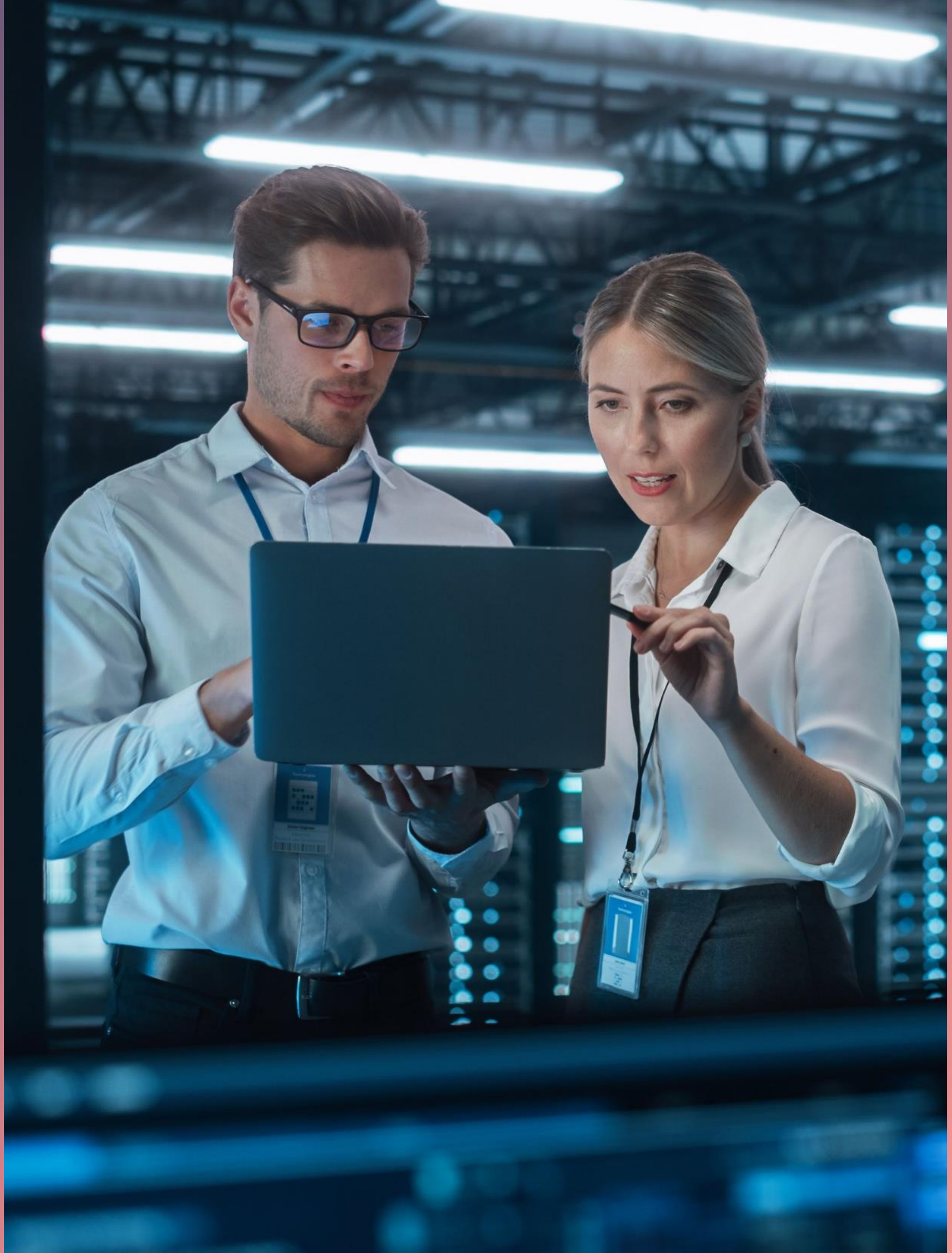
# ● มีอะไรใหม่ ใน ISO/IEC 27701 new version

**Kittipong Keatniyomrung**

**Technical Product Manager**

BSI Group (Thailand)



# หัวข้อชวนคุย

1 Basic ISO/IEC 27701structure

2 Why change for ISO/IEC 27701

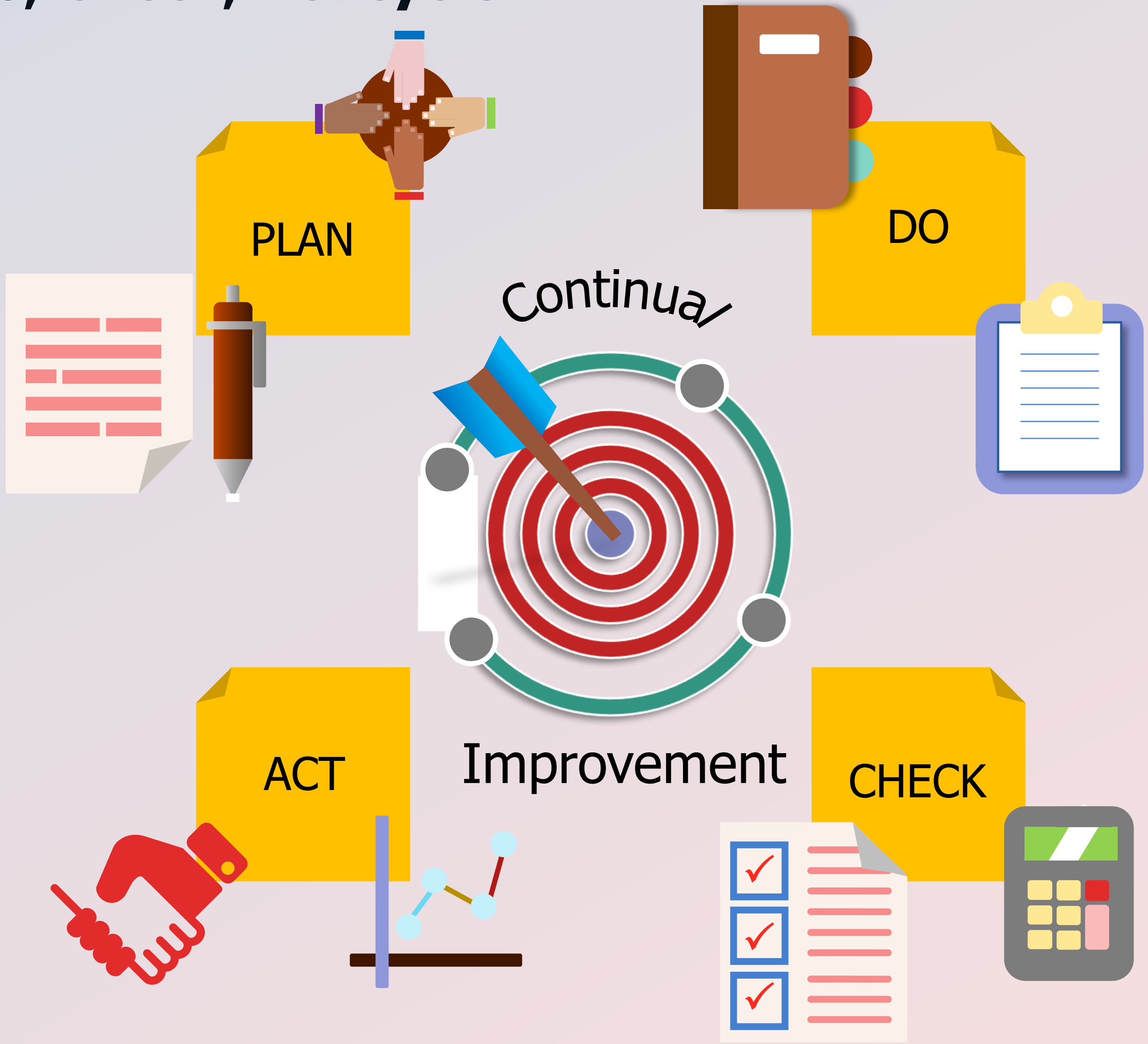
3 Requirement ISO/IEC 27701 new version

# Basic ISO/IEC 27701 structure

# ISO/IEC 27701

Privacy Information Management System (PIMS)

