bsi.

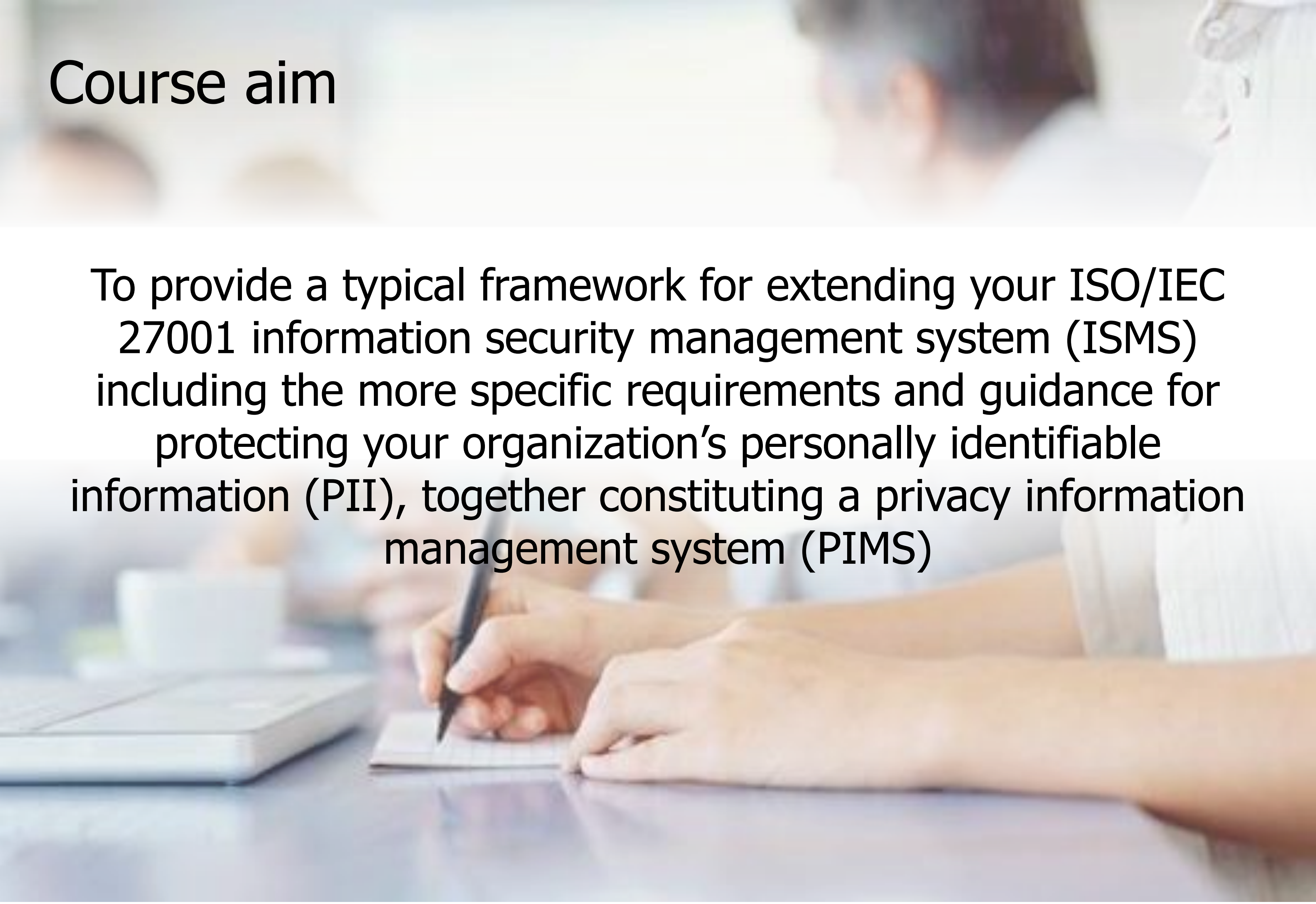
...making excellence a habit.™

ISO/IEC 27701:2019

Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for Privacy Information Management – Requirement and guidelines

By Royal Charter

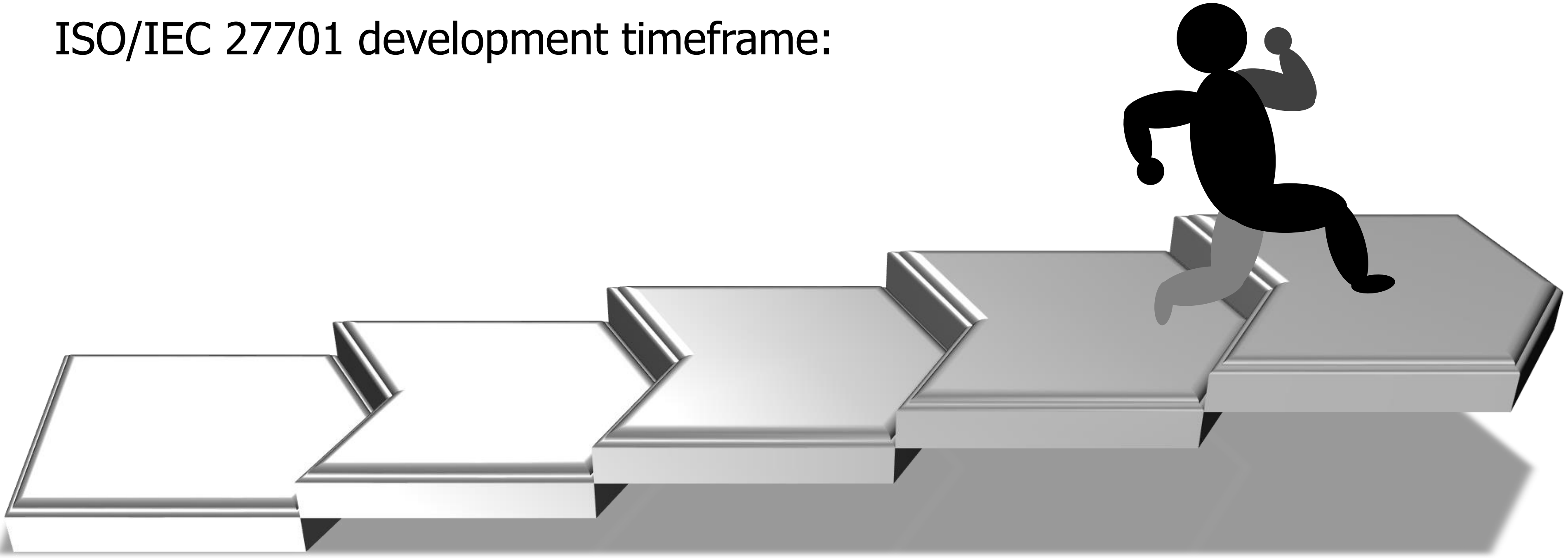
Course aim



To provide a typical framework for extending your ISO/IEC 27001 information security management system (ISMS) including the more specific requirements and guidance for protecting your organization’s personally identifiable information (PII), together constituting a privacy information management system (PIMS)

Reminder: Background of ISO/IEC 27701

ISO/IEC 27701 development timeframe:



2018 → **2019**

December 2018: Draft International Standard (DIS) made available and open for public comment for 3 months	**June 2019:** Final Draft International Standard (FDIS) made available	**August 2019:** Final Standard published

Benefits of implementing ISO/IEC 27701

Reduces complexity

Generates documentary evidence

Maps to GDPR and various frameworks

Provides assurance and confidence

Tailored to PII controllers and processors

bsi.

Reminder: Key terms and alternative terms

Terms as used in ISO/IEC 27701	Alternative term
Privacy information management system (PIMS)	Personal information management system (PIMS)
Personally identifiable information (PII)	Personal data
PII principal	Data subject
Privacy by design	Data protection by design
Privacy by default	Data protection by default
PII controller	Controller
PII processor	Processor

