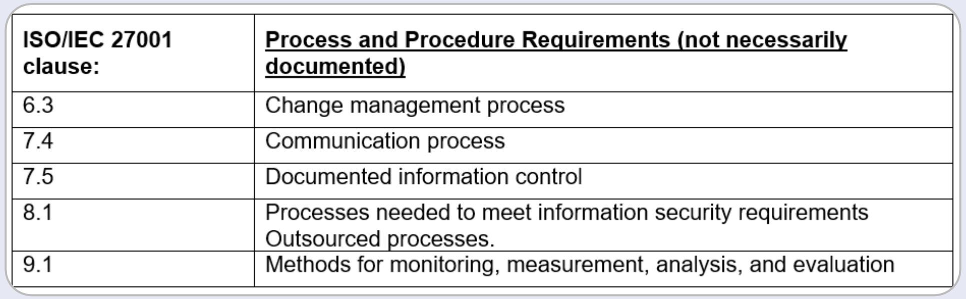
ISO/IEC 27001 clause:	Documented Requirements
4.1	-
4.2	-
4.3	Scope
4.4	-
5.1	-
5.2	Policy
5.3	-
6.1.1	-
6.1.2	Information security risk assessment process
6.1.3	Statement of Applicability Information security risk treatment plan Information security risk treatment process



6.2	Information security objectives
6.3	-
7.1	-
7.2	Evidence of competence
7.3	-
7.4	-
7.5.1	Documented information required by this International Standard as well as documented information, determined by the organization, as being required for the effectiveness of the information security management system
7.5.2	-



7.5.3	Documented information of external origin determined by the organization to be necessary.
8.1	Information to the extent necessary to have confidence that the processes have been carried out as planned
8.2	Results of information security risk assessments
8.3	Results of information security risk treatment
9.1	Evidence of monitoring and measurement results
9.2	Audit programme(s) Evidence of the implementation of the audit programme(s) and the audit results
9.3	Information as evidence of the results of the management reviews
10.1	-
10.2	Information of the nature of the nonconformities and any subsequent actions taken, and the results of any corrective action.



ISO/IEC 27001 clause:	**Process and Procedure Requirements (not necessarily documented)**
6.3	Change management process
7.4	Communication process
7.5	Documented information control
8.1	Processes needed to meet information security requirements Outsourced processes.
9.1	Methods for monitoring, measurement, analysis, and evaluation

- ภาพรวมการเปลี่ยนแปลง และเทคนิคการ implement การเปลี่ยนแปลงข้อ 4-10

nurl:/admin/login.asp
inurl:/cgi-bin/sqwebmail?
inurl:/Citrix/Nfuse17/
inurl:/dana-na/auth/welcom
inurl:/eprise/
inurl:/Merchant2/admin.mv
inurl:/modcp/ intext:Modera
inurl:/SUSAdmin intitle:"Mi
inurl:/webedit.* intext:Web
inurl:1810 "Oracle Enterpri
inurl:2000 intitle:RemotelyA
inurl::2082/frontend -demo

ISO/IEC 27001:2022 change highlights

- International Standard’ replaced with document throughout’
- Re-arranging of some English to allow for easier translation
- Minor numbering re-structure to align with the harmonized approach
- Requirement to **define your process needs** and their **interactions** as part of your ISMS
- Explicit requirement to communicate organizational roles relevant to information security within in the organization

- Removal of reference to control objectives as they no longer exist either in **Annex A or ISO/IEC 27002**
- New requirement to monitor information security objectives
- **New Clause 6.3 – Planning of changes**
- New requirement to ensure the organization determines **how to communicate** as part of Clause

- New requirements to establish **criteria for operational processes** and implementing control of the processes
- Internal audit and management review clauses aligned with harmonized approach
- Clause 10.1 Continual Improvement and Clause 10.2 now nonconformity and corrective action but requirements remain the same