# PIMS Plan, Do, Check, Act cycle



PLAN

DO

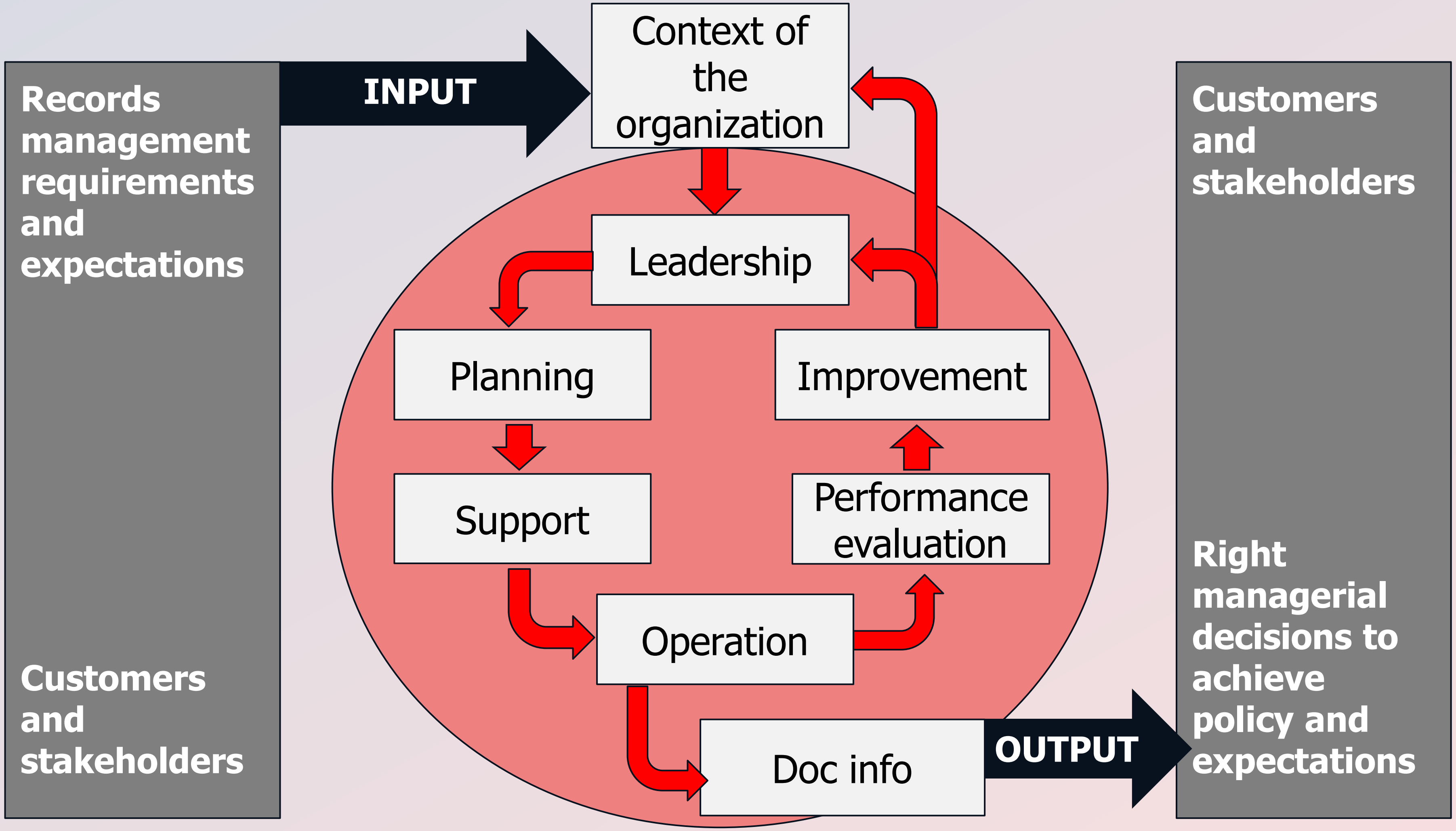
Continual

Improvement

ACT

CHECK

# Integration – High level structure



Records management requirements and expectations

Customers and stakeholders

INPUT

Context of the organization

Leadership

Planning

Support

Operation

Performance evaluation

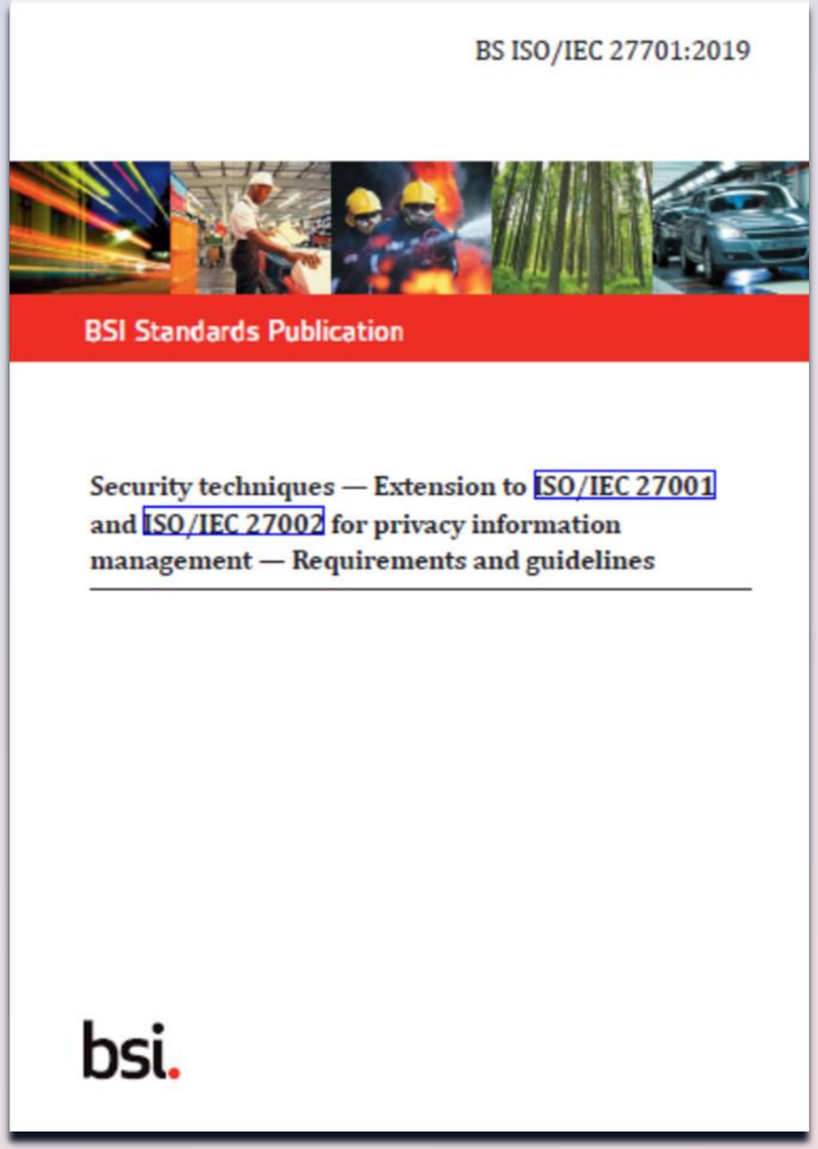
Improvement

Doc info

OUTPUT

Customers and stakeholders

Right managerial decisions to achieve policy and expectations



BS ISO/IEC 27701:2019

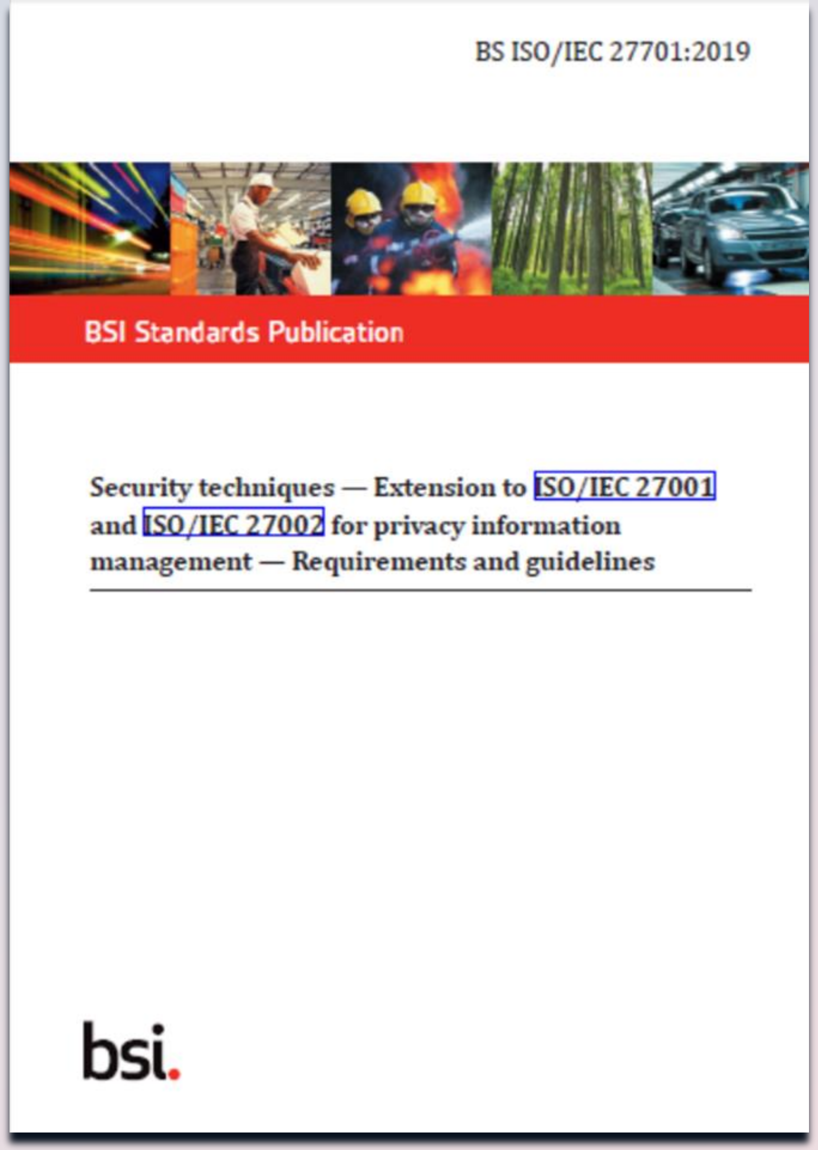
BSI Standards Publication

Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines

bsi.

## Requirement and Guidelines

Extension to ISO/IEC27001 and ISO/IEC 27002 for Privacy Information Management



BS ISO/IEC 27701:2019

BSI Standards Publication

Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines

bsi.

1. Scope
2. Normative Reference
3. Terms, definitions and abbreviations

# 4 General

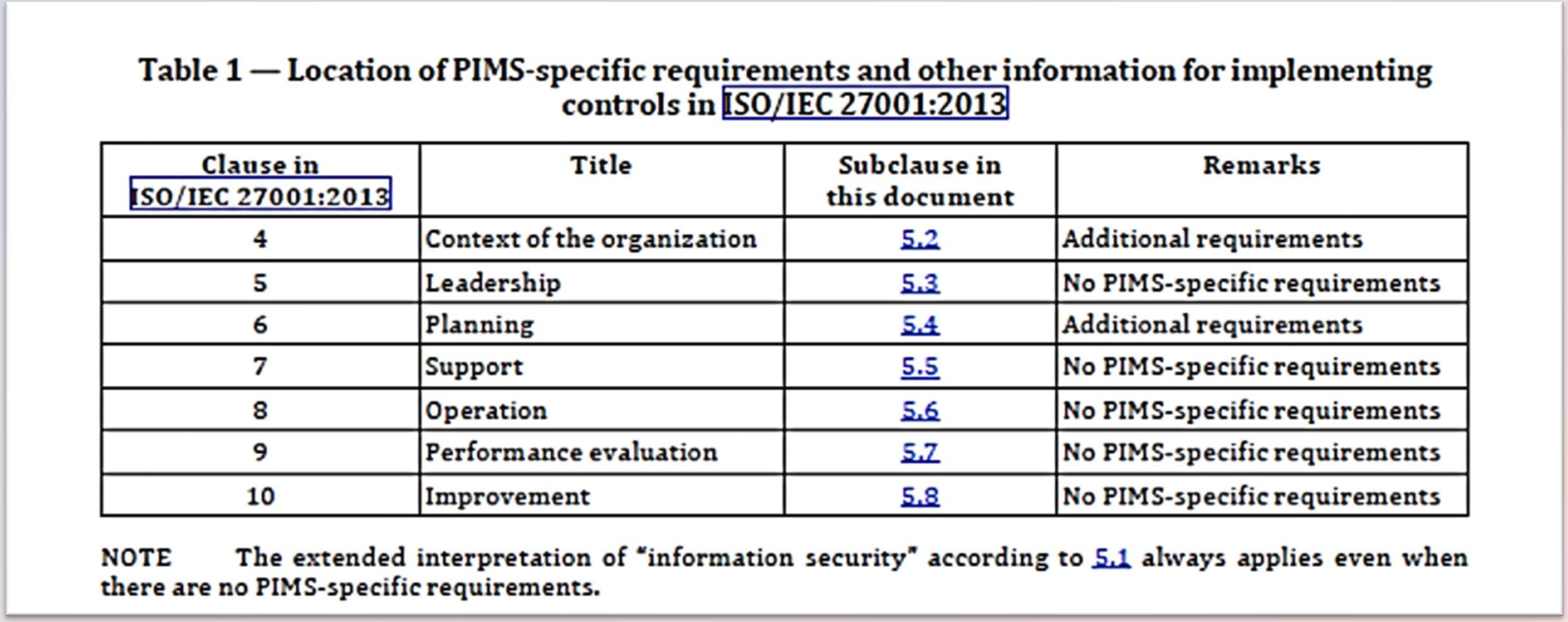


Table 1 — Location of PIMS-specific requirements and other information for implementing controls in ISO/IEC 27001:2013

| Clause in ISO/IEC 27001:2013 | Title | Subclause in this document | Remarks |
|---|---|---|---|
| 4 | Context of the organization | 5.2 | Additional requirements |
| 5 | Leadership | 5.3 | No PIMS-specific requirements |
| 6 | Planning | 5.4 | Additional requirements |
| 7 | Support | 5.5 | No PIMS-specific requirements |
| 8 | Operation | 5.6 | No PIMS-specific requirements |
| 9 | Performance evaluation | 5.7 | No PIMS-specific requirements |
| 10 | Improvement | 5.8 | No PIMS-specific requirements |

NOTE The extended interpretation of "information security" according to 5.1 always applies even when there are no PIMS-specific requirements.