KEY Terms

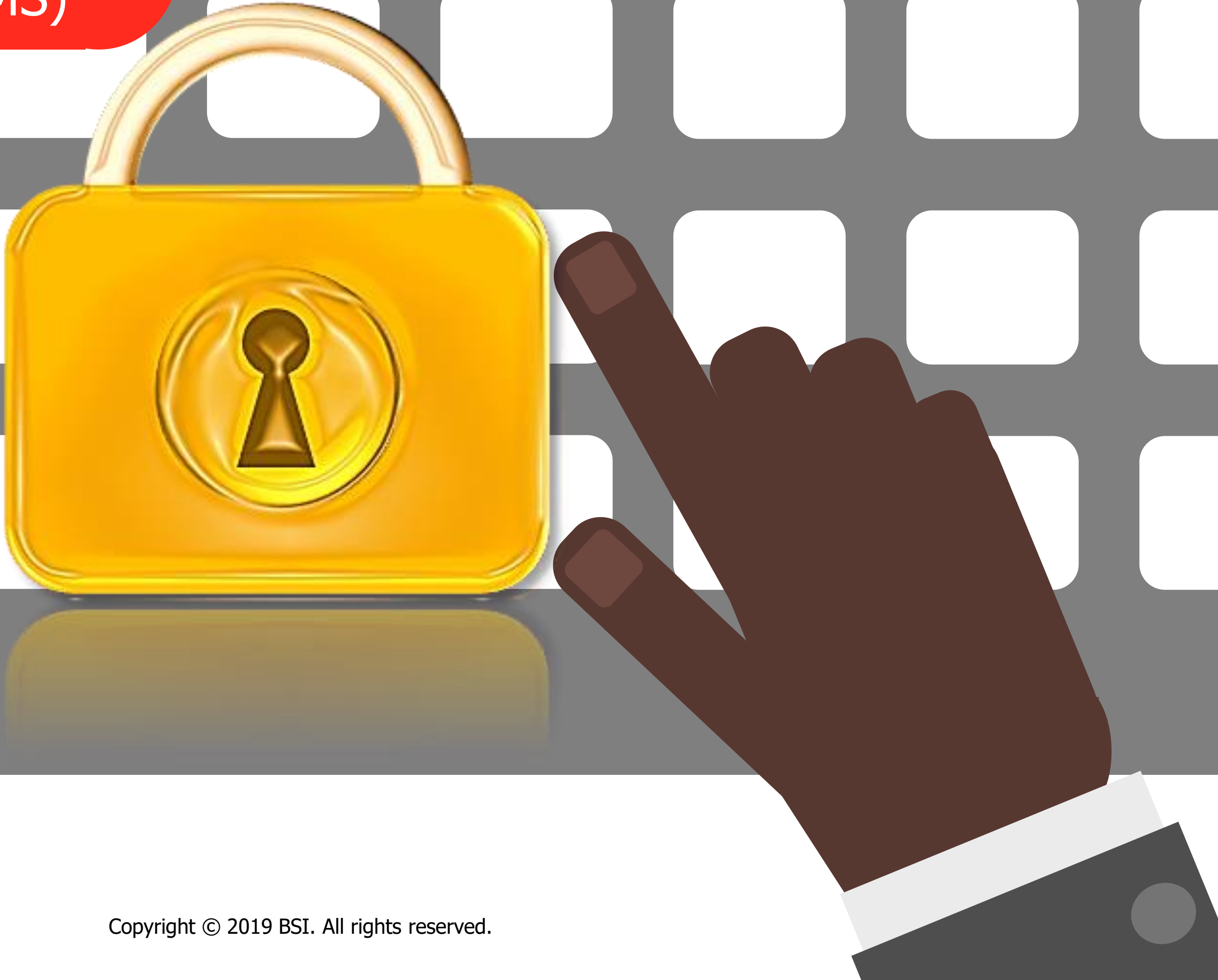
Term	Definition
Personally identifiable information (PII)	any information that (a) can be used to establish a link between the information and the natural person to whom such information relates, or (b) is or can be directly or indirectly linked to a natural person
Privacy information management system (PIMS)	information security management system which addresses the protection of privacy as potentially affected by the processing of PII
PII principal	natural person to whom the personally identifiable information (PII) relates

KEY Terms

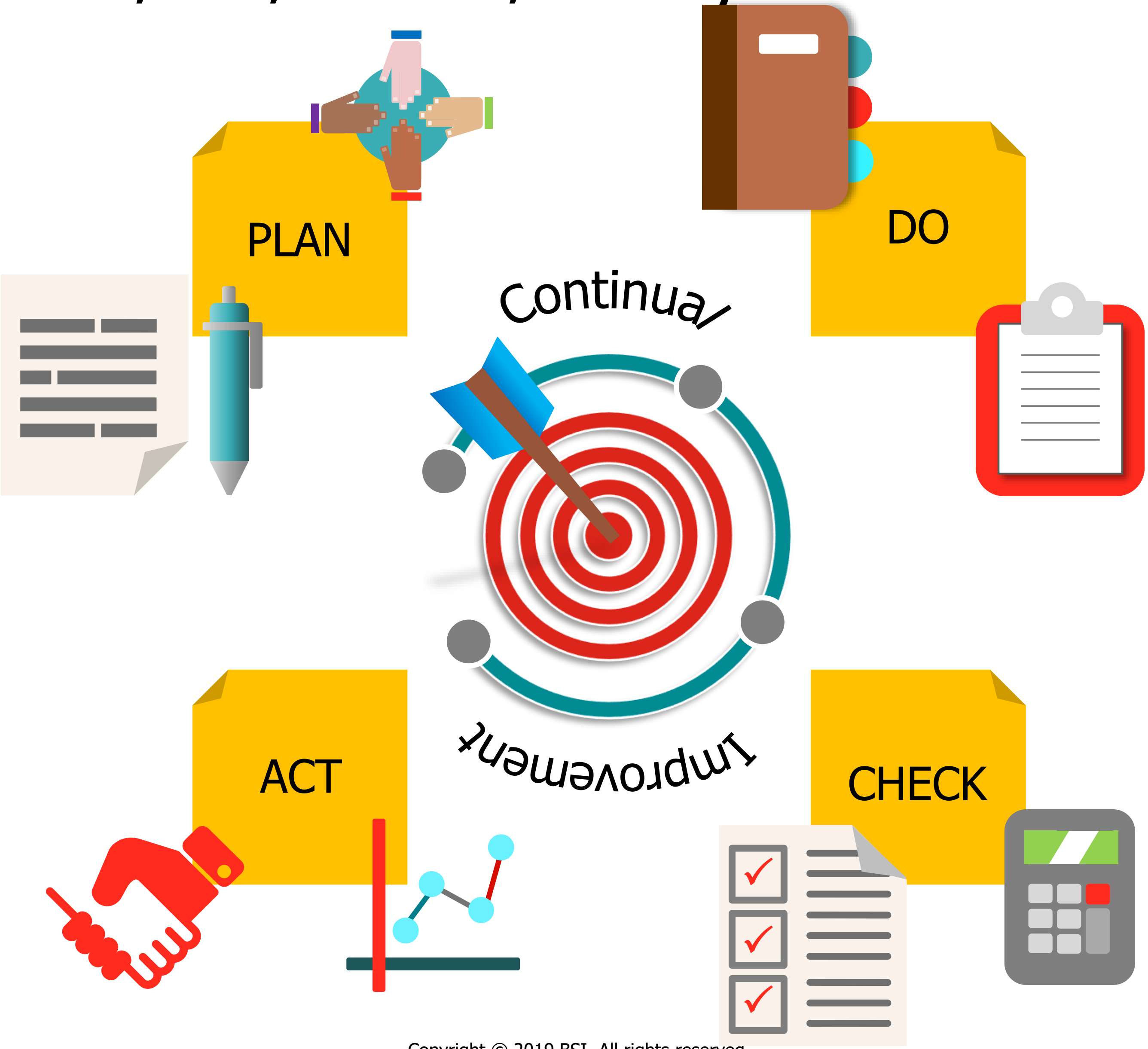
Term	Definition
PII controller	privacy stakeholder (or privacy stakeholders) that determines the purposes and means for processing personally identifiable information (PII) other than natural persons who use data for personal purposes
PII processor	privacy stakeholder that processes personally identifiable information (PII) on behalf of and in accordance with the instructions of a PII controller
privacy risk	effect of uncertainty on privacy
privacy impact assessment PIA privacy risk assessment	overall process of identifying, analyzing, evaluating, consulting, communicating and planning the treatment of potential privacy impacts with regard to the processing of personally identifiable information, framed within an organization's broader risk management framework

Reminder: What is a PIMS?