Clause 4.4

Confidentiality

Integrity

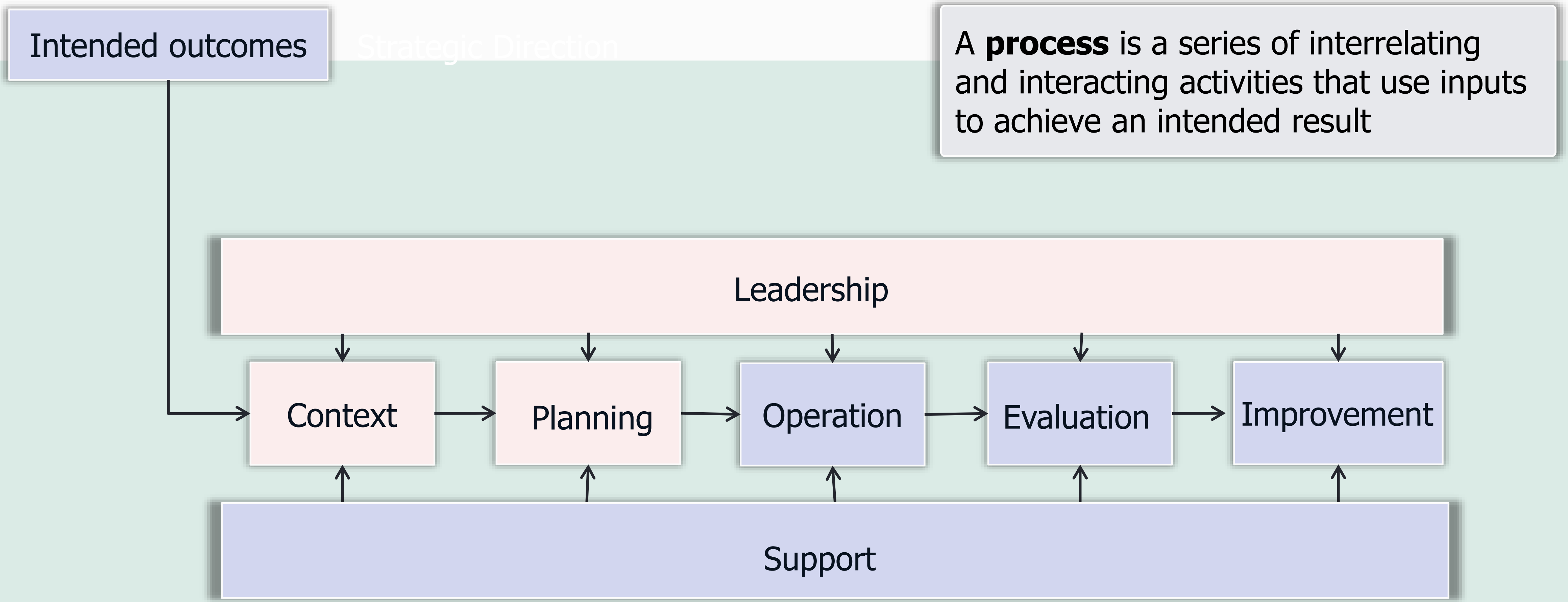
Availability

Effective implementation of the system

Internal audit

Management review

Clause 4.4

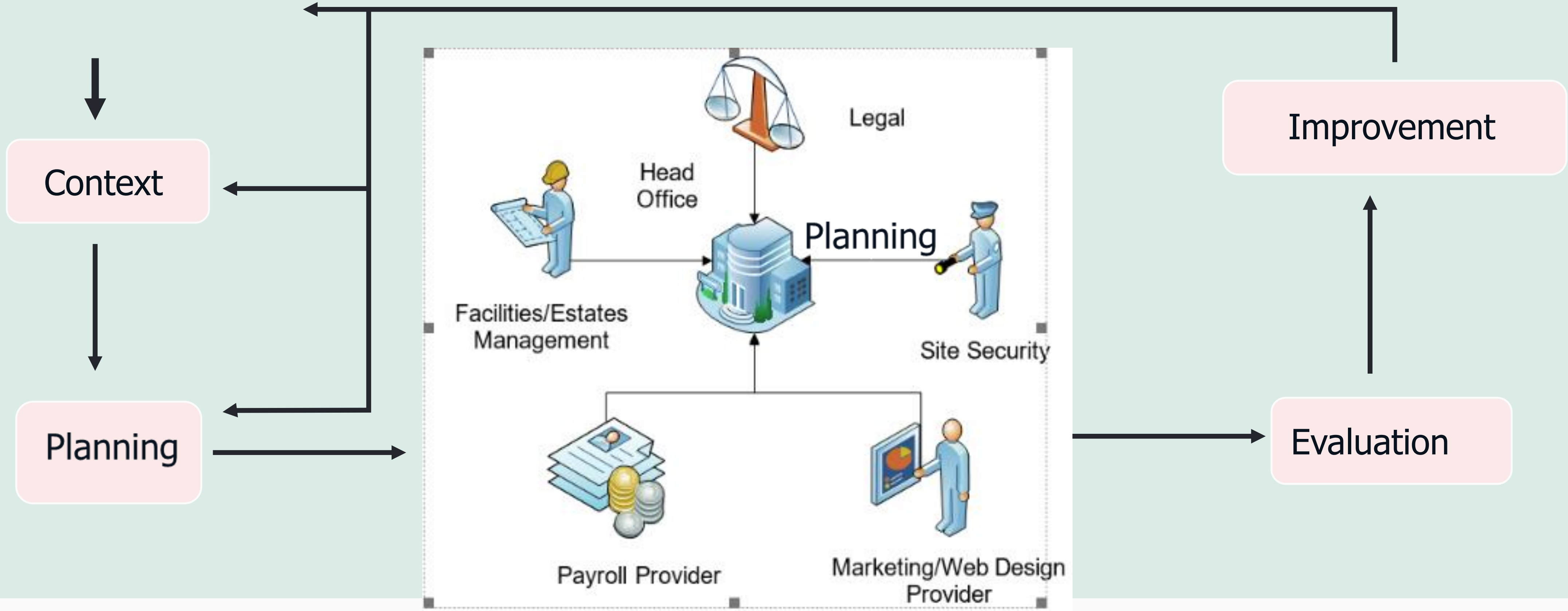


A **process** is a series of interrelating and interacting activities that use inputs to achieve an intended result

Resources Management Process

Communication Process

Document control Process



Context

Planning

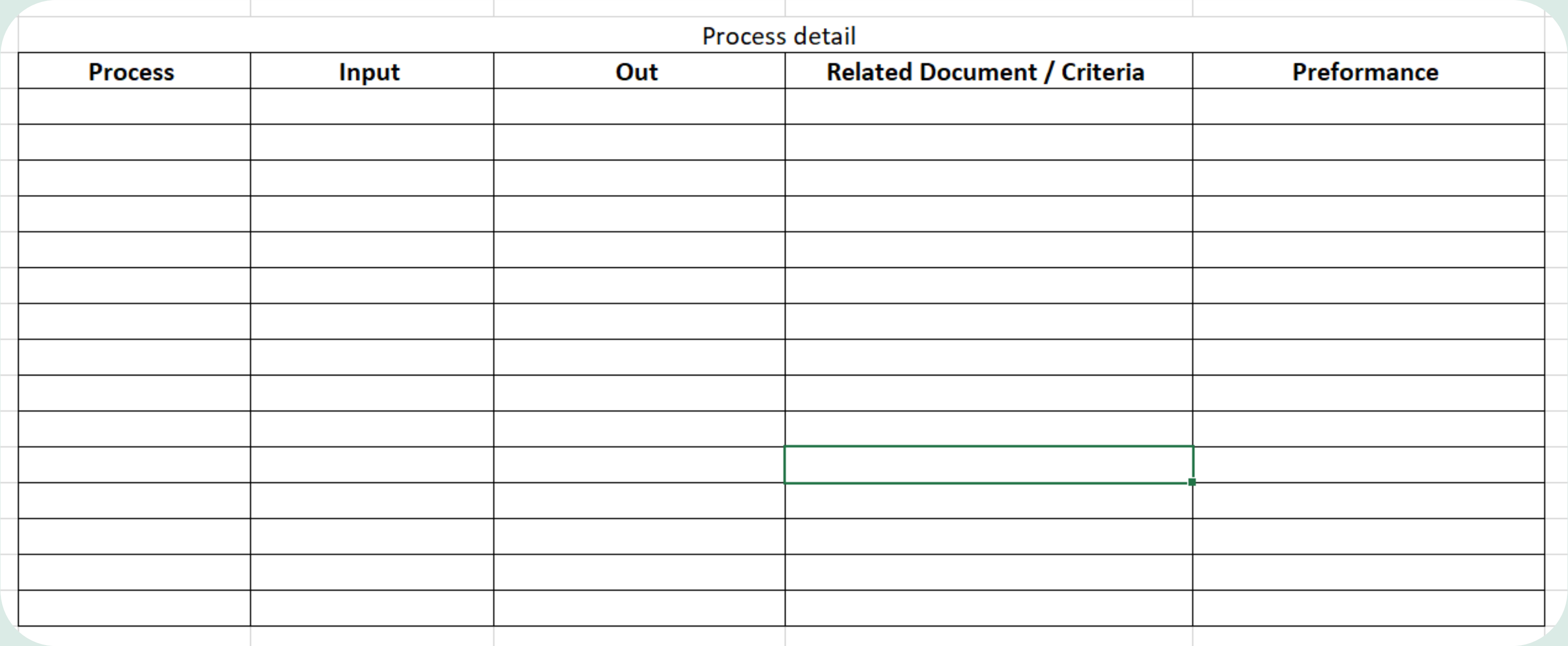
Evaluation

Improvement

Management Process

Process Detail

Example.

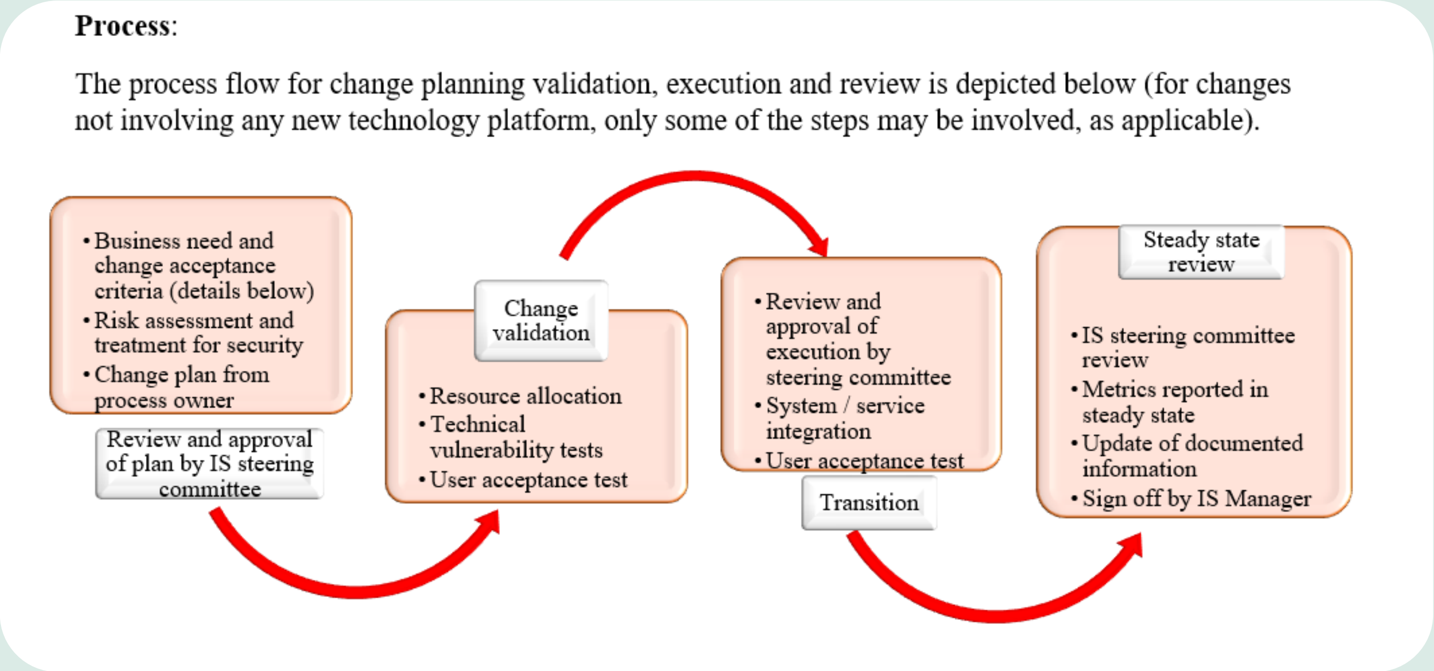


Process detail

Process	Input	Out	Related Document / Criteria	Preformance

Clause 6.3: Planning of changes

Consider the change in relevant to ISMS and implement the relevant actions



Process:

The process flow for change planning validation, execution and review is depicted below (for changes not involving any new technology platform, only some of the steps may be involved, as applicable).