# 4 General

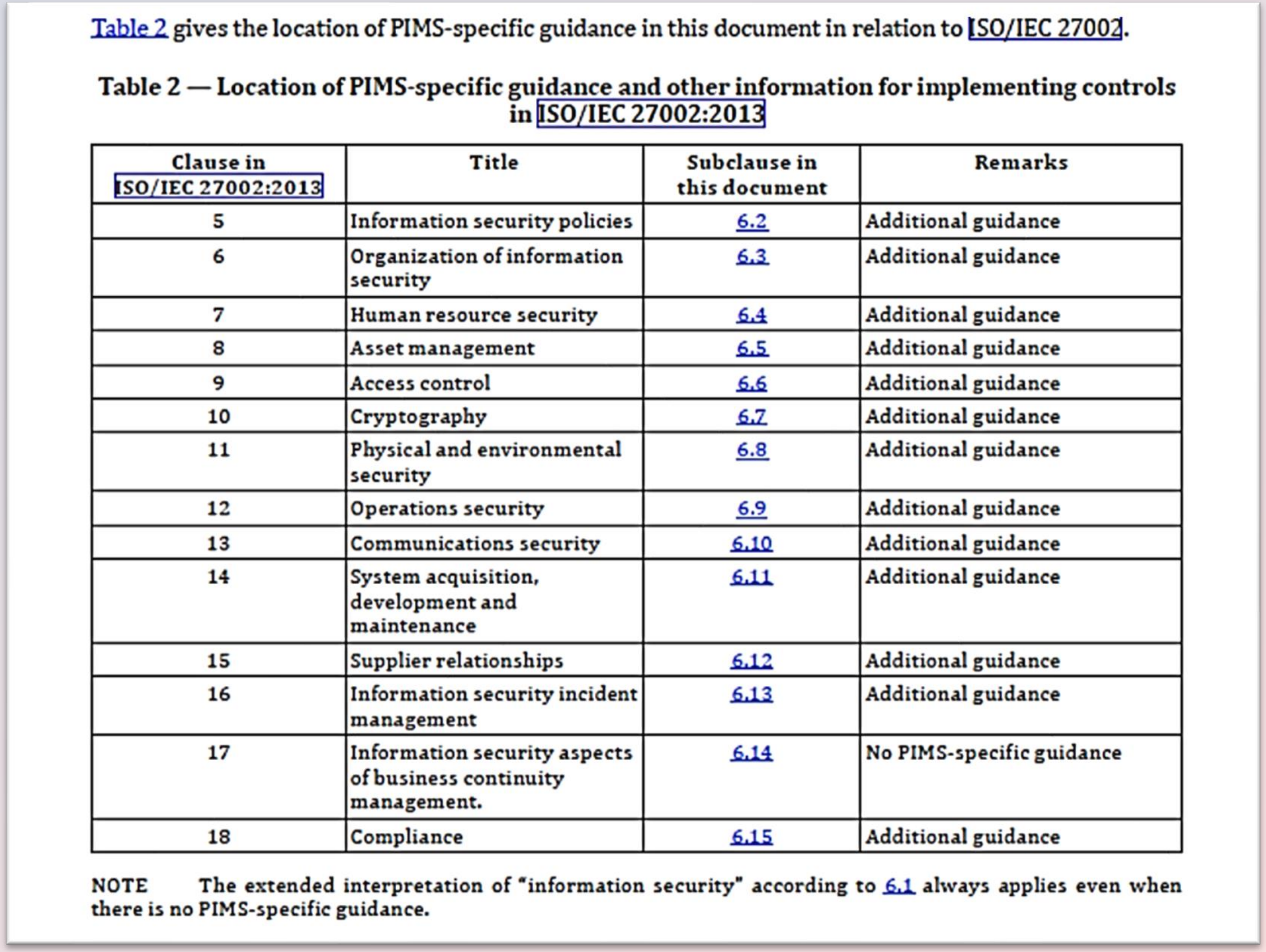


Table 2 gives the location of PIMS-specific guidance in this document in relation to ISO/IEC 27002.

**Table 2 — Location of PIMS-specific guidance and other information for implementing controls in ISO/IEC 27002:2013**

| Clause in ISO/IEC 27002:2013 | Title | Subclause in this document | Remarks |
|---|---|---|---|
| 5 | Information security policies | 6.2 | Additional guidance |
| 6 | Organization of information security | 6.3 | Additional guidance |
| 7 | Human resource security | 6.4 | Additional guidance |
| 8 | Asset management | 6.5 | Additional guidance |
| 9 | Access control | 6.6 | Additional guidance |
| 10 | Cryptography | 6.7 | Additional guidance |
| 11 | Physical and environmental security | 6.8 | Additional guidance |
| 12 | Operations security | 6.9 | Additional guidance |
| 13 | Communications security | 6.10 | Additional guidance |
| 14 | System acquisition, development and maintenance | 6.11 | Additional guidance |
| 15 | Supplier relationships | 6.12 | Additional guidance |
| 16 | Information security incident management | 6.13 | Additional guidance |
| 17 | Information security aspects of business continuity management. | 6.14 | No PIMS-specific guidance |
| 18 | Compliance | 6.15 | Additional guidance |

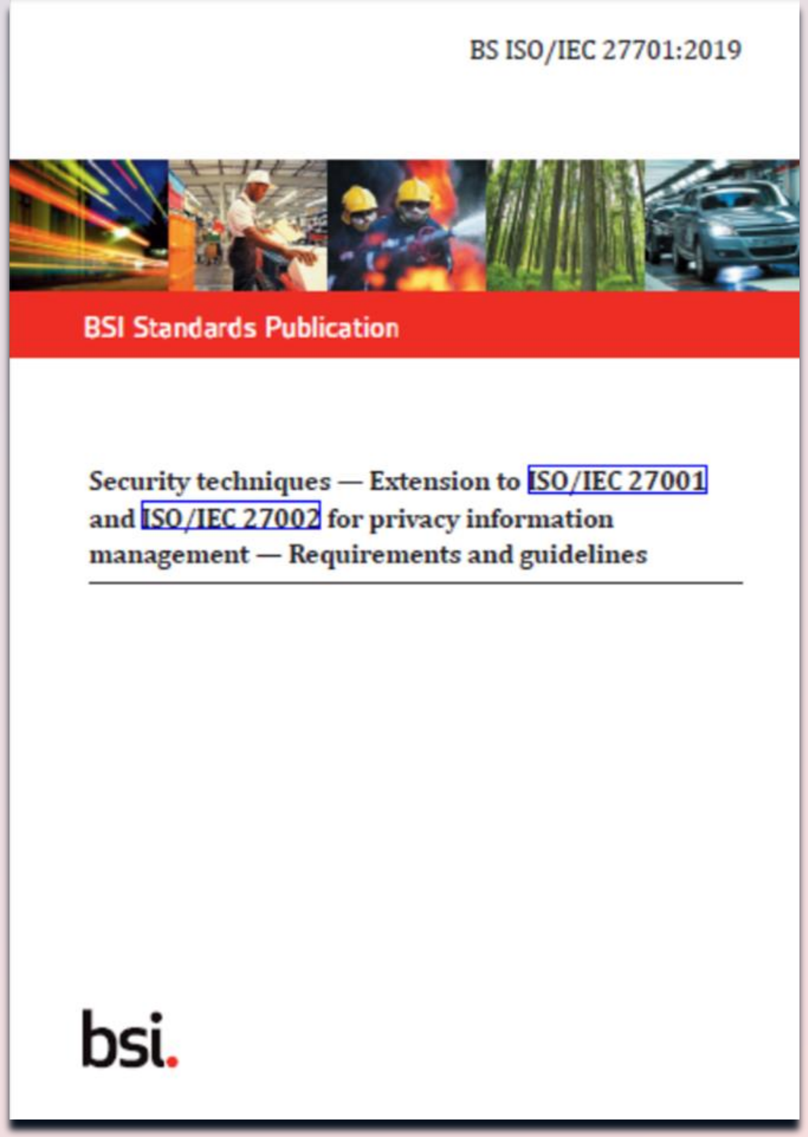
NOTE The extended interpretation of "information security" according to 6.1 always applies even when there is no PIMS-specific guidance.