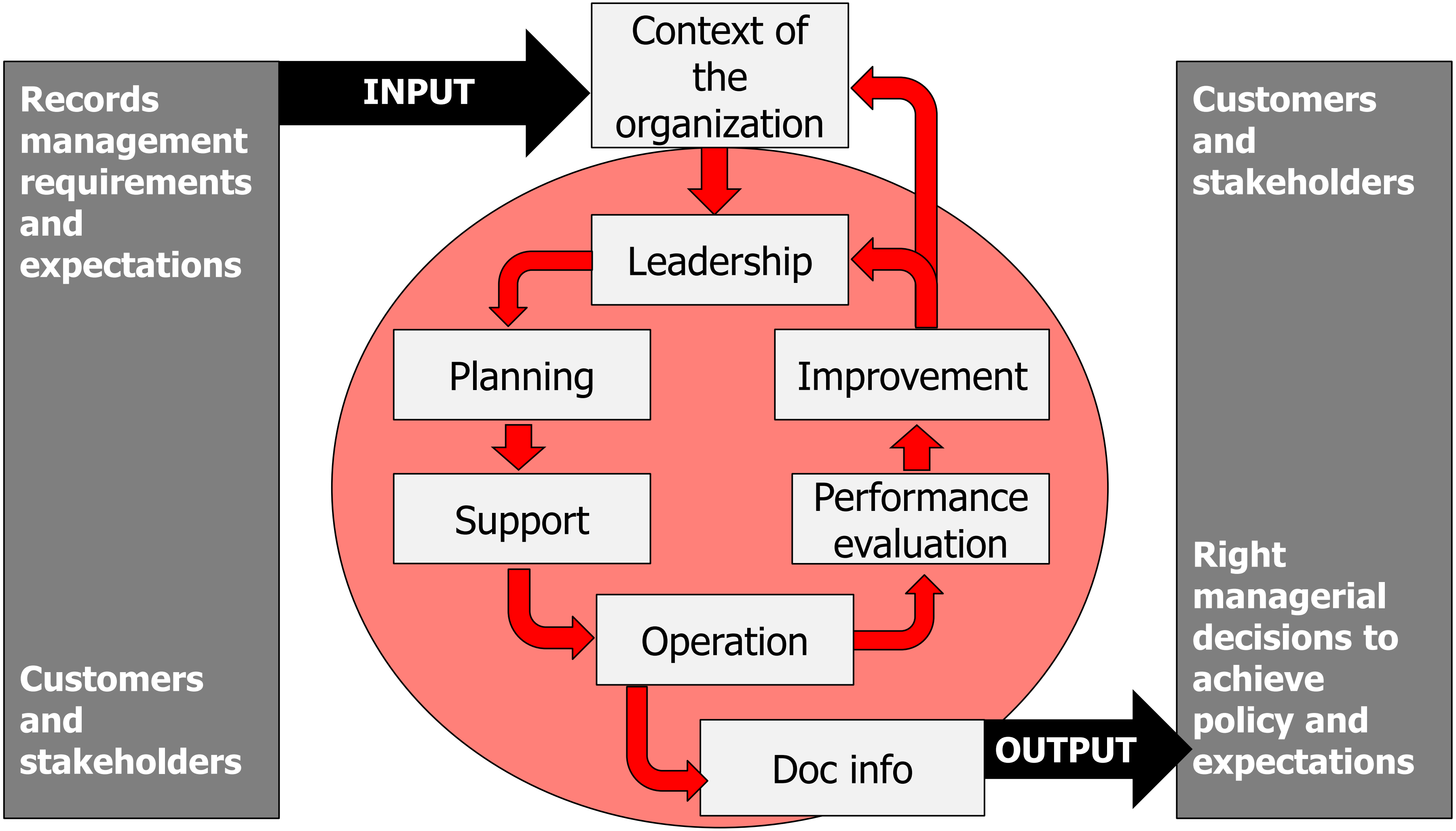
Privacy Information Management System (PIMS)



PIMS Plan, Do, Check, Act cycle



Integration – High level structure



Records management requirements and expectations

Customers and stakeholders

INPUT

Context of the organization

Leadership

Planning

Support

Operation

Doc info

Performance evaluation

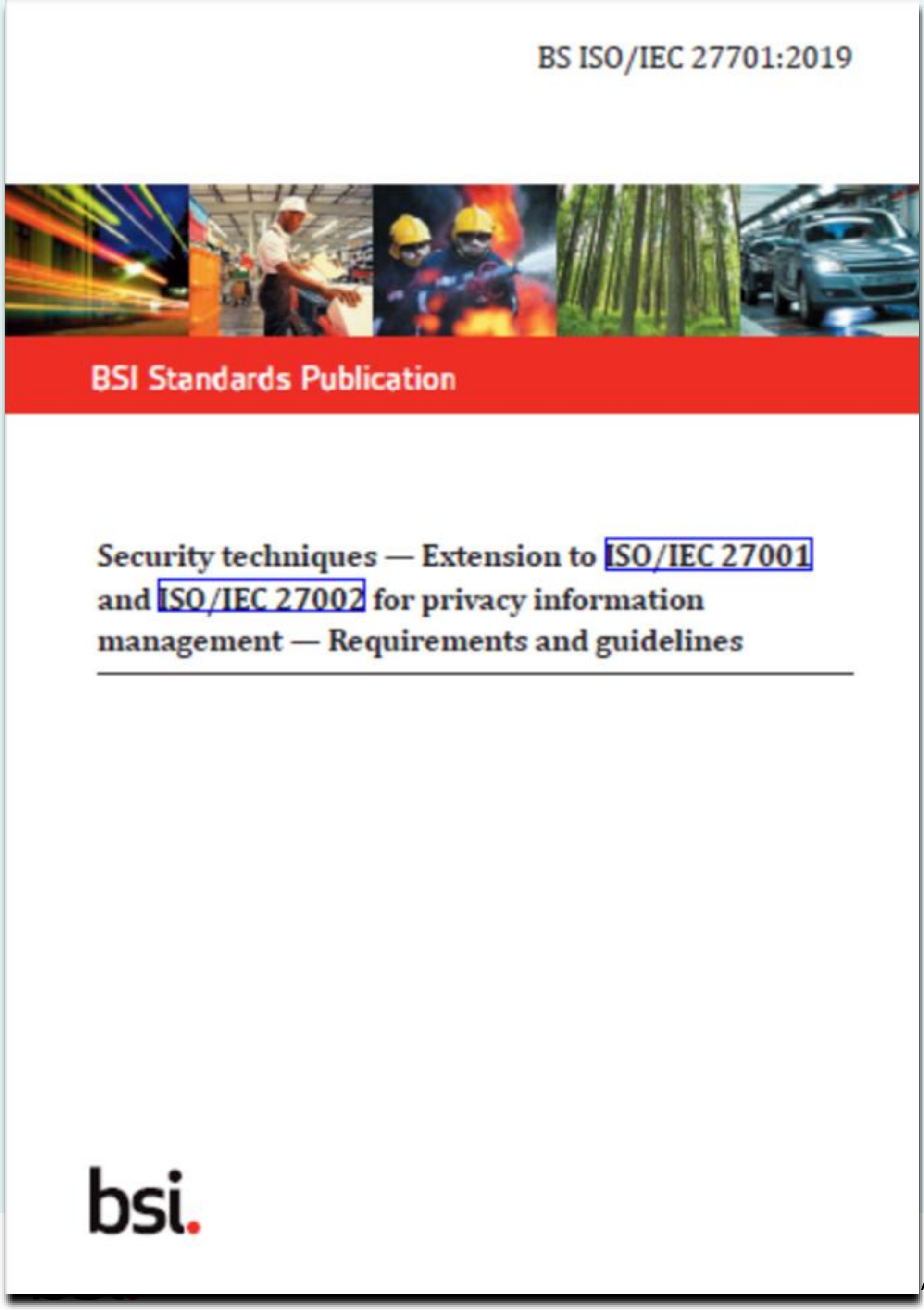
Improvement

OUTPUT

Customers and stakeholders

Right managerial decisions to achieve policy and expectations

Contents in ISO/IEC 27701



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

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

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

4 General

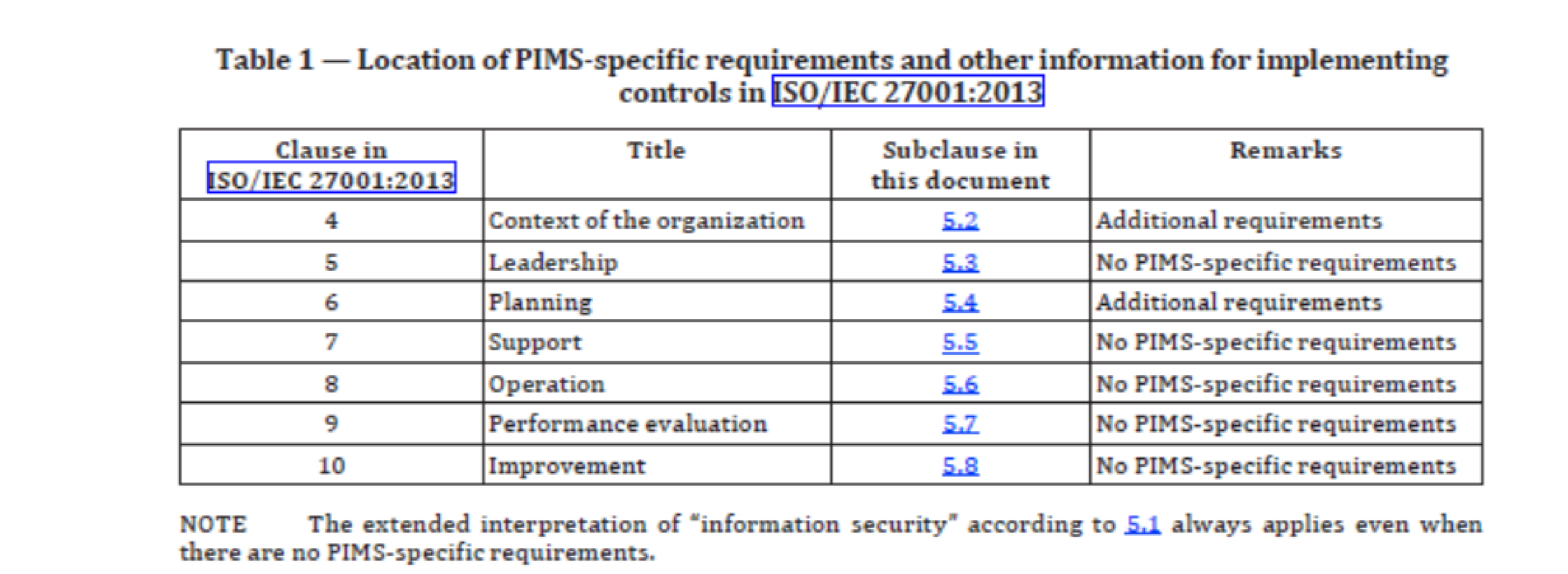


Table 1 — Location of PIMS-specific requirements and other information for implementing controls in ISO/IEC 27001:2013