- Business need and change acceptance criteria (details below)
- Risk assessment and treatment for security
- Change plan from process owner

Review and approval of plan by IS steering committee

Change validation

- Resource allocation
- Technical vulnerability tests
- User acceptance test

- Review and approval of execution by steering committee
- System / service integration
- User acceptance test

Transition

Steady state review

- IS steering committee review
- Metrics reported in steady state
- Update of documented information
- Sign off by IS Manager

Example of planning of change

- ภาพรวมการเปลี่ยนแปลงเทคนิคการ implement การเปลี่ยนแปลง control (Annex A)

ISO/IEC 27001:2022 Annex A

Clause 5
Organizational controls
37 controls, 34 existing, 3 new

Clause 6
People controls
8 controls, all existing

Clause 7
Physical controls
14 controls, 13 existing, 1 new

Clause 8
Technological controls
34 controls, 27 existing, 7 new

11 New controls

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

Updated controls

- Majority of existing controls remain relevant
- Many needed updating to reflect latest best practices and removal of obsolete technologies
- Link between corresponding control numbers

58 updated controls

ISO/IEC 27001:2013	ISO/IEC 27001:2022	ISO/IEC 27001:2013	ISO/IEC 27001:2022	ISO/IEC 27001:2013	ISO/IEC 27001:2022
A6.1.1	5.02	A18.2.1	5.35	A09.2.3	8.02
A6.1.2	5.03	A12.1.1	5.37	A09.4.1	8.03
A7.2.1	5.04	A07.1.1	6.01	A09.4.5	8.04
A6.1.3	5.05	A07.1.2	6.02	A09.4.2	8.05
A6.1.4	5.06	A07.2.2	6.03	A12.1.3	8.06
A8.1.4	5.11	A07.2.3	6.04	A12.2.1	8.07
A8.2.1	5.12	A07.3.1	6.05	A12.3.1	8.13
A8.2.2	5.13	A13.2.4	6.06	A17.2.1	8.14
A9.2.1	5.16	A06.2.2	6.07	A12.4.4	8.17
A15.1.1	5.19	A11.1.1	7.01	A09.4.4	8.18
A15.1.2	5.20	A11.1.3	7.03	A13.1.1	8.20
A15.1.3	5.21	A11.1.4	7.05	A13.1.2	8.21
A16.1.1	5.24	A11.1.5	7.06	A13.1.3	8.22
A16.1.4	5.25	A11.2.9	7.07	A14.2.1	8.25
A16.1.5	5.26	A11.2.1	7.08	A14.2.5	8.27
A16.1.6	5.27	A11.2.6	7.09	A14.2.7	8.30
A16.1.7	5.28	A11.2.2	7.11	A14.3.1	8.33
A18.1.2	5.32	A11.2.3	7.12	A12.7.1	8.34
A18.1.3	5.33	A11.2.4	7.13		
A18.1.4	5.34	A11.2.7	7.14		

Merged controls

Merged where existing controls are inseparable or closely related

24 merged controls

ISO/IEC 27001:2013	ISO/IEC 27001:2022	ISO/IEC 27001:2013	ISO/IEC 27001:2022
A05.1.1, A05.1.2	5.01	**A16.1.2, A16.1.3**	6.08
A06.1.5, A14.1.1	5.08	**A11.1.2, A11.1.6**	7.02
A08.1.1, A08.1.2	5.09	**A08.3.1, A08.3.2, A08.3.3, A11.2.5**	7.10
A08.1.3, A08.2.3	5.10	**A06.2.1, A11.2.8**	8.01
A13.2.1, A13,2,2, A13.3.3	5.14	**A12.6.1, A18.2.3**	8.08
A09.1.1, A09.2.2	5.15	**A12.4.1, A12.4.2, A12.4.3**	8.15
A09.2.4, A09.2.5, A09.2.6	5.17	**A12.5.1, A12.6.2**	8.19
A09.2.2, A09.2.5, A09.2.6	5.18	**A10.1.1, A10.1.2**	8.24
A15.1.1, A15.1.2	5.22	**A14.1.2, A14.1.3**	8.26
A17.1.1, A17.1.2, A17.1.3	5.29	**A14.2.8, A14.2.9**	8.29
A18.1.1, A18.1.5	5.31	**A12.1.4, A12.2.6**	8.31
A18.2.2, A18.2.3	5.36	**A12.1.2, A14.2.2, A14.2.3, A14.2.4**	8.32

Understanding changes to Annex A Clauses 5

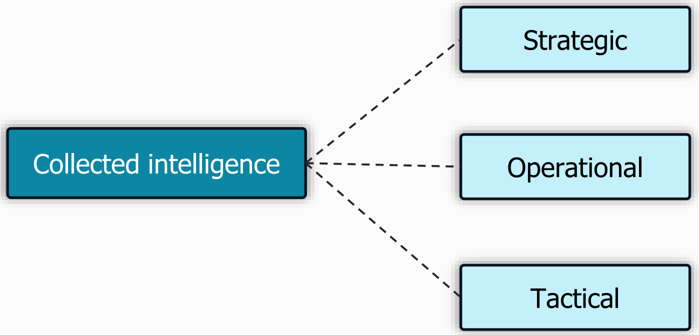
37 controls: 34 existing and 3 new

5.7	Threat intelligence
5.23	Information security for use on cloud services
5.30	ICT readiness for business continuity

Control 5.7 threat intelligence

- Intelligence should be relevant, insightful, contextual and actionable
- Establish activities to identify, vet, select, collect, process, analyze and communicate relevant information
- Consider internal and external threats

Layered threat intelligence



Control 5.23 Information security for use of cloud services

- Establish processes for acquisition, use management and exit from cloud services
- Establish and communicate a topic-specific policy
- Identify all information security requirements
- Responsibilities of the cloud service provider vs the organization
- Manage information security risks in relation to cloud services

Control 5.30 ICT readiness for business continuity

Business Impact Analysis (BIA)	Process of analysing the impact over time of a disruption on the organization
Recovery Point Objective (RPO)	Point to which information used by an activity is restored to enable the activity to operate on resumption
Recovery Time Objective (RTO)	Period of time following an incident within which a product and service or an activity is resumed, or resources are recovered

Understanding changes to Annex A Clauses 6 and Clause 7 controls

Clause 6 - People controls
8 controls, all existing

Clause 7 - Physical controls
14 controls, 13 existing, 1 new

Control 7.4 - Physical security monitoring

Consider data protection laws and regulations

Alarm unoccupied areas continuously

Security guard

All members of staff should know the position of monitoring systems to prevent false alarms

CCTV

Iris scanner

Infra-red technology can be used as a motion detector

Barrier gate

Critical systems should be monitored systems continuously

Monitoring systems should be tested monthly

Understanding changes to Annex A Clause 8

Control 8.9 Configuration management
- Processes and tools to enforce defined configurations of hardware, software, services and networks
- Use of standard templates and databases to manage configurations
- Configuration monitoring utilizing system management tools
- Integration with asset management

Control 8.10 Information deletion
- Prevent unnecessary exposure of sensitive information
- Consider deletion methods
- Record deletion
- Consider third-parties storing information on the organization's behalf

Control 8.11 data masking
- Limit the exposure of sensitive data including PII
- Consider the use of different data masking techniques to disguise the true data, including the identity of PII principals
- Consider legal, regulatory and contractual obligations when considering techniques