**Clause 5: PIMS-specific requirements related to ISO/IEC 27001**

**Clause 6: PIMS-specific guidance related to ISO/IEC 27002**

**Clause 7: Additional ISO/IEC 27002 guidance for PII controllers**

**Clause 8: Additional ISO/IEC 27002 guidance for PII processors**



BS ISO/IEC 27701:2019

BSI Standards Publication

Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines

# Annex A- F

| Annex | Detail |
|---|---|
| Annex A (informative) | PIMS-specific reference control objectives and controls (**PII Controllers**) |
| Annex B (normative) | PIMS-specific reference control objectives and controls (**PII Processors**) |
| Annex C (informative) | Mapping to ISO/IEC 29100<br>Table C.1 — Mapping of controls for **PII controllers** and ISO/IEC 29100<br>Table C.2 — Mapping of controls for **PII processors** and ISO/IEC 29100 |
| Annex D (informative) | Mapping to the **General Data Protection Regulation** |
| Annex E (informative) | Mapping to ISO/IEC 27018 and ISO/IEC 29151 |
| Annex F (informative) | How to apply ISO/IEC 27701 to ISO/IEC 27001 and ISO/IEC 27002 |

# Why change for ISO/IEC 27701

# Structure ISO/IEC 27701

**1. Scope**
**2. Normative Reference**

**3. Terms, definitions and abbreviations**

**4. General**

**5. Clause 5: PIMS-specific requirements related to ISO/IEC 27001: 2013** → **Change to ISO/IEC 27001:2022**

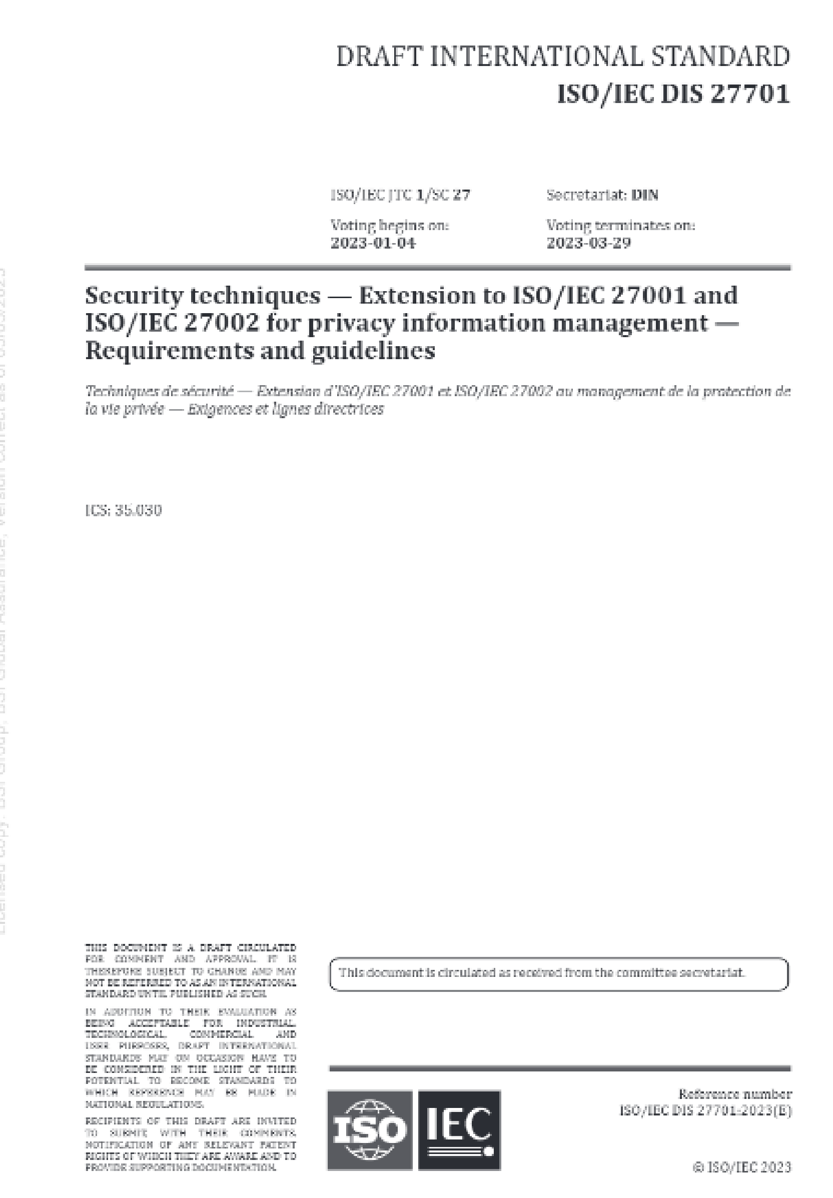
**Clause 6: PIMS-specific guidance related to ISO/IEC 27002:2013** → **Change to ISO/IEC 27002:2022**

**Clause 7: Additional ISO/IEC 27002 guidance for PII controllers**

**Clause 8: Additional ISO/IEC 27002 guidance for PII processors**

# Requirement ISO/IEC 27701 new version

# ISO/IEC **DIS** 27701:2022



DRAFT INTERNATIONAL STANDARD
**ISO/IEC DIS 27701**

ISO/IEC JTC 1/SC 27 Secretariat: **DIN**

Voting begins on: **2023-01-04** Voting terminates on: **2023-03-29**

**Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines**

*Techniques de sécurité — Extension d'ISO/IEC 27001 et ISO/IEC 27002 au management de la protection de la vie privée — Exigences et lignes directrices*

ICS: 35.030

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENT AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

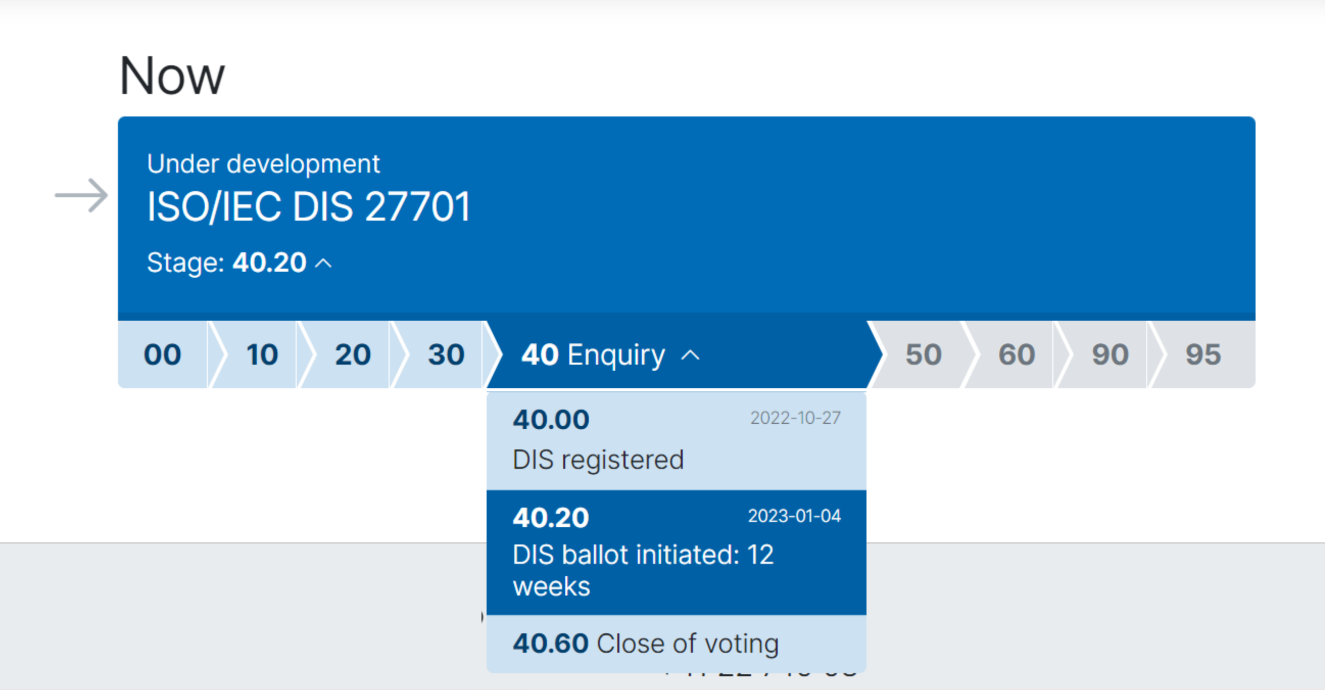
IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

This document is circulated as received from the committee secretariat.

Reference number
ISO/IEC DIS 27701:2023(E)

© ISO/IEC 2023



Now

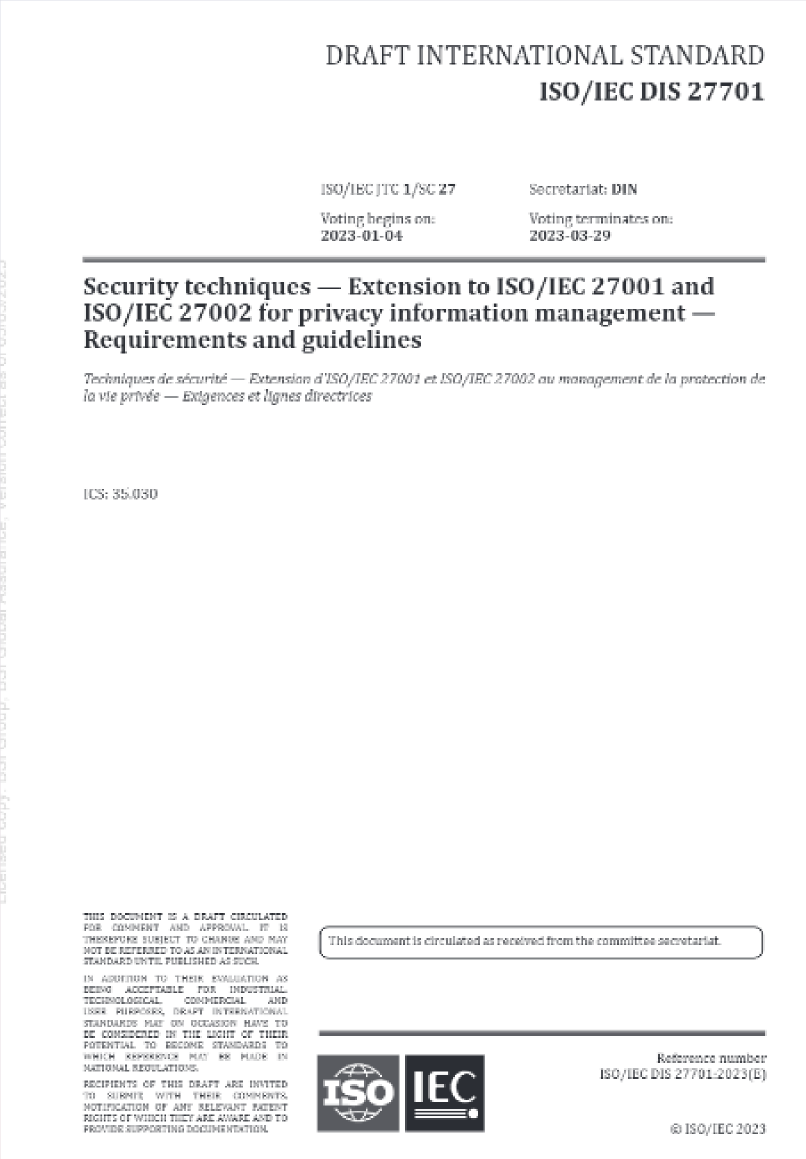
Under development
ISO/IEC DIS 27701
Stage: **40.20**