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

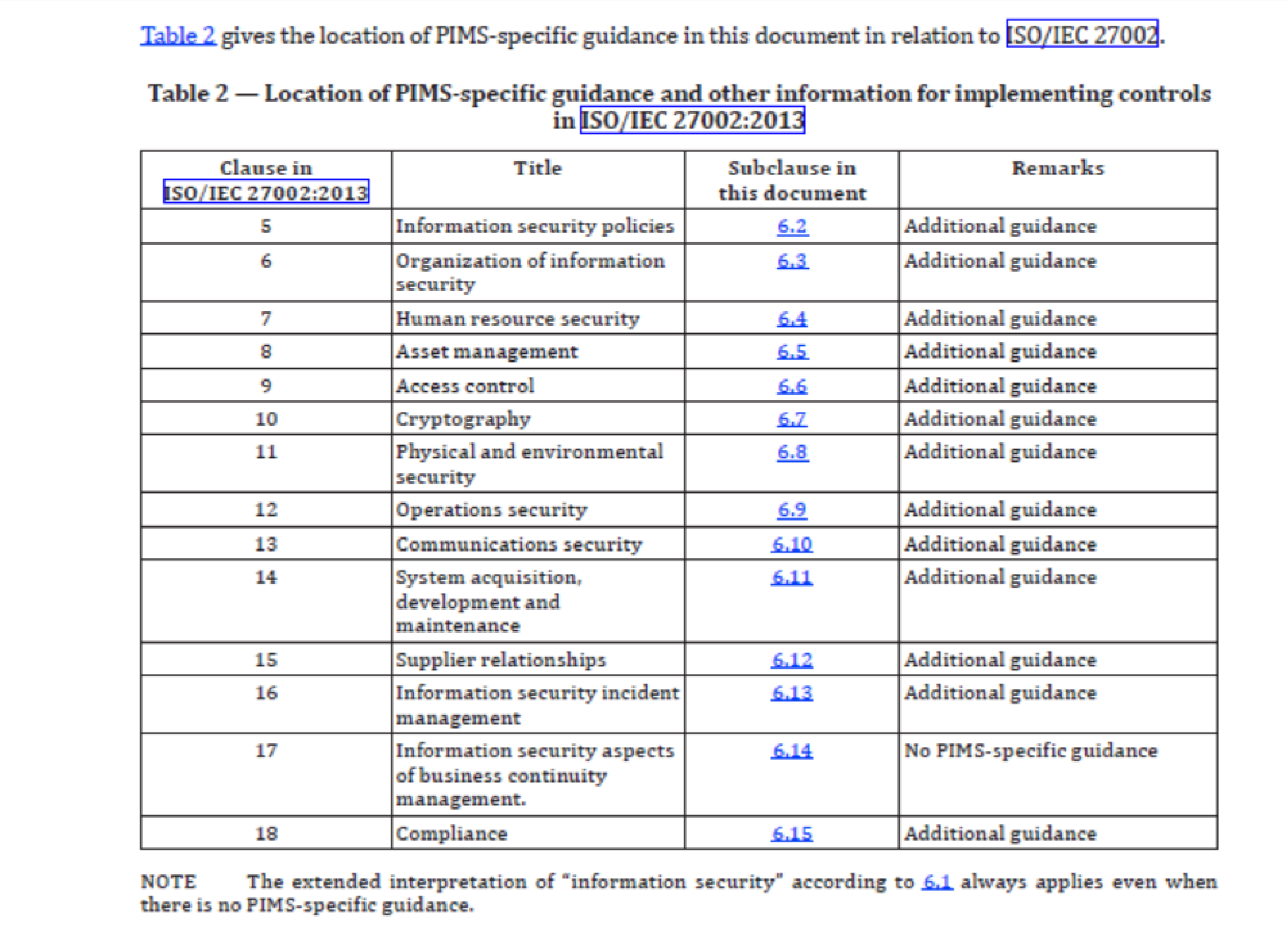


Table 2 gives the location of PIMS-specific guidance in this document in relation to ISO/IEC 27002.

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.

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.

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

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

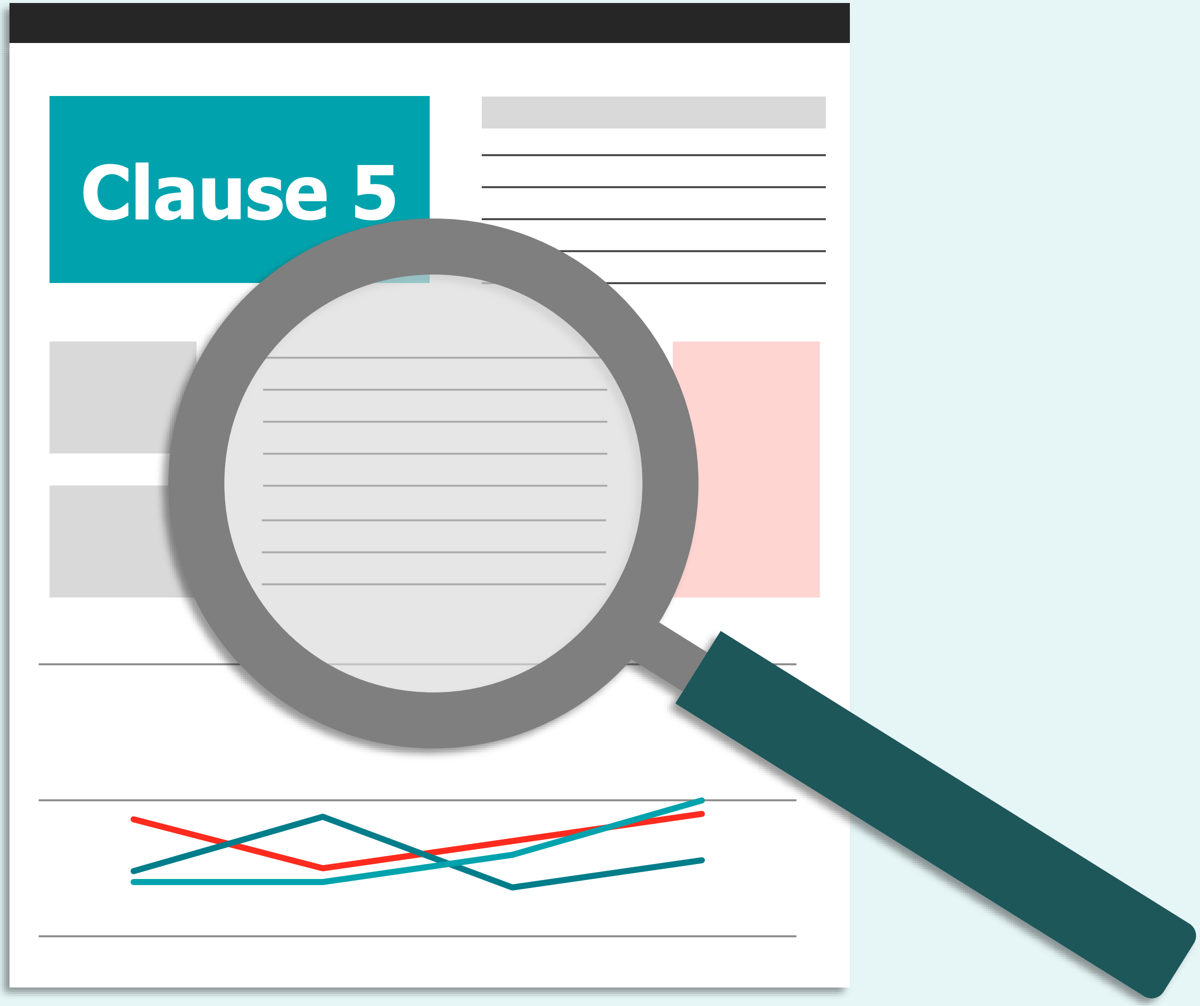
Clause 7: Additional ISO/IEC 27002 guidance for PII controllers