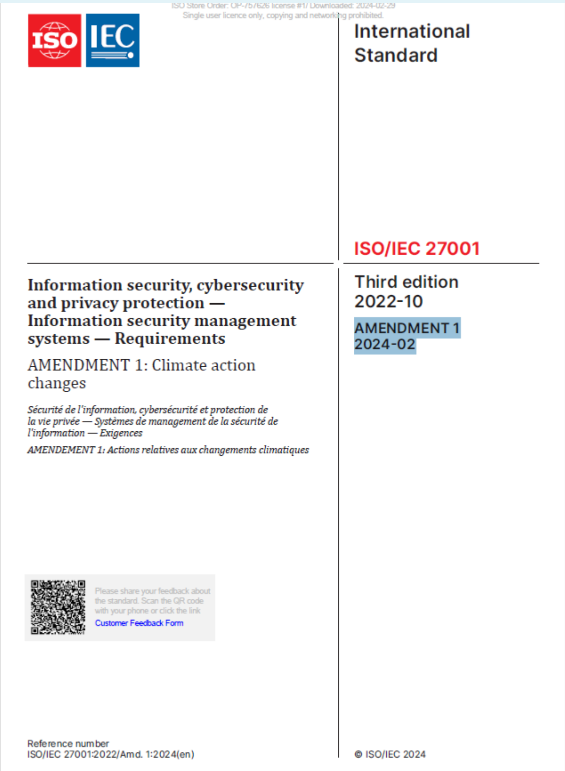
Control 8.12 Data leakage prevention
- Apply to systems, networks and any other devices that process, store or transmit sensitive information
- Identify and classify the information, monitor channels and prevent information from leaking
- Use data leakage prevention tools
- What are you protecting the information against?

Control 8.16 Monitoring activities
- Monitor network systems and applications for anomalous behaviour and evaluate potential information security incidents
- Use monitoring tools for continuous monitoring
- Have the ability to adapt to differing threats
- Alert function capability to allow abnormal events to be communicated to relevant interested parties

Control 8.23 Web filtering
- Protect systems being compromised by malware and access to unauthorized web resources
- Identify types of websites personnel should or should not have access to
- Establish rules for safe and appropriate use of online resources
- Provide training to personnel on secure and appropriate use of online resources

Control 8.28 Secure coding
- Ensure software is written securely to reduce potential information security vulnerabilities
- Establish a minimum secure baseline including third-parties and open source software
- Keep up to date on real world software threats
- Consider the whole coding life cycle including reuse

ISO/IEC 27001 - AMENDMENT 1 2024-02



International Standard

ISO/IEC 27001

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

AMENDMENT 1: Climate action changes

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

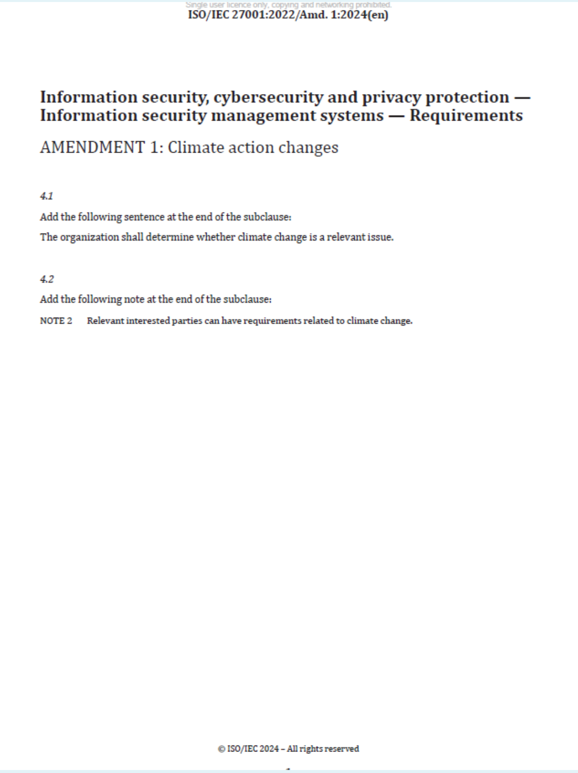
AMENDEMENT 1: Actions relatives aux changements climatiques

Third edition
2022-10

AMENDMENT 1
2024-02

Please share your feedback about the standard. Scan the QR code with your phone or click the link
Customer Feedback Form

Reference number
ISO/IEC 27001:2022/Amd. 1:2024(en)



ISO/IEC 27001:2022/Amd. 1:2024(en)

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

AMENDMENT 1: Climate action changes

4.1

Add the following sentence at the end of the subclause:

The organization shall determine whether climate change is a relevant issue.

4.2

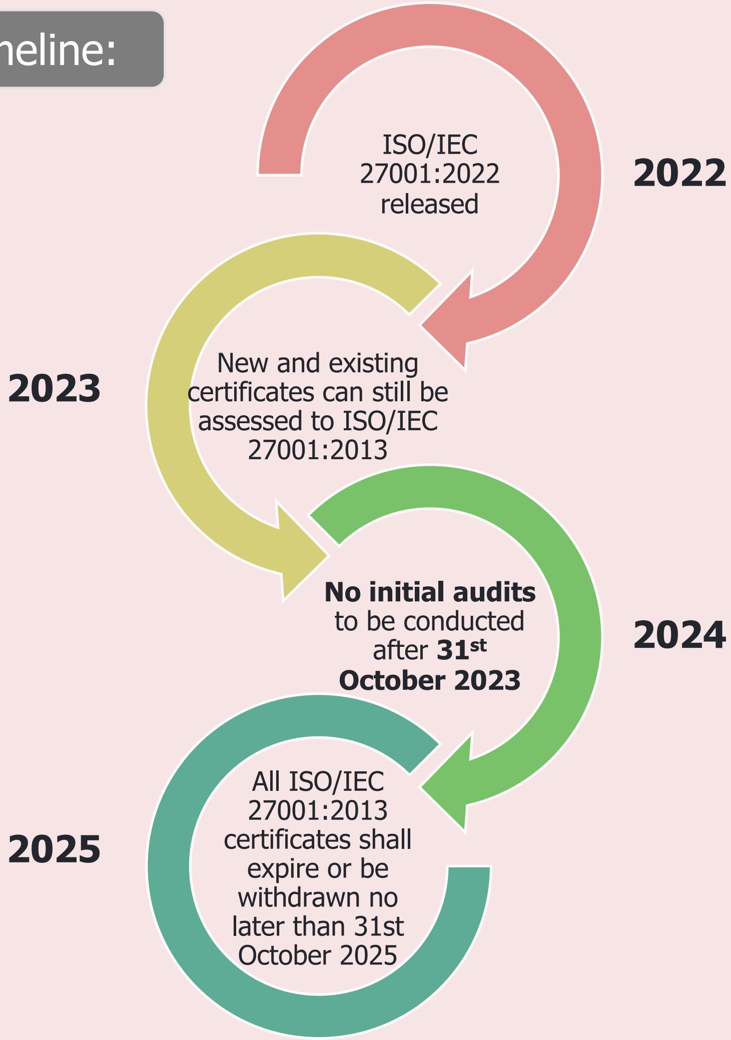
Add the following note at the end of the subclause:

NOTE 2 Relevant interested parties can have requirements related to climate change.

- Transitioning your ISO/IEC 27001:2013 ISMS

Transitioning your ISO/IEC 27001:2013 ISMS

Transition timeline:



2022

ISO/IEC 27001:2022 released

2023

New and existing certificates can still be assessed to ISO/IEC 27001:2013

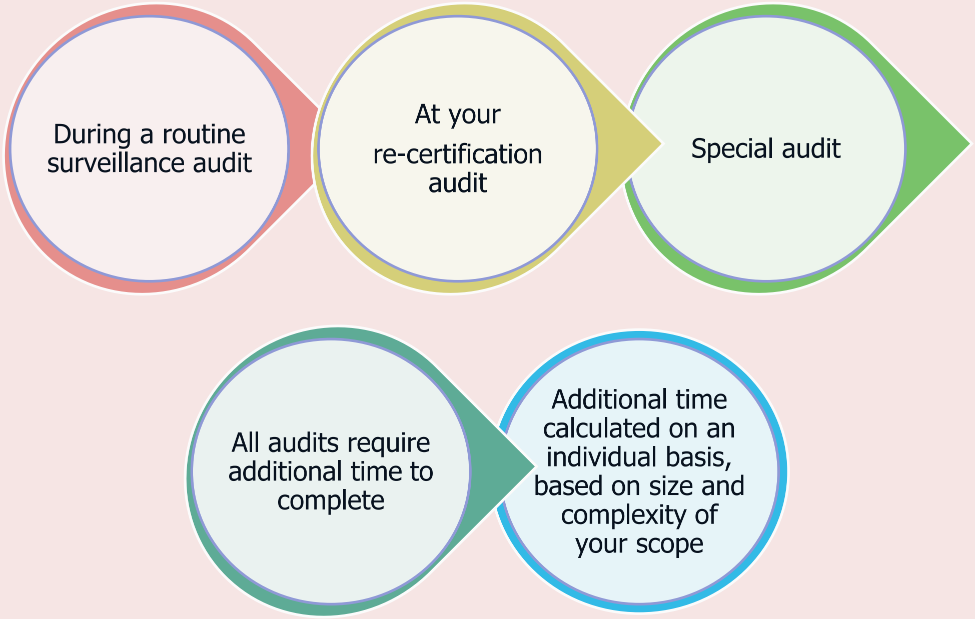
2024

No initial audits to be conducted after **31st October 2023**

2025

All ISO/IEC 27001:2013 certificates shall expire or be withdrawn no later than 31st October 2025