**40.00** 2022-10-27
DIS registered

**40.20** 2023-01-04
DIS ballot initiated: 12 weeks

**40.60** Close of voting

# ISO/IEC DIS 27701:2022



DRAFT INTERNATIONAL STANDARD
**ISO/IEC DIS 27701**

ISO/IEC JTC 1/SC 27 Secretariat: DIN

Voting begins on: 2023-01-04
Voting terminates on: 2023-03-29

**Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines**

*Techniques de sécurité — Extension d'ISO/IEC 27001 et ISO/IEC 27002 au management de la protection de la vie privée — Exigences et lignes directrices*

ICS: 35.030

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENT AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

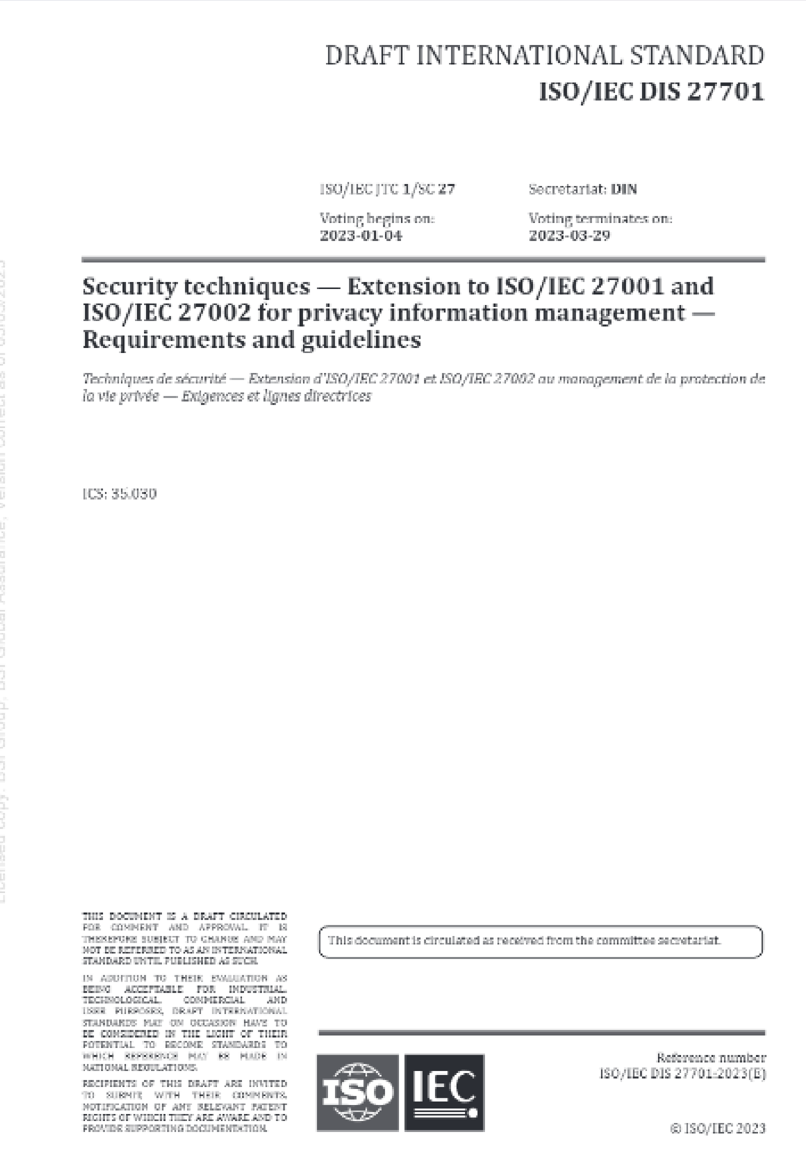
This document is circulated as received from the committee secretariat.

Reference number
ISO/IEC DIS 27701:2023(E)

## Requirement and Guidelines

Extension to ISO/IEC27001 and ISO/IEC 27002 for Privacy Information Management

# ISO/IEC DIS 27701:2022



DRAFT INTERNATIONAL STANDARD
**ISO/IEC DIS 27701**

ISO/IEC JTC 1/SC 27 Secretariat: DIN

Voting begins on:
2023-01-04

Voting terminates on:
2023-03-29

**Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines**

*Techniques de sécurité — Extension d'ISO/IEC 27001 et ISO/IEC 27002 au management de la protection de la vie privée — Exigences et lignes directrices*

ICS: 35.030

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENT AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

This document is circulated as received from the committee secretariat.

Reference number
ISO/IEC DIS 27701:2023(E)

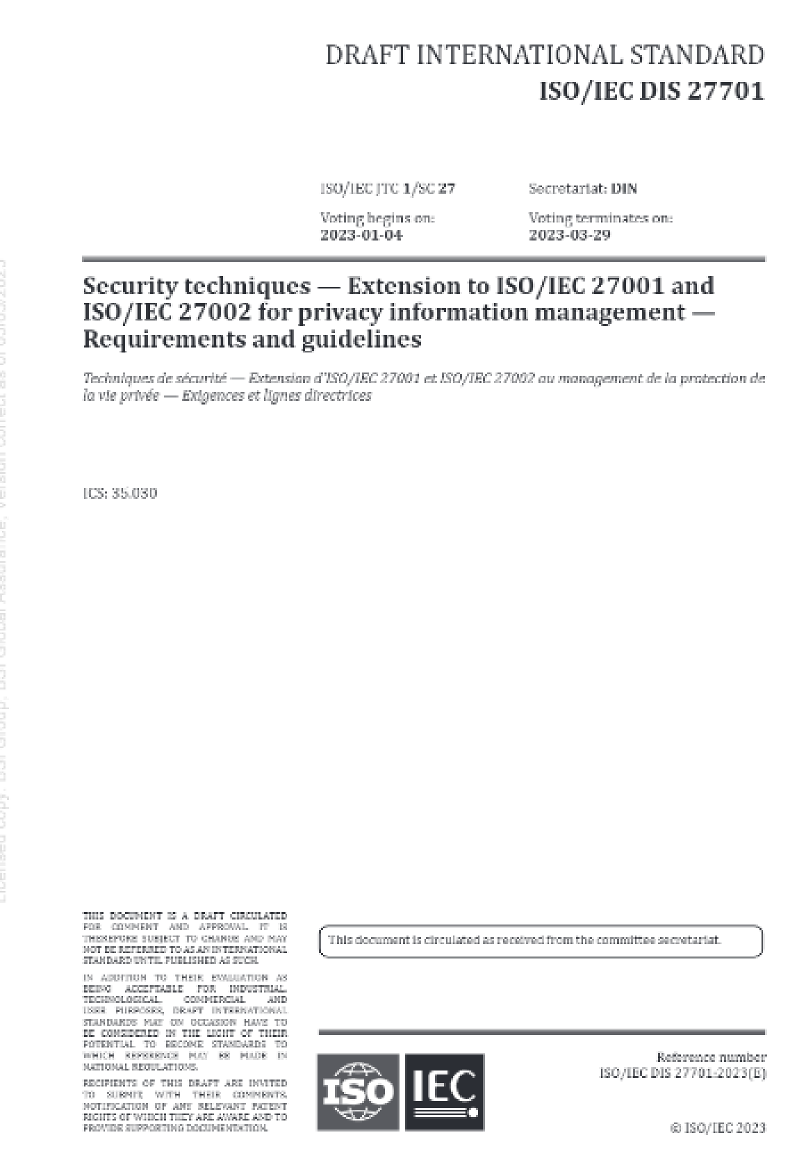
**1. Scope**

**2. Normative Reference**

**3. Terms, definitions and abbreviations**

**4. General**

# ISO/IEC DIS 27701:2022



DRAFT INTERNATIONAL STANDARD
**ISO/IEC DIS 27701**

ISO/IEC JTC 1/SC 27 Secretariat: DIN

Voting begins on:
2023-01-04

Voting terminates on:
2023-03-29

**Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines**

*Techniques de sécurité — Extension d'ISO/IEC 27001 et ISO/IEC 27002 au management de la protection de la vie privée — Exigences et lignes directrices*

ICS: 35.030

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENT AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

This document is circulated as received from the committee secretariat.

Reference number
ISO/IEC DIS 27701:2023(E)

**Clause 5: PIMS-specific requirements related to ISO/IEC 27001**

**Clause 6: PIMS-specific guidance related to ISO/IEC 27002**

**Clause 7: Additional ISO/IEC 27002 guidance for PII controllers**

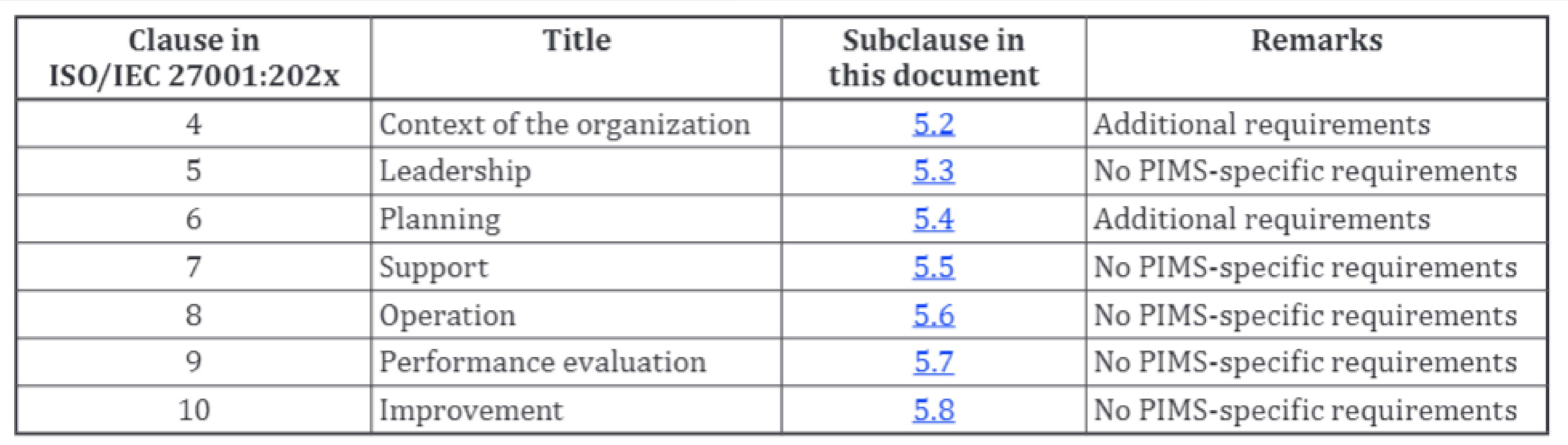
**Clause 8: Additional ISO/IEC 27002 guidance for PII processors**