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

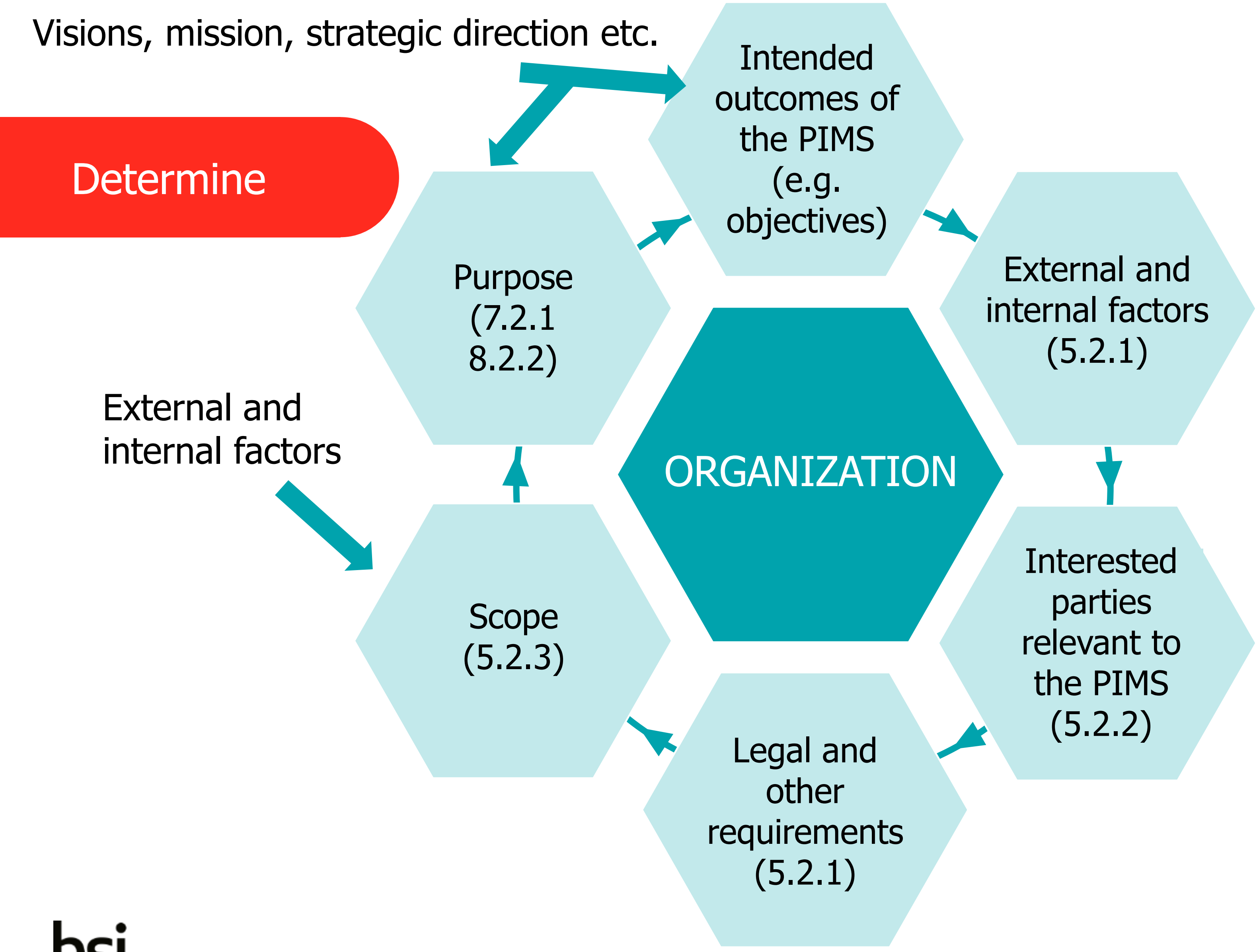
Annex A- F

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 Table C.1 — Mapping of controls for PII controllers and ISO/IEC 29100 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

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



Clause 5.2 Context of the organization


Visions, mission, strategic direction etc.
Determine
Intended outcomes of the PIMS (e.g. objectives)
Purpose (7.2.1 8.2.2)
External and internal factors (5.2.1)
External and internal factors
ORGANIZATION
Scope (5.2.3)
Interested parties relevant to the PIMS (5.2.2)
Legal and other requirements (5.2.1)