Transition audit:



During a routine surveillance audit

At your re-certification audit

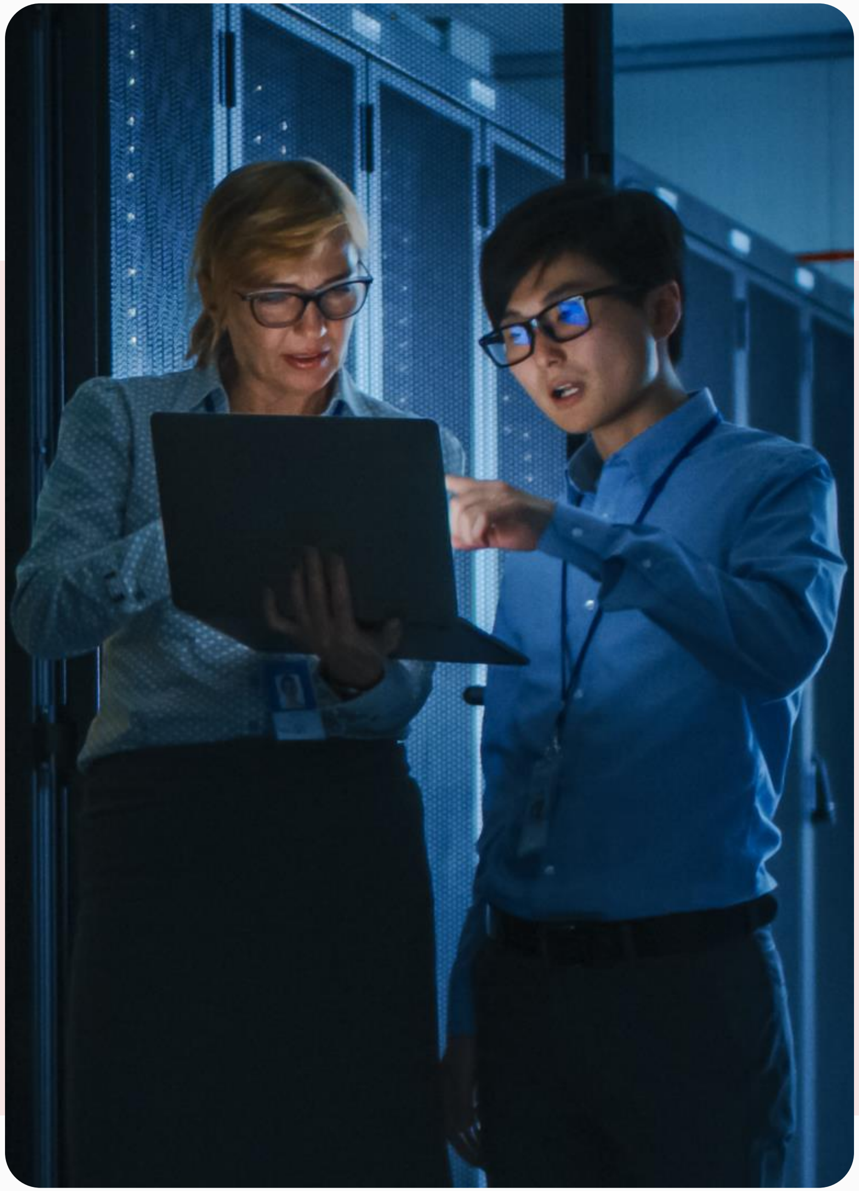
Special audit

All audits require additional time to complete

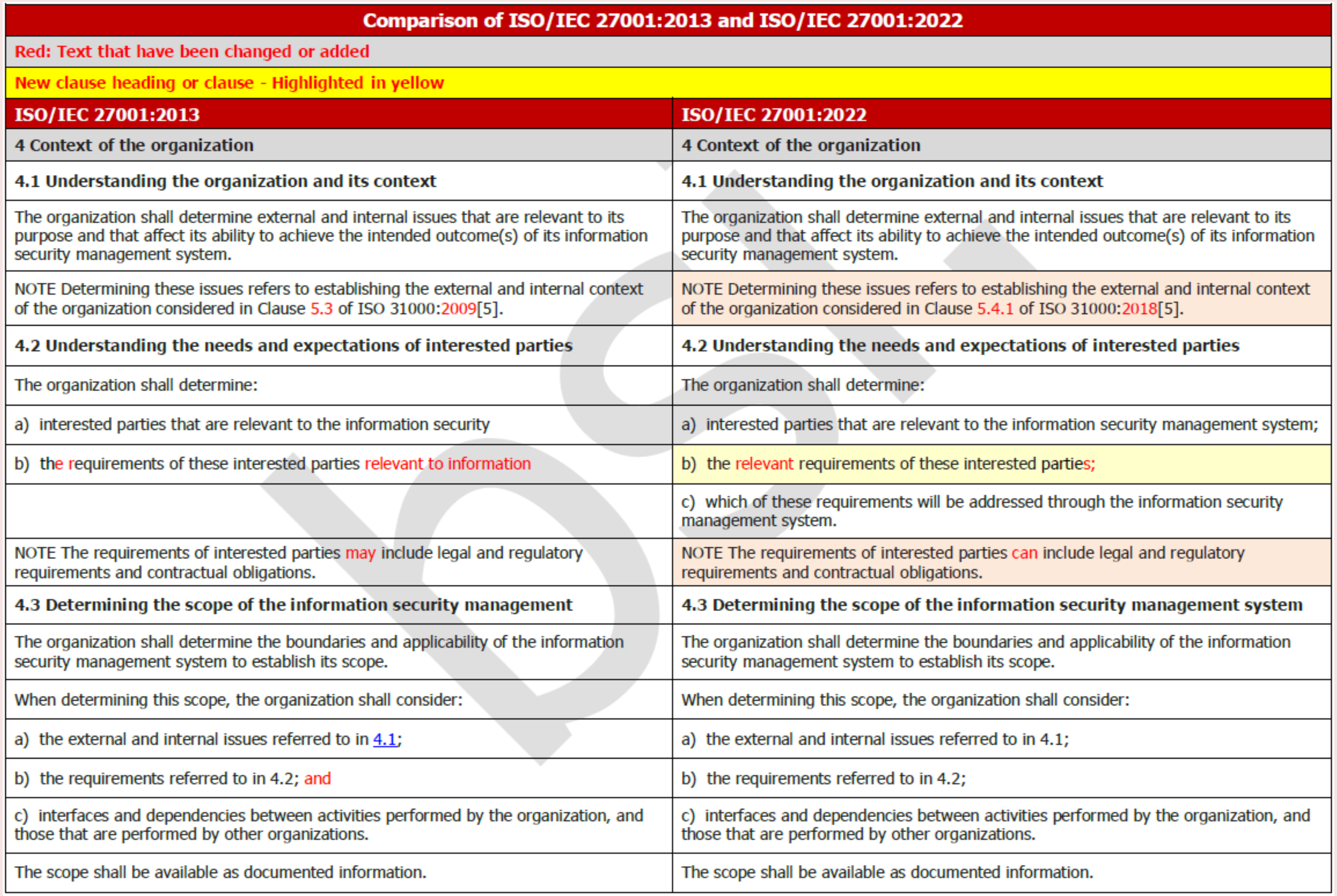
Additional time calculated on an individual basis, based on size and complexity of your scope