# ISO/IEC DIS 27701:2022

**Annex A- F**

| Annex | Detail |
|---|---|
| Annex A (informative) | PIMS-specific reference control objectives and controls (**PII Controllers**) |
| Annex B (normative) | PIMS-specific reference control objectives and controls (**PII Processors**) |
| Annex C (informative) | Mapping to ISO/IEC 29100<br>Table C.1 — Mapping of controls for **PII controllers** and ISO/IEC 29100<br>Table C.2 — Mapping of controls for **PII processors** and ISO/IEC 29100 |
| Annex D (informative) | Mapping to the **General Data Protection Regulation** |
| Annex E (informative) | Mapping to ISO/IEC 27018 and ISO/IEC 29151 |
| Annex F (informative) | How to apply ISO/IEC 27701 to ISO/IEC 27001 and ISO/IEC 27002 |
| Annex G (informative) | Correspondence with ISO/IEC 27001:2019 |

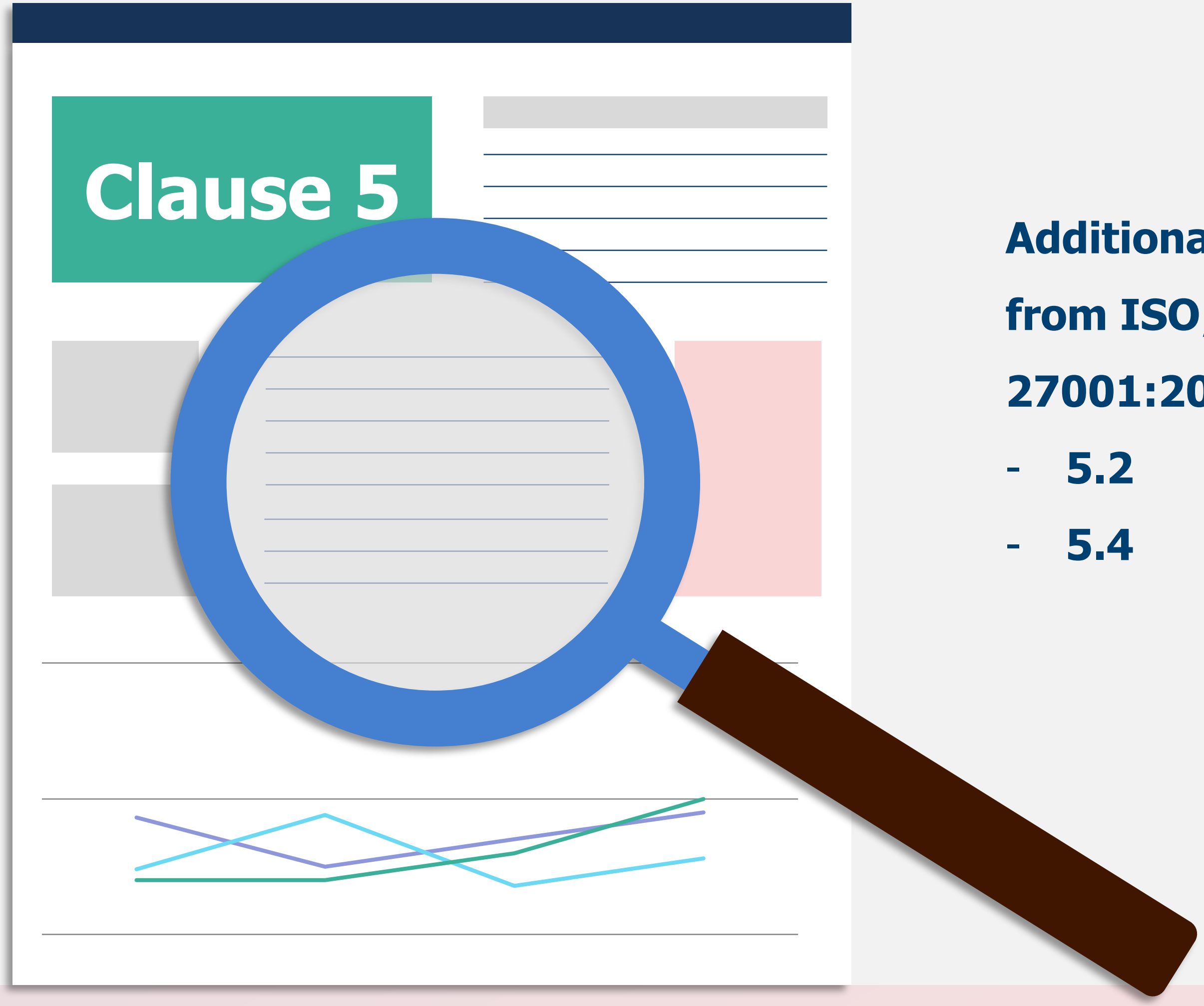
# ISO/IEC DIS 27701:2022



| Clause in ISO/IEC 27001:202x | Title | Subclause in this document | Remarks |
|---|---|---|---|
| 4 | Context of the organization | 5.2 | Additional requirements |
| 5 | Leadership | 5.3 | No PIMS-specific requirements |
| 6 | Planning | 5.4 | Additional requirements |
| 7 | Support | 5.5 | No PIMS-specific requirements |
| 8 | Operation | 5.6 | No PIMS-specific requirements |
| 9 | Performance evaluation | 5.7 | No PIMS-specific requirements |
| 10 | Improvement | 5.8 | No PIMS-specific requirements |

# ISO/IEC DIS 27701:2022

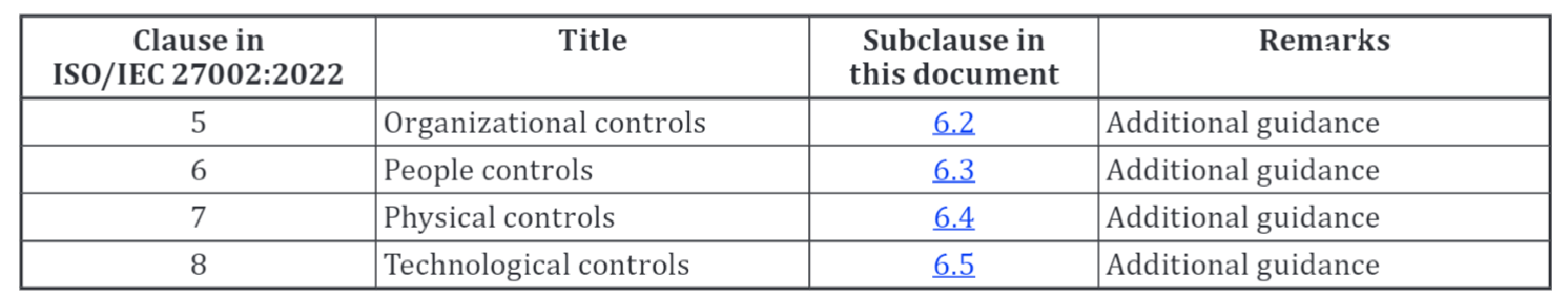
Clause 5: PIMS-specific requirements related to ISO/IEC 27001:2022



**Additional requirement from ISO/IEC 27001:2022**

- **5.2**
- **5.4**

# ISO/IEC DIS 27701:2022



| Clause in ISO/IEC 27002:2022 | Title | Subclause in this document | Remarks |
|---|---|---|---|
| 5 | Organizational controls | 6.2 | Additional guidance |
| 6 | People controls | 6.3 | Additional guidance |
| 7 | Physical controls | 6.4 | Additional guidance |
| 8 | Technological controls | 6.5 | Additional guidance |

# ISO/IEC DIS 27701:2022 (6.2 Organizational controls)

| | | | |
|---|---|---|---|
| 6.2.1 | Policies for information security | 6.2.11 | Return of assets |
| 6.2.2 | Information security roles and responsibilities | 6.2.12 | Classification of information |
| 6.2.3 | Segregation of duties | 6.2.13 | Labelling of information |
| 6.2.4 | Management responsibilities | 6.2.14 | Information transfer |
| 6.2.5 | Contact with authorities | 6.2.15 | Access control |
| 6.2.6 | Contact with special interest groups | 6.2.16 | Identity management |
| 6.2.7 | Threat intelligence | 6.2.17 | Authentication information |
| 6.2.8 | Information security in project management | 6.2.18 | Access rights |
| 6.2.9 | Inventory of information and other associated assets | 6.2.19 | Information security in supplier relationships |
| 6.2.10 | Acceptable use of information and other associated assets | 6.2.20 | Addressing information security within supplier agreements |

# ISO/IEC DIS 27701:2022 (6.2 Organizational controls)

| | | | |
|---|---|---|---|
| 6.2.21 | Managing information security in the ICT supply chain | 6.2.29 | Information security during disruption |
| 6.2.22 | Monitoring, review and change management of supplier services | 6.2.30 | ICT readiness for business continuity |
| 6.2.23 | Information security for use of cloud services | 6.2.31 | Legal, statutory, regulatory and contractual requirements |
| 6.2.24 | Information security incident management planning and preparation | 6.2.32 | Intellectual property rights |
| 6.2.25 | Assessment and decision on information security events | 6.2.33 | Protection of records |
| 6.2.26 | Response to information security incidents | 6.2.34 | Privacy and protection of PII |
| 6.2.27 | Learning from information security incidents | 6.2.35 | Independent review of information security |
| 6.2.28 | Collection of evidence | 6.2.36 | Compliance with policies, rules and standards for information security |
| | | 6.2.37 | Documented operating procedures |

# ISO/IEC DIS 27701:2022 (6.3 People control)

| | |
|---|---|
| 6.3.1 | Screening |
| 6.3.2 | Terms and conditions of employment |
| 6.3.3 | Information security awareness, education and training |
| 6.3.4 | Disciplinary process |
| 6.3.5 | Responsibilities after termination or change of employment |
| 6.3.6 | Confidentiality or non-disclosure agreements |
| 6.3.7 | Remote working |
| 6.3.8 | Information security event reporting |

# ISO/IEC DIS 27701:2022  (6.4 Physical controls)

| | | | |
|---|---|---|---|
| 6.4.1 | Physical security perimeters | 6.4.8 | Equipment siting and protection |
| 6.4.2 | Physical entry | 6.4.9 | Security of assets off-premises |
| 6.4.3 | Securing offices, rooms and facilities | 6.4.10 | Storage media |
| 6.4.4 | Physical security monitoring | 6.4.11 | Supporting utilities |
| 6.4.5 | Protecting against physical and environmental threats | 6.4.12 | Cabling security |
| 6.4.6 | Working in secure areas | 6.4.13 | Equipment maintenance |
| 6.4.7 | Clear desk and clear screen | 6.4.14 | Secure disposal or re-use of equipment |