Clause 5.3 Leadership

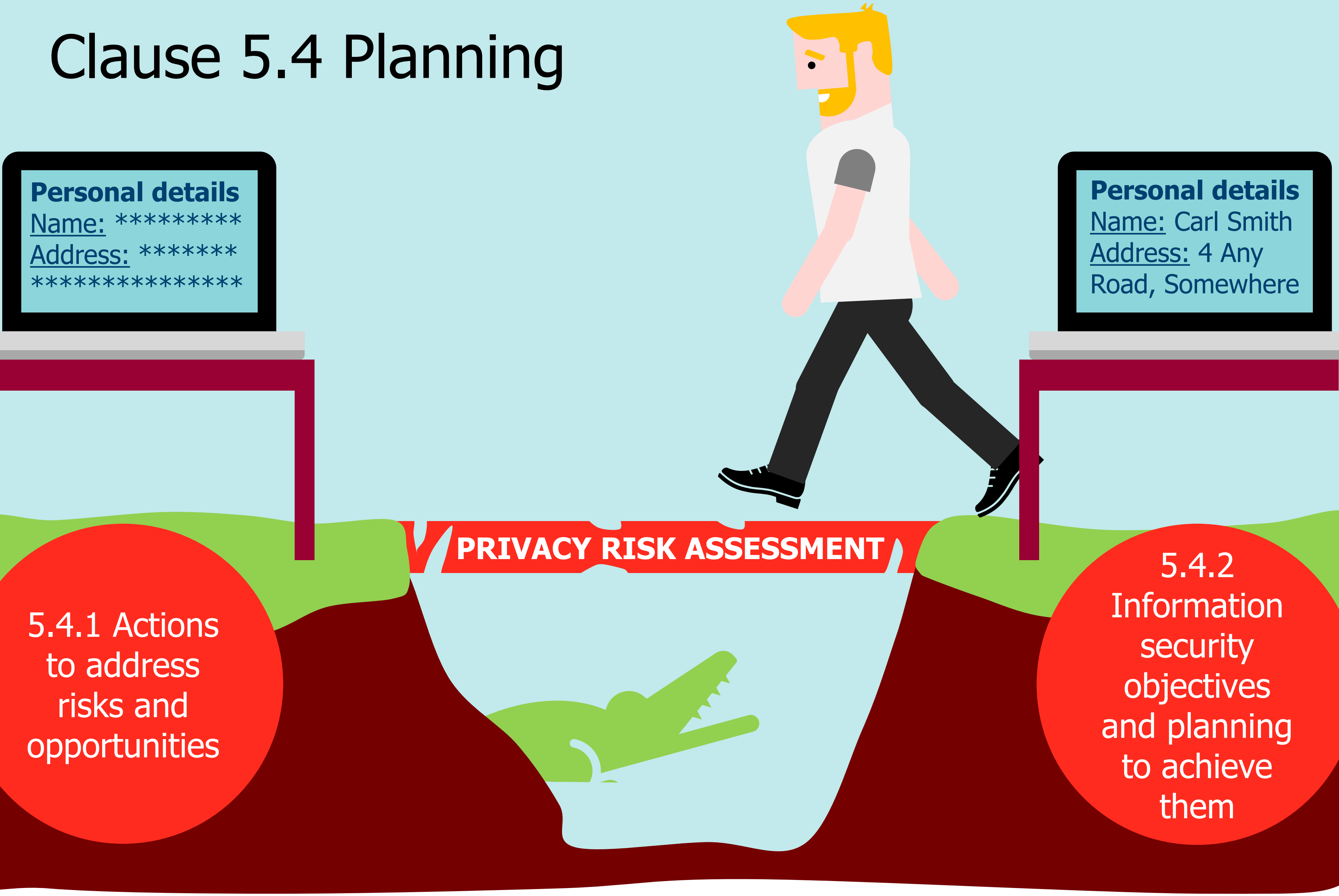
Leadership and commitment

Policy

Organizational roles, responsibilities and authorities

Embedding the PIMS in the organization’s culture

Clause 5.4 Planning



Personal details
Name: *********
Address: *******
****

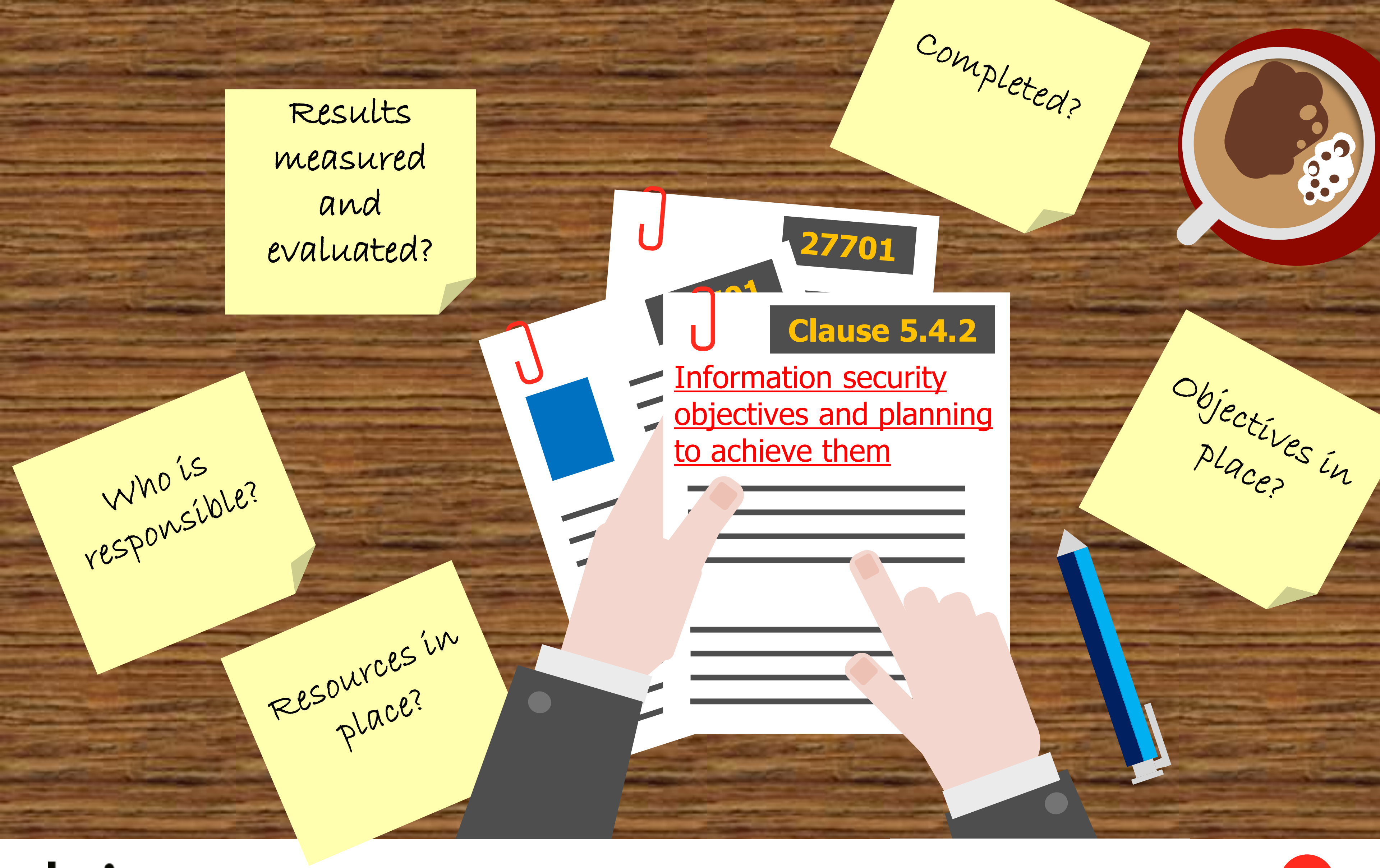
Personal details
Name: Carl Smith
Address: 4 Any
Road, Somewhere

PRIVACY RISK ASSESSMENT

5.4.1 Actions to address risks and opportunities

5.4.2 Information security objectives and planning to achieve them

Clause 5.4 Planning



Results measured and evaluated?

Completed?

27701

Clause 5.4.2

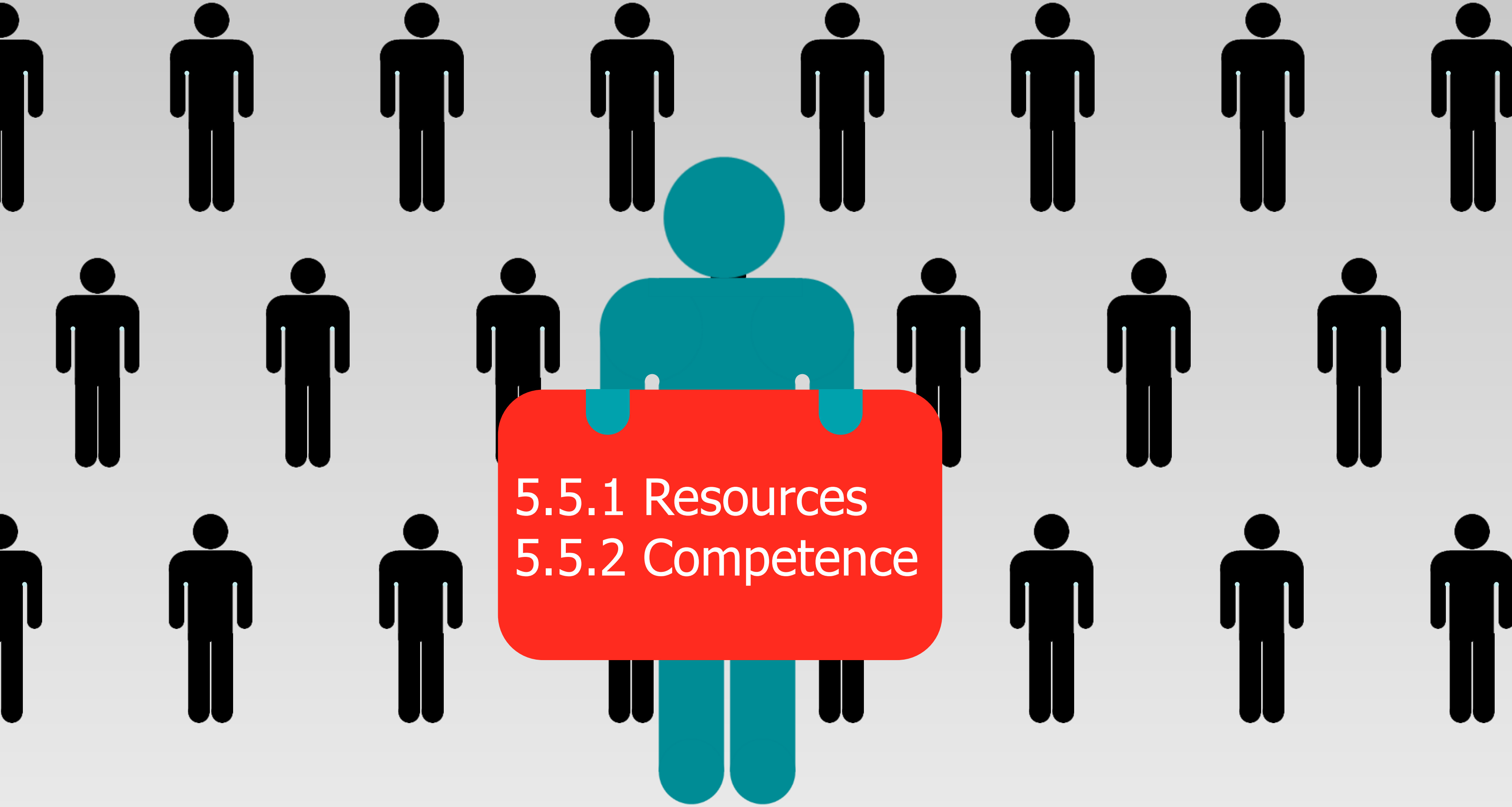
Information security objectives and planning to achieve them

Who is responsible?

Objectives in place?

Resources in place?