Next steps

- Access a copy of ISO/IEC 27001:2022 and where necessary ISO/IEC 27002:2022
- Carry out a gap analysis of your ISMS against the new requirements and Annex A
- Implement and changes necessary, gather evidence of effective implementation
- Update your SoA to reflect the new Annex A and your existing controls, justifying their inclusion and exclusion.
- Work with your client manager on a transition timeline for your ISMS



Comparison of ISO/IEC 27001:2013 and ISO/IEC 27001:2022



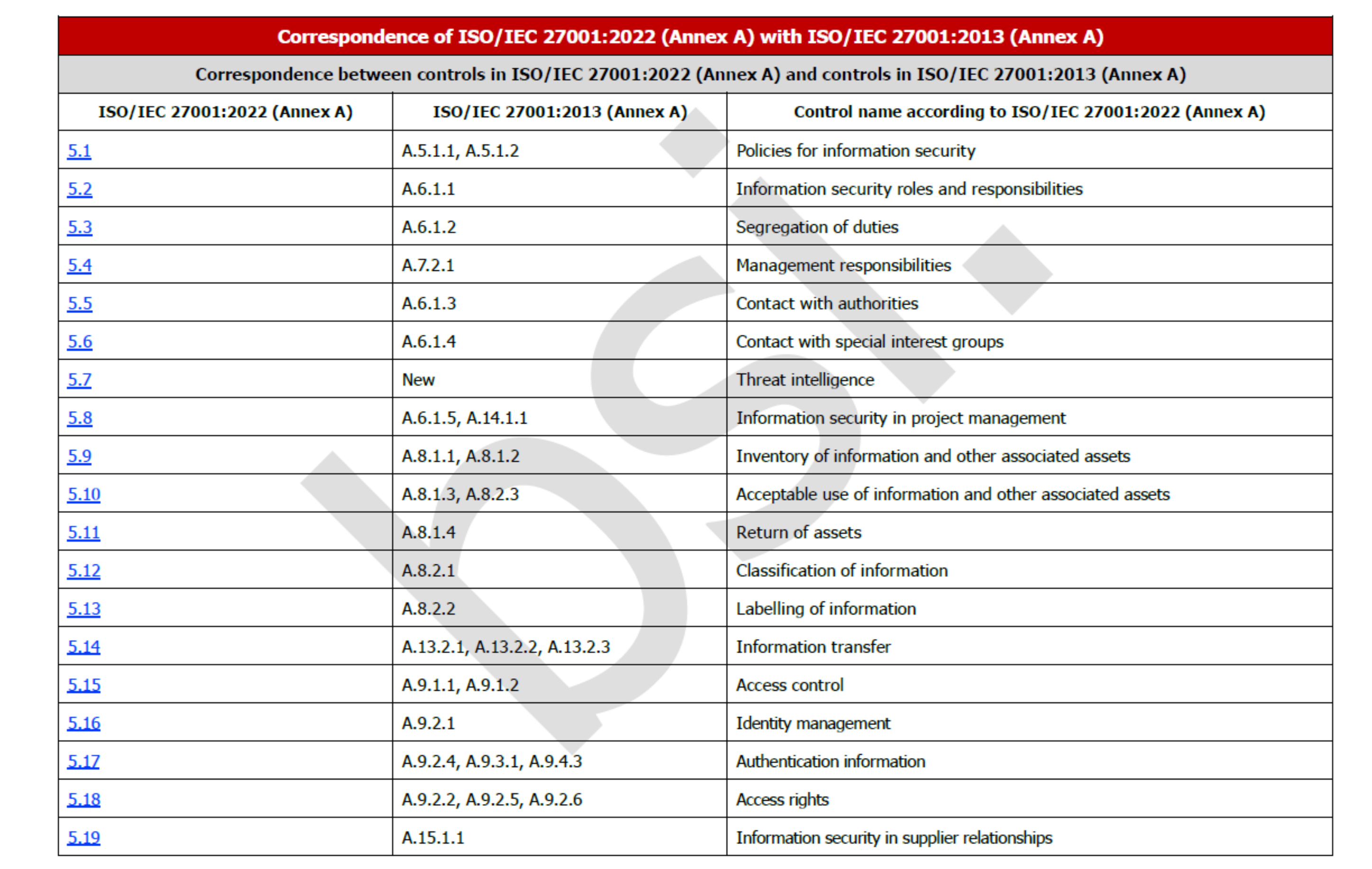
Comparison of ISO/IEC 27001:2013 and ISO/IEC 27001:2022

Red: Text that have been changed or added

New clause heading or clause - Highlighted in yellow

ISO/IEC 27001:2013	ISO/IEC 27001:2022
4 Context of the organization	**4 Context of the organization**
4.1 Understanding the organization and its context	**4.1 Understanding the organization and its context**
The organization shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its information security management system.	The organization shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its information security management system.
NOTE Determining these issues refers to establishing the external and internal context of the organization considered in Clause 5.3 of ISO 31000:2009[5].	NOTE Determining these issues refers to establishing the external and internal context of the organization considered in Clause 5.4.1 of ISO 31000:2018[5].
4.2 Understanding the needs and expectations of interested parties	**4.2 Understanding the needs and expectations of interested parties**
The organization shall determine:	The organization shall determine:
a) interested parties that are relevant to the information security	a) interested parties that are relevant to the information security management system;
b) the requirements of these interested parties relevant to information	b) the relevant requirements of these interested parties;
	c) which of these requirements will be addressed through the information security management system.
NOTE The requirements of interested parties may include legal and regulatory requirements and contractual obligations.	NOTE The requirements of interested parties can include legal and regulatory requirements and contractual obligations.
4.3 Determining the scope of the information security management	**4.3 Determining the scope of the information security management system**
The organization shall determine the boundaries and applicability of the information security management system to establish its scope.	The organization shall determine the boundaries and applicability of the information security management system to establish its scope.
When determining this scope, the organization shall consider:	When determining this scope, the organization shall consider:
a) the external and internal issues referred to in 4.1;	a) the external and internal issues referred to in 4.1;
b) the requirements referred to in 4.2; and	b) the requirements referred to in 4.2;
c) interfaces and dependencies between activities performed by the organization, and those that are performed by other organizations.	c) interfaces and dependencies between activities performed by the organization, and those that are performed by other organizations.
The scope shall be available as documented information.	The scope shall be available as documented information.