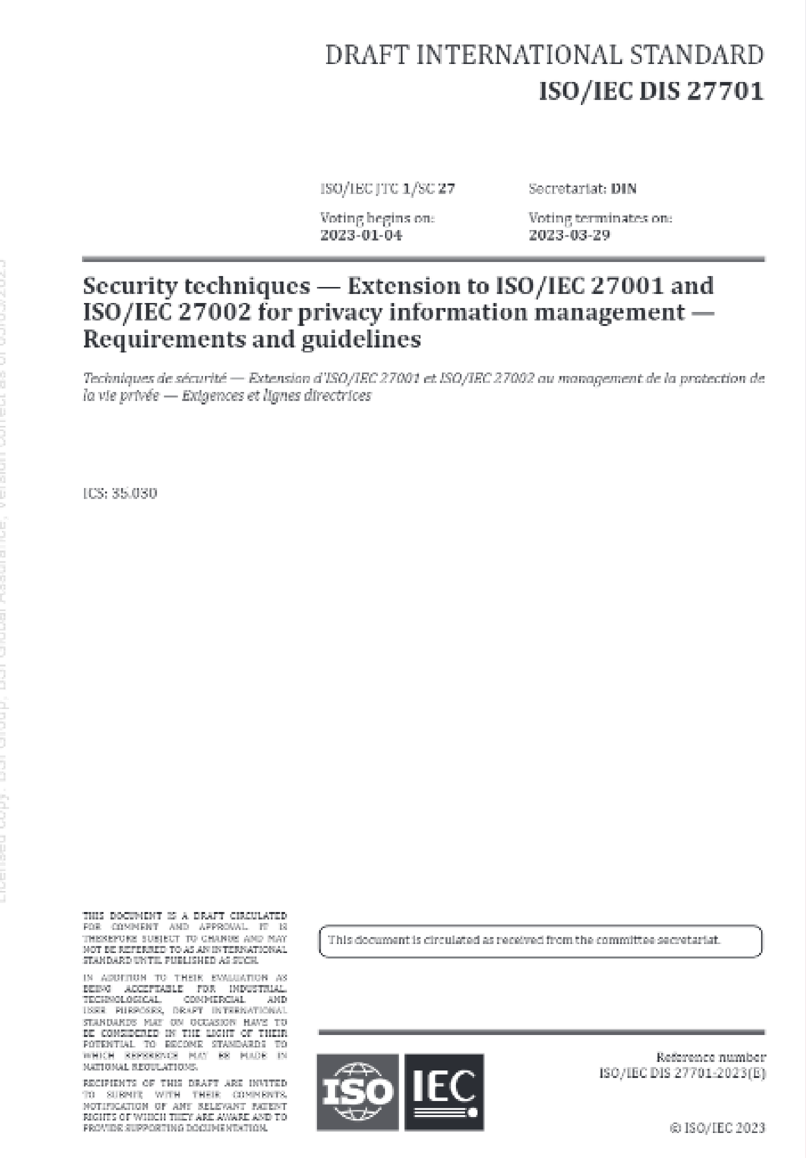
# ISO/IEC DIS 27701:2022 (6.5 Technological controls)

| | | | |
|---|---|---|---|
| 6.5.1 | User endpoint devices | 6.5.11 | Data masking |
| 6.5.2 | Privileged access rights | 6.5.12 | Data leakage prevention |
| 6.5.3 | Information access restriction | 6.5.13 | Information backup |
| 6.5.4 | Access to source code | 6.5.14 | Redundancy of information processing facilities |
| 6.5.5 | Secure authentication | 6.5.15 | Logging |
| 6.5.6 | Capacity management | 6.5.16 | Monitoring activities |
| 6.5.7 | Protection against malware | 6.5.17 | Clock synchronization |
| 6.5.8 | Management of technical vulnerabilities | 6.5.18 | Use of privileged utility programs |
| 6.5.9 | Configuration management | 6.5.19 | Installation of software on operational systems |
| 6.5.10 | Information deletion | 6.5.20 | Networks security |

# ISO/IEC DIS 27701:2022 (6.5 Technological controls)

| | | | |
|---|---|---|---|
| 6.5.21 | Security of network services | 6.5.28 | Secure coding |
| 6.5.22 | Segregation of networks | 6.5.29 | Security testing in development and acceptance |
| 6.5.23 | Web filtering | 6.5.30 | Outsourced development |
| 6.5.24 | Use of cryptography | 6.5.31 | Separation of development, test and production environments |
| 6.5.25 | Secure development life cycle | 6.5.32 | Change management |
| 6.5.26 | Application security requirements | 6.5.33 | Test information |
| 6.5.27 | Secure system architecture and engineering principles | 6.5.34 | Protection of information systems during audit testing |

# ISO/IEC DIS 27701:2022



DRAFT INTERNATIONAL STANDARD
**ISO/IEC DIS 27701**

ISO/IEC JTC 1/SC 27 Secretariat: **DIN**

Voting begins on: **2023-01-04** Voting terminates on: **2023-03-29**

**Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines**

*Techniques de sécurité — Extension d'ISO/IEC 27001 et ISO/IEC 27002 au management de la protection de la vie privée — Exigences et lignes directrices*

ICS: 35.030

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENT AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

This document is circulated as received from the committee secretariat.

Reference number
ISO/IEC DIS 27701:2023(E)

## Clause 7: Additional ISO/IEC 27002 guidance for PII controllers

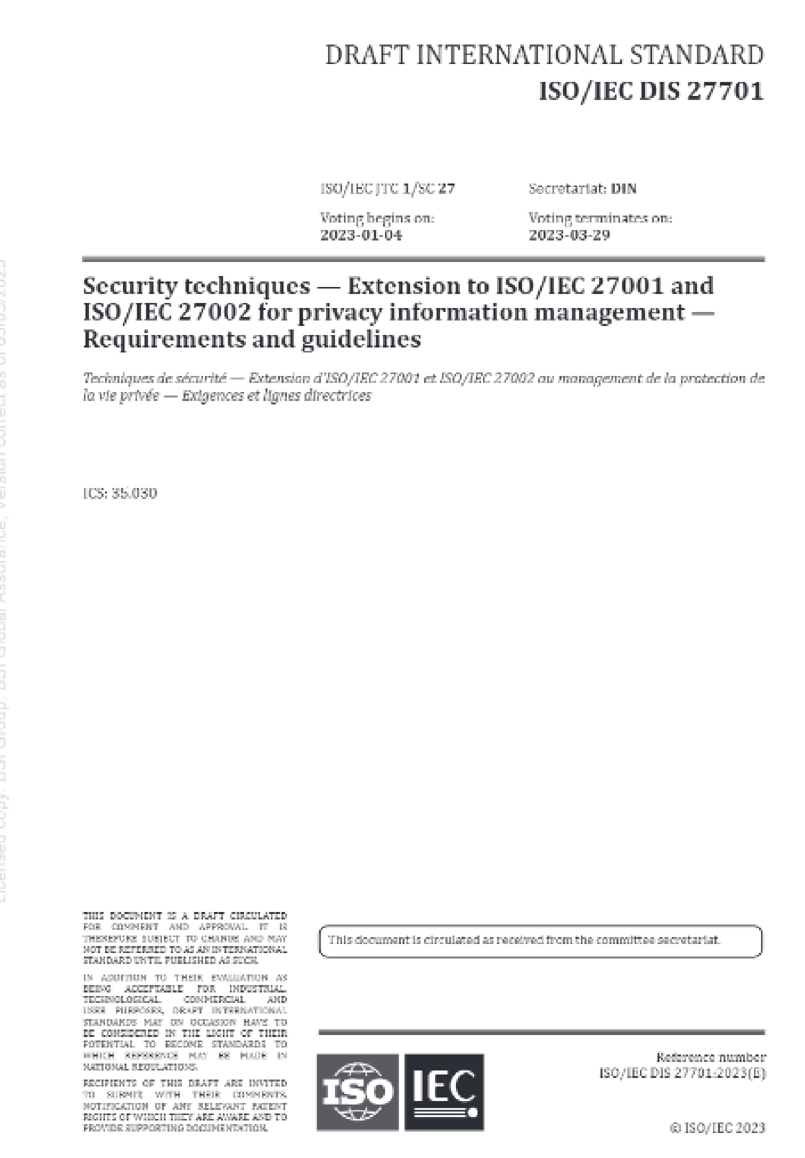
► **Not changed**

## Clause 8: Additional ISO/IEC 27002 guidance for PII processors

► **Not changed**

# Summary change

# ISO/IEC DIS 27701:2022



DRAFT INTERNATIONAL STANDARD
**ISO/IEC DIS 27701**

ISO/IEC JTC 1/SC **27** Secretariat: **DIN**

Voting begins on:
**2023-01-04**

Voting terminates on:
**2023-03-29**

**Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines**

*Techniques de sécurité — Extension d'ISO/IEC 27001 et ISO/IEC 27002 au management de la protection de la vie privée — Exigences et lignes directrices*

ICS: 35.030

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENT AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

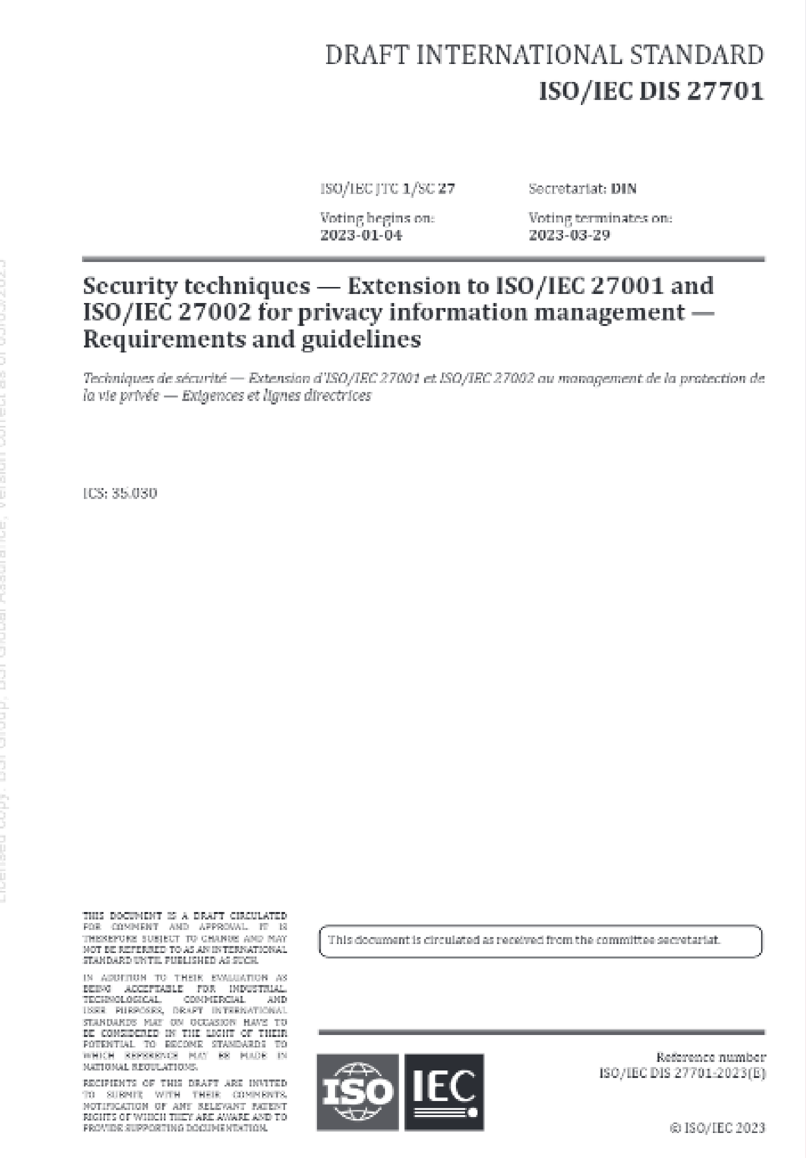
This document is circulated as received from the committee secretariat.