Clause 5.5 Support



5.5.1 Resources

5.5.2 Competence

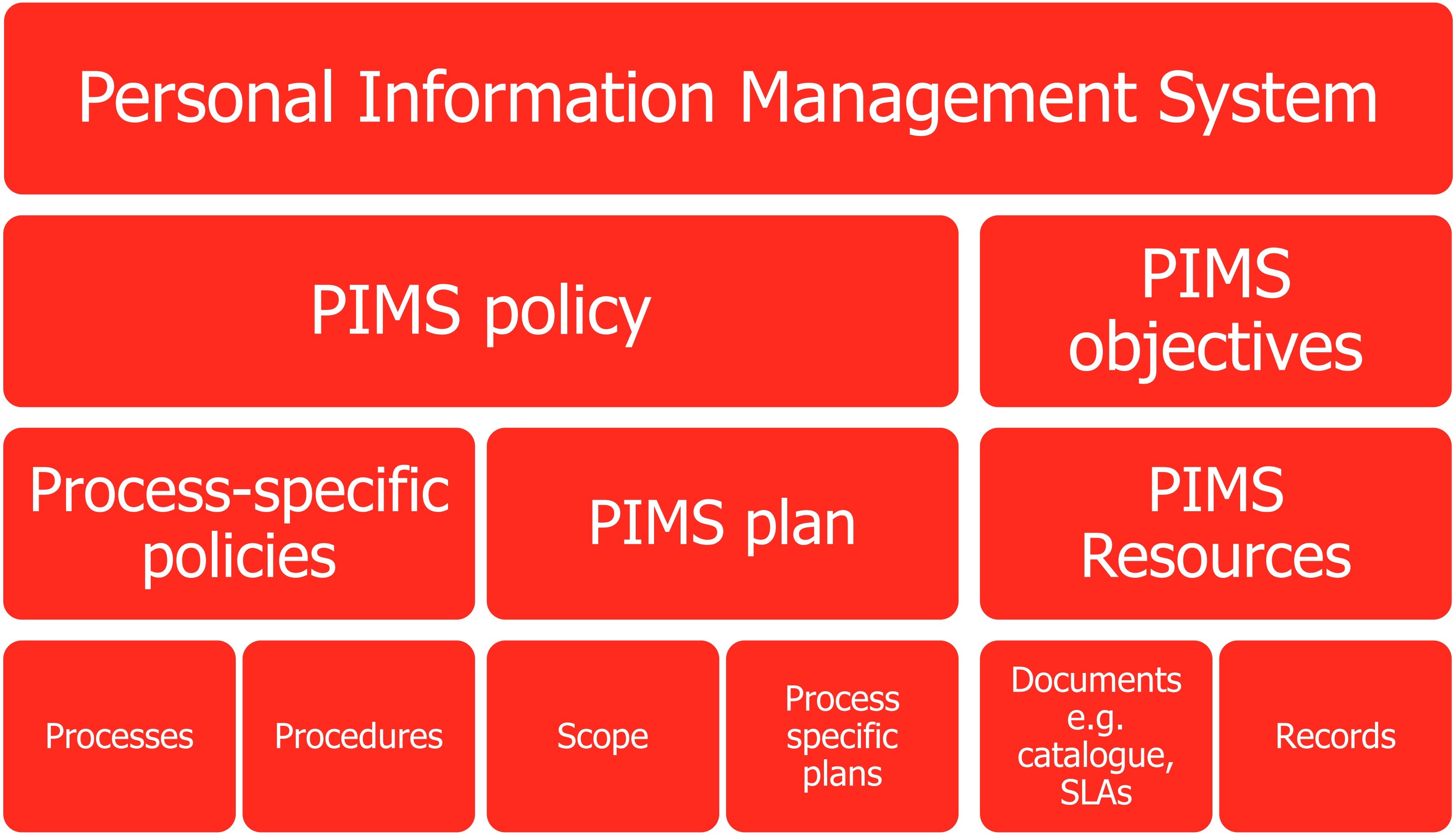
Clause 5.5 Support

5.5.3 Awareness

5.5.4 Communication

5.5.5 Documented information

Clause 5.5.5 Documented information



Personal Information Management System

PIMS policy

PIMS objectives

Process-specific policies

PIMS plan

PIMS Resources

Processes

Procedures

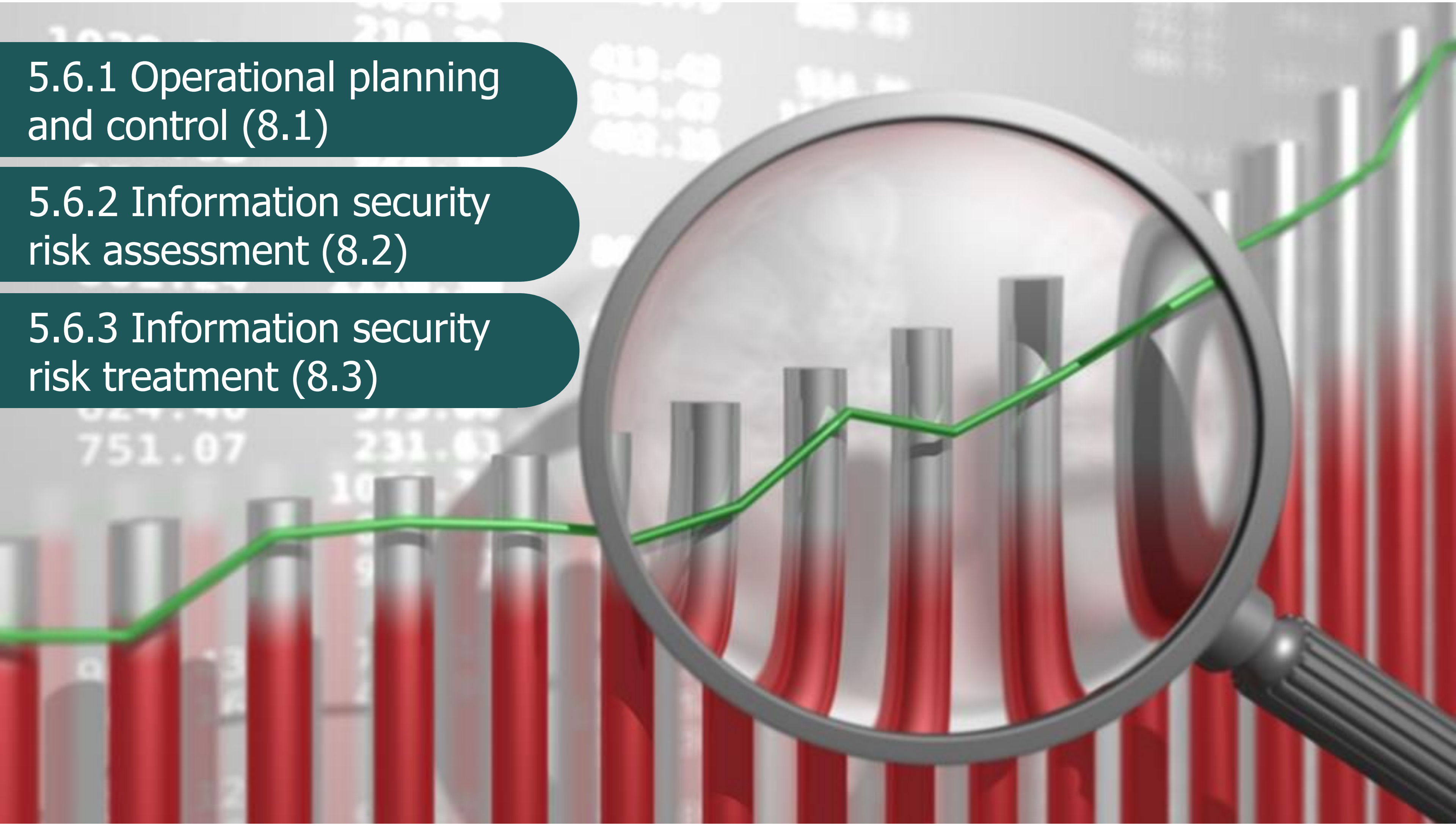
Scope

Process specific plans

Documents e.g. catalogue, SLAs

Records

Clause 5.6 subclauses



5.6.1 Operational planning and control (8.1)

5.6.2 Information security risk assessment (8.2)

5.6.3 Information security risk treatment (8.3)

Clause 5.7 Performance evaluation

Clause 5.7.1: Monitoring, measuring, analysis and evaluation (9.1)

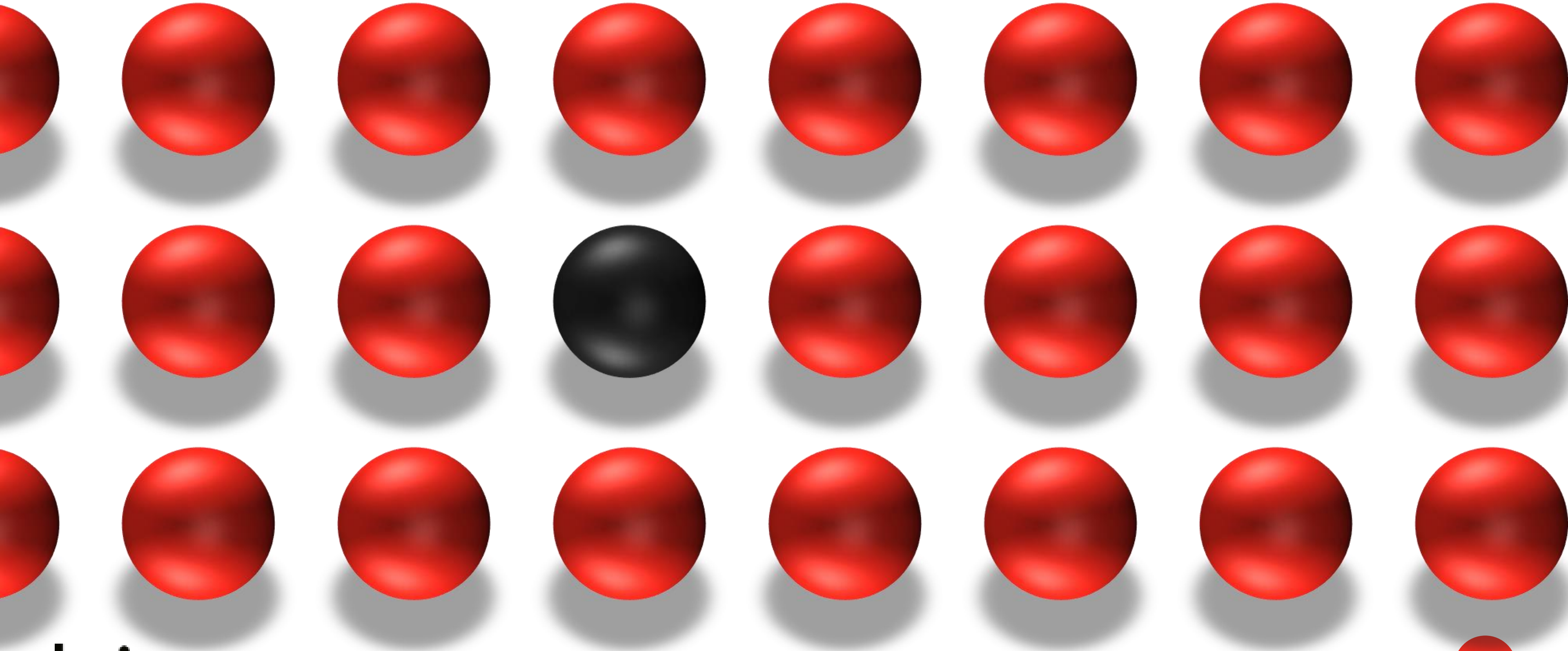
5.7.2 Internal audit (9.2)