Comparison of ISO/IEC 27001:2013 and ISO/IEC27001/2022

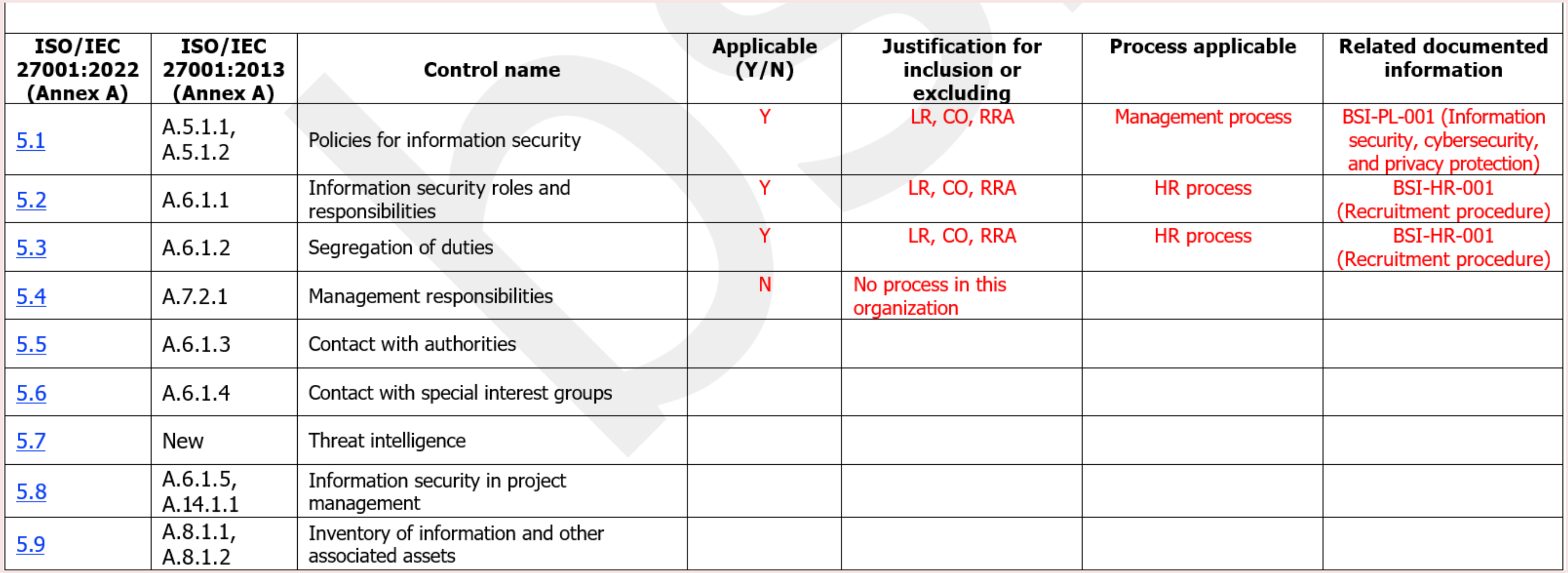


Correspondence of ISO/IEC 27001:2022 (Annex A) with ISO/IEC 27001:2013 (Annex A)

Correspondence between controls in ISO/IEC 27001:2022 (Annex A) and controls in ISO/IEC 27001:2013 (Annex A)

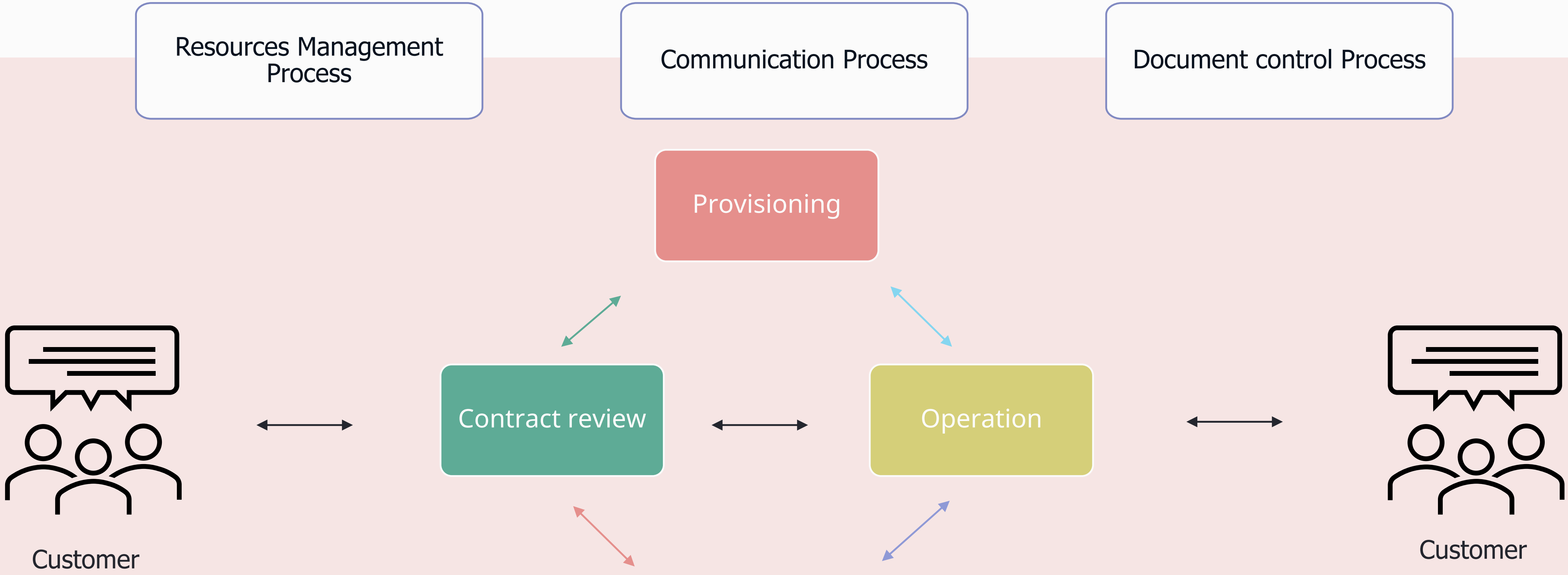
ISO/IEC 27001:2022 (Annex A)	ISO/IEC 27001:2013 (Annex A)	Control name according to ISO/IEC 27001:2022 (Annex A)
5.1	A.5.1.1, A.5.1.2	Policies for information security
5.2	A.6.1.1	Information security roles and responsibilities
5.3	A.6.1.2	Segregation of duties
5.4	A.7.2.1	Management responsibilities
5.5	A.6.1.3	Contact with authorities
5.6	A.6.1.4	Contact with special interest groups
5.7	New	Threat intelligence
5.8	A.6.1.5, A.14.1.1	Information security in project management
5.9	A.8.1.1, A.8.1.2	Inventory of information and other associated assets
5.10	A.8.1.3, A.8.2.3	Acceptable use of information and other associated assets
5.11	A.8.1.4	Return of assets
5.12	A.8.2.1	Classification of information
5.13	A.8.2.2	Labelling of information
5.14	A.13.2.1, A.13.2.2, A.13.2.3	Information transfer
5.15	A.9.1.1, A.9.1.2	Access control
5.16	A.9.2.1	Identity management
5.17	A.9.2.4, A.9.3.1, A.9.4.3	Authentication information
5.18	A.9.2.2, A.9.2.5, A.9.2.6	Access rights
5.19	A.15.1.1	Information security in supplier relationships

Statement of Applicability (ISO/IEC 27001:2022)



ISO/IEC 27001:2022 (Annex A)	ISO/IEC 27001:2013 (Annex A)	Control name	Applicable (Y/N)	Justification for inclusion or excluding	Process applicable	Related documented information
5.1	A.5.1.1, A.5.1.2	Policies for information security	Y	LR, CO, RRA	Management process	BSI-PL-001 (Information security, cybersecurity, and privacy protection)
5.2	A.6.1.1	Information security roles and responsibilities	Y	LR, CO, RRA	HR process	BSI-HR-001 (Recruitment procedure)
5.3	A.6.1.2	Segregation of duties	Y	LR, CO, RRA	HR process	BSI-HR-001 (Recruitment procedure)
5.4	A.7.2.1	Management responsibilities	N	No process in this organization		
5.5	A.6.1.3	Contact with authorities				
5.6	A.6.1.4	Contact with special interest groups				
5.7	New	Threat intelligence				
5.8	A.6.1.5, A.14.1.1	Information security in project management				
5.9	A.8.1.1, A.8.1.2	Inventory of information and other associated assets				