Reference number
ISO/IEC DIS 27701:2023(E)

**Clause 5: PIMS-specific requirements related to ISO/IEC 27001**

- ► **Change as requirement ISO/IEC 27001:2022**

# ISO/IEC DIS 27701:2022



DRAFT INTERNATIONAL STANDARD

**ISO/IEC DIS 27701**

ISO/IEC JTC 1/SC 27 — Secretariat: DIN

Voting begins on: 2023-01-04 — Voting terminates on: 2023-03-29

**Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines**

*Techniques de sécurité — Extension d'ISO/IEC 27001 et ISO/IEC 27002 au management de la protection de la vie privée — Exigences et lignes directrices*

ICS: 35.030

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENT AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

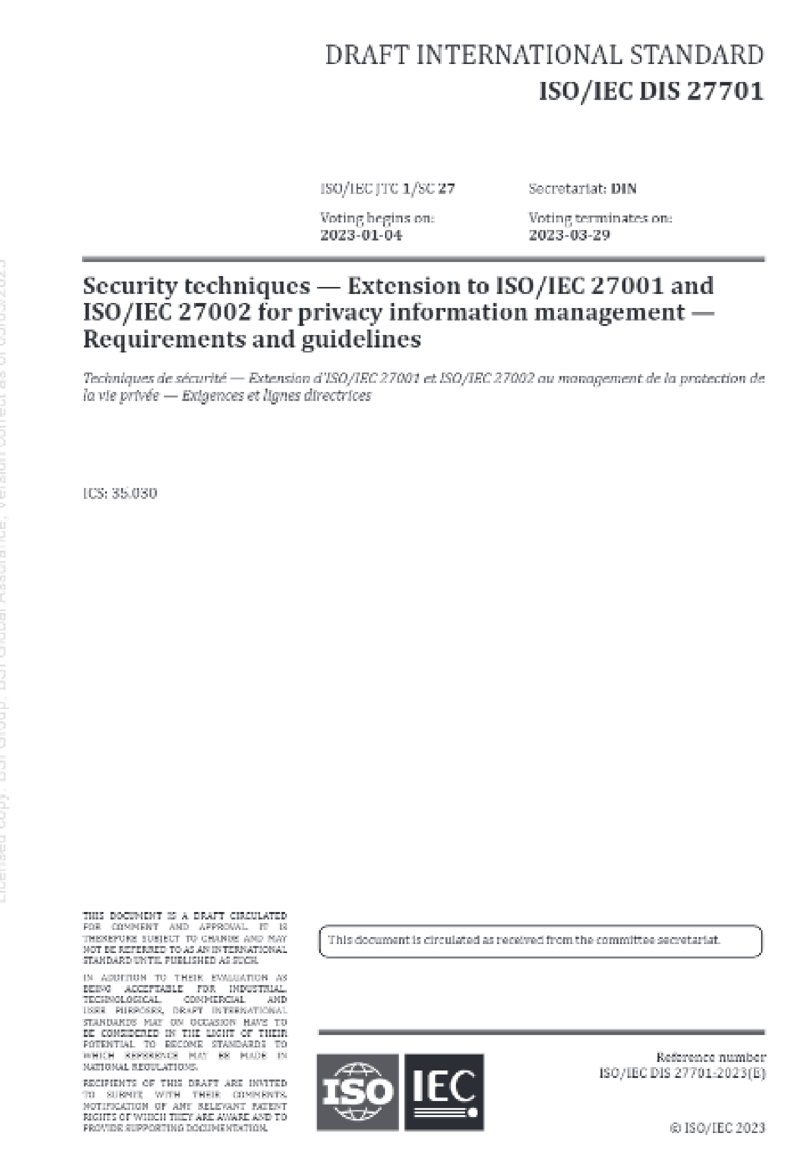
This document is circulated as received from the committee secretariat.

Reference number
ISO/IEC DIS 27701:2023(E)

**Clause 6: PIMS-specific guidance related to ISO/IEC 27002**

**► Change as ISO/IEC 27002:2022**

# ISO/IEC DIS 27701:2022



DRAFT INTERNATIONAL STANDARD
**ISO/IEC DIS 27701**

| | |
|---|---|
| ISO/IEC JTC 1/SC 27 | Secretariat: DIN |
| Voting begins on:<br>2023-01-04 | Voting terminates on:<br>2023-03-29 |

**Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines**

*Techniques de sécurité — Extension d'ISO/IEC 27001 et ISO/IEC 27002 au management de la protection de la vie privée — Exigences et lignes directrices*

ICS: 35.030

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENT AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

This document is circulated as received from the committee secretariat.

Reference number
ISO/IEC DIS 27701:2023(E)

**Clause 7: Additional ISO/IEC 27002 guidance for PII controllers**

**► Not changed**

**Clause 8: Additional ISO/IEC 27002 guidance for PII processors**

**► Not changed**

# Consequence for Implementation

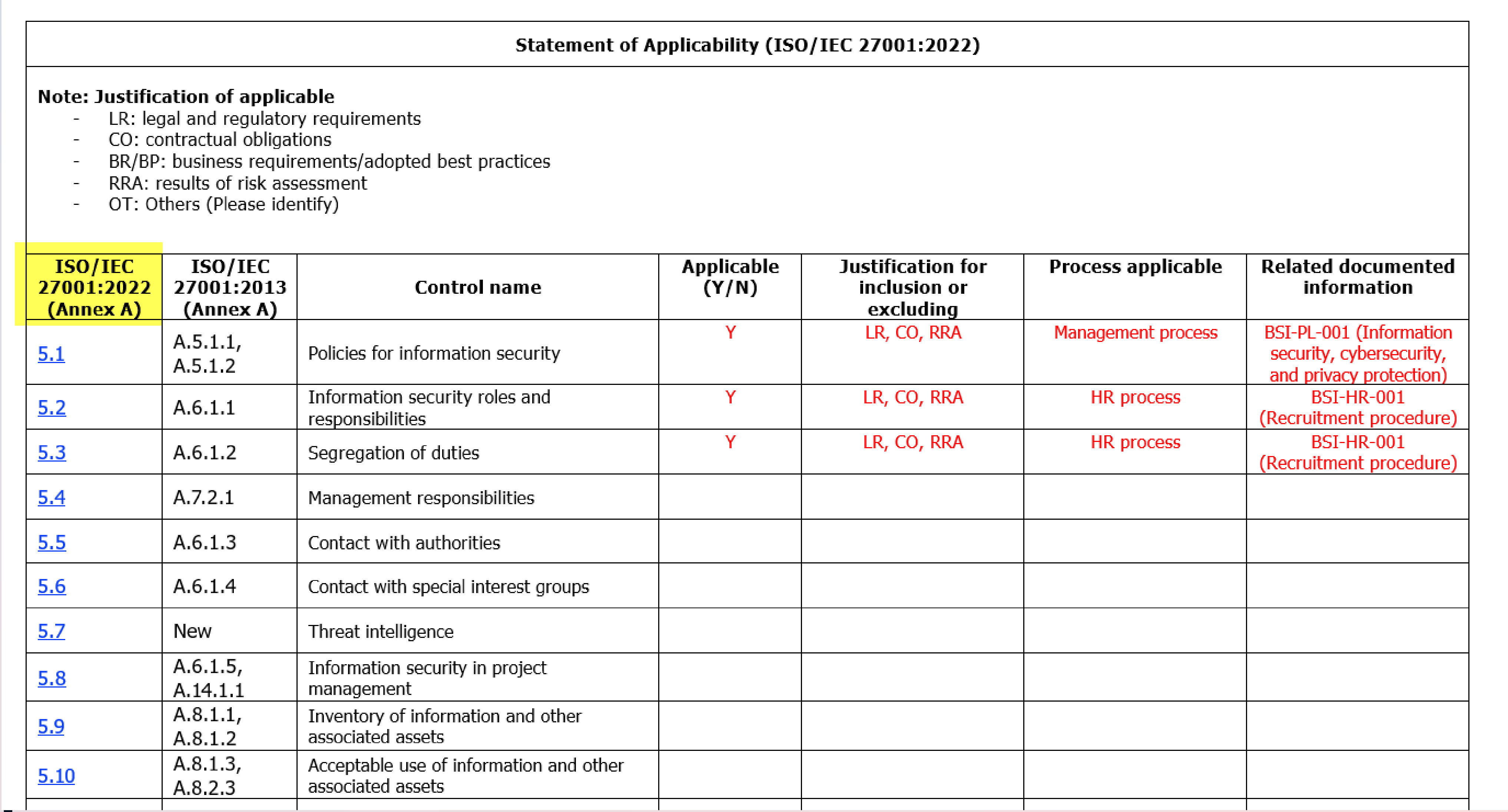
Transition ISO/IEC 27001:2022 (within 1 November 2025)

Study requirement ISO/IEC 27701:202x and implement

Inform BSI for transition (If BSI is approved to audit ISO/IEC 27701:202X)

Transition period will be announcement. After deadline, ISO/IEC 27701:2019 will be expired.

# ISO/IEC DIS 27701:2022



**Statement of Applicability (ISO/IEC 27001:2022)**

**Note: Justification of applicable**

- LR: legal and regulatory requirements
- CO: contractual obligations
- BR/BP: business requirements/adopted best practices
- RRA: results of risk assessment
- OT: Others (Please identify)

| 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 | | | | |
| 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 | | | | |

# Certified and Transition – BSI

Waiting public for ISO/IEC 27701:202X

Waiting AB (ANAB) approve for ISO/IEC 27701:202X

# Contact us

www.bsigroup.com/th-TH/

BSI Thailand

@bsithailand

Tel: 02 294 4889-92 Email: infothai@bsigroup.com