Management Process, Risk management, Legal and compliance



Resources Management Process

Communication Process

Document control Process

Provisioning

Contract review

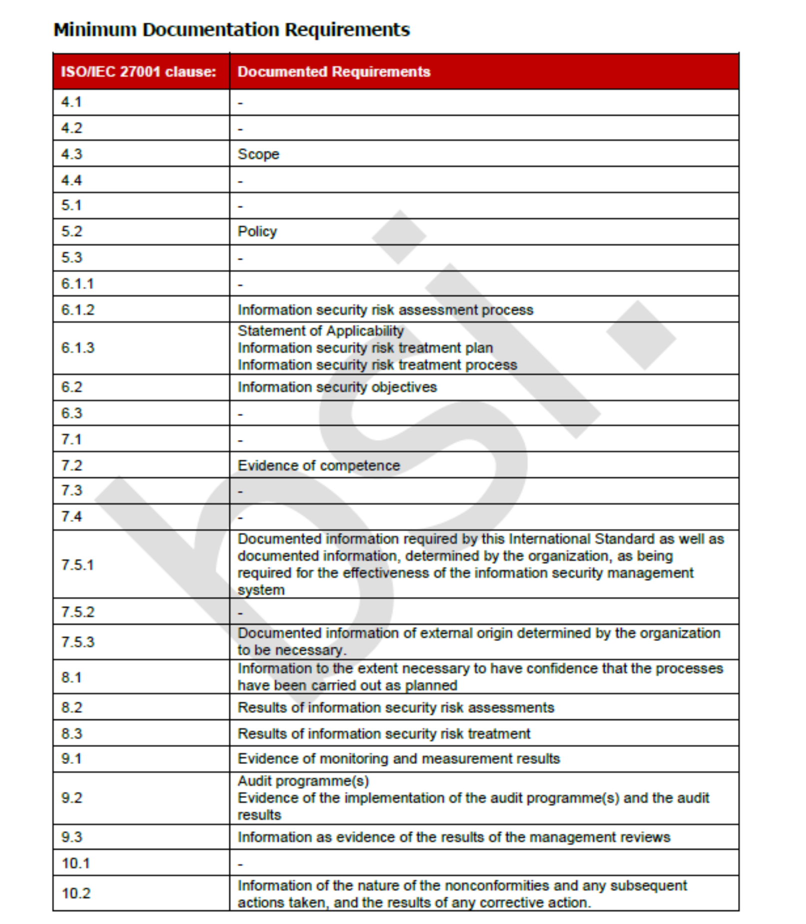
Operation

Reporting

Customer

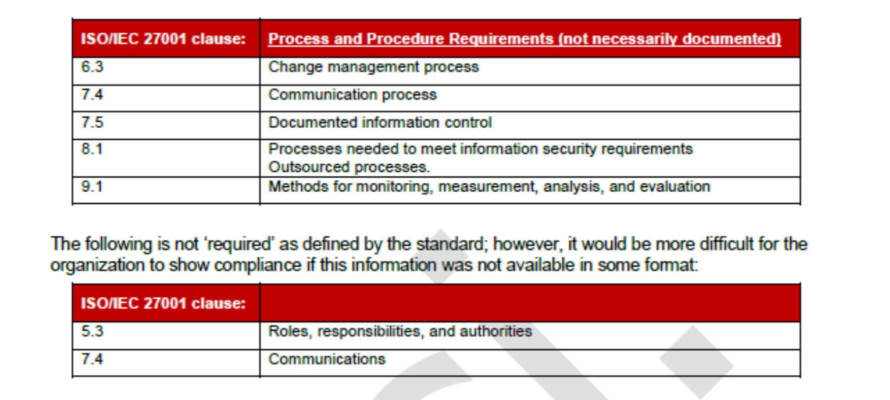
Customer

Minimum Documentation Requirements



Minimum Documentation Requirements

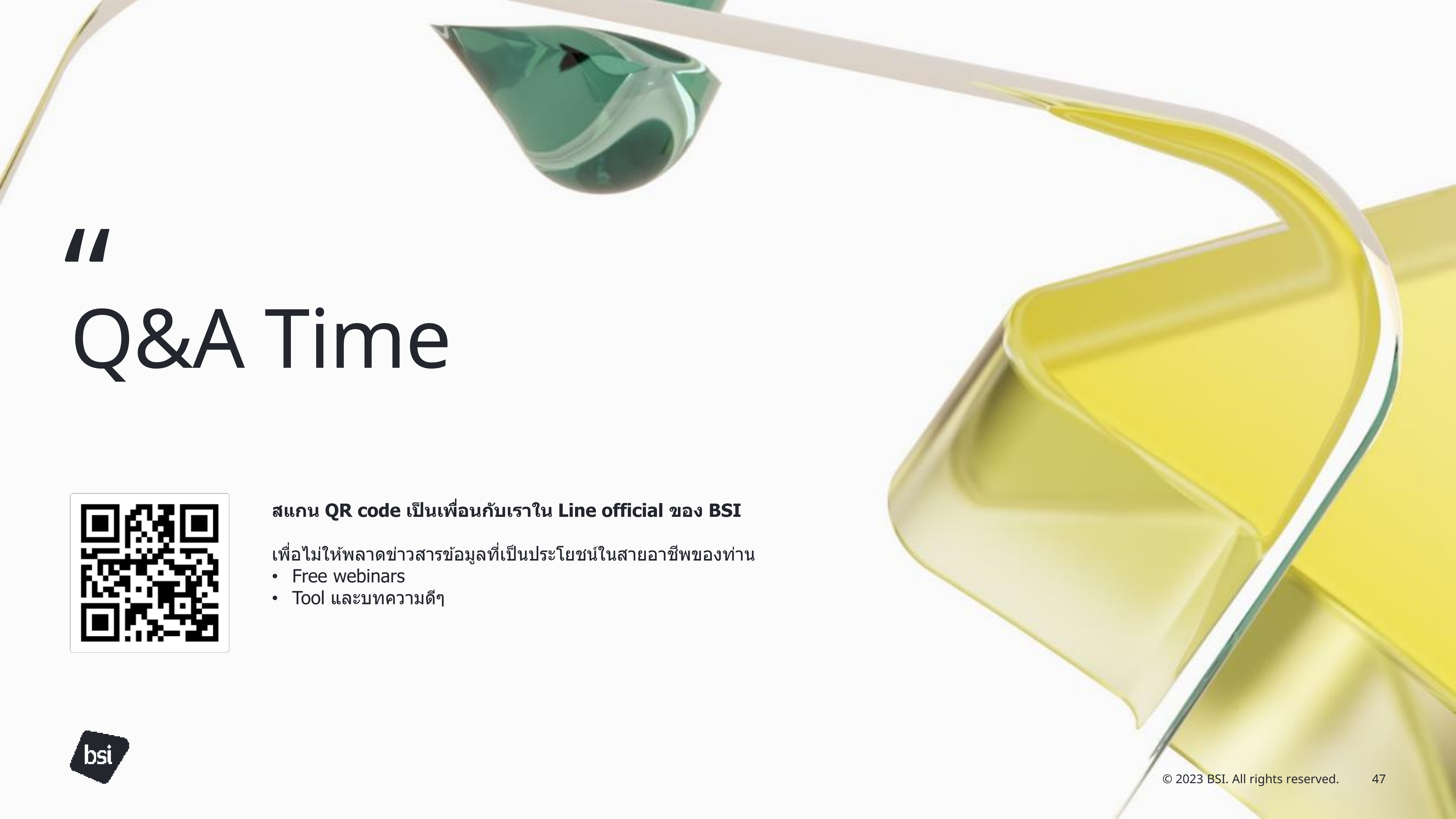
ISO/IEC 27001 clause:	Documented Requirements
4.1	-
4.2	-
4.3	Scope
4.4	-
5.1	-
5.2	Policy
5.3	-
6.1.1	-
6.1.2	Information security risk assessment process
6.1.3	Statement of Applicability Information security risk treatment plan Information security risk treatment process
6.2	Information security objectives
6.3	-
7.1	-
7.2	Evidence of competence
7.3	-
7.4	-
7.5.1	Documented information required by this International Standard as well as documented information, determined by the organization, as being required for the effectiveness of the information security management system
7.5.2	-
7.5.3	Documented information of external origin determined by the organization to be necessary.
8.1	Information to the extent necessary to have confidence that the processes have been carried out as planned
8.2	Results of information security risk assessments
8.3	Results of information security risk treatment
9.1	Evidence of monitoring and measurement results
9.2	Audit programme(s) Evidence of the implementation of the audit programme(s) and the audit results
9.3	Information as evidence of the results of the management reviews
10.1	-
10.2	Information of the nature of the nonconformities and any subsequent actions taken, and the results of any corrective action.



ISO/IEC 27001 clause:	Process and Procedure Requirements (not necessarily documented)
6.3	Change management process
7.4	Communication process
7.5	Documented information control
8.1	Processes needed to meet information security requirements Outsourced processes.
9.1	Methods for monitoring, measurement, analysis, and evaluation

The following is not 'required' as defined by the standard; however, it would be more difficult for the organization to show compliance if this information was not available in some format:

ISO/IEC 27001 clause:	
5.3	Roles, responsibilities, and authorities
7.4	Communications



"

Q&A Time

สแกน QR code เป็นเพื่อนกับเราใน Line official ของ BSI

เพื่อไม่ให้พลาดข่าวสารข้อมูลที่เป็นประโยชน์ในสายอาชีพของท่าน

- Free webinars
- Tool และบทความดีๆ