5.7.2 Management review (9.3)

Clause 5.8.1 and Clause 5.8.2

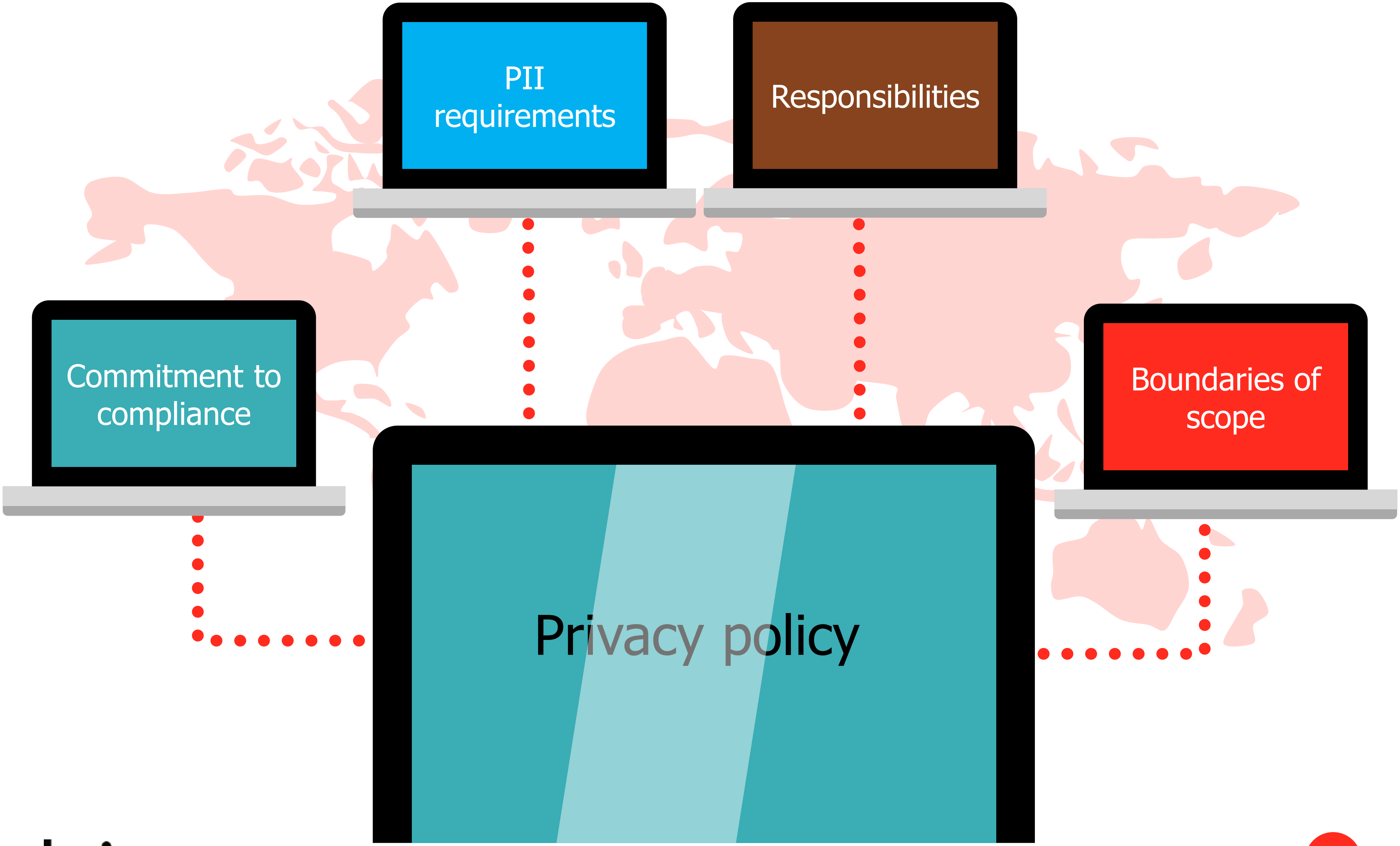
5.8.1 Nonconformity and corrective action (10.1)

5.8.2 Continual improvement (10.2)



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

Clause 6.2 Information security policies



PII requirements

Responsibilities

Commitment to compliance

Boundaries of scope

Privacy policy

Clause 6.4 Human resource security

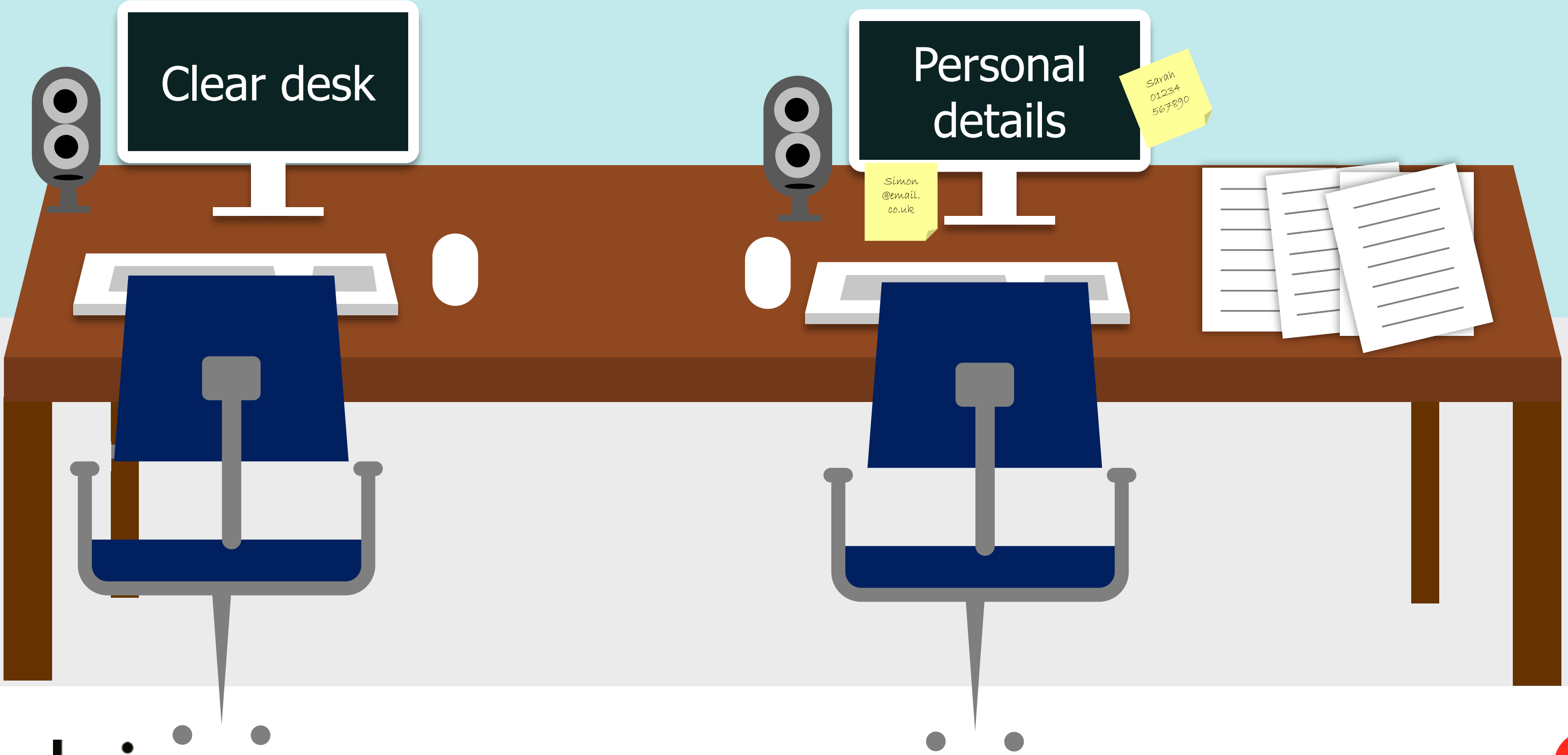
6.4.2.2 Information security, awareness, education and training

Clause 6.7 Cryptography and Clause 6.8 Physical and environmental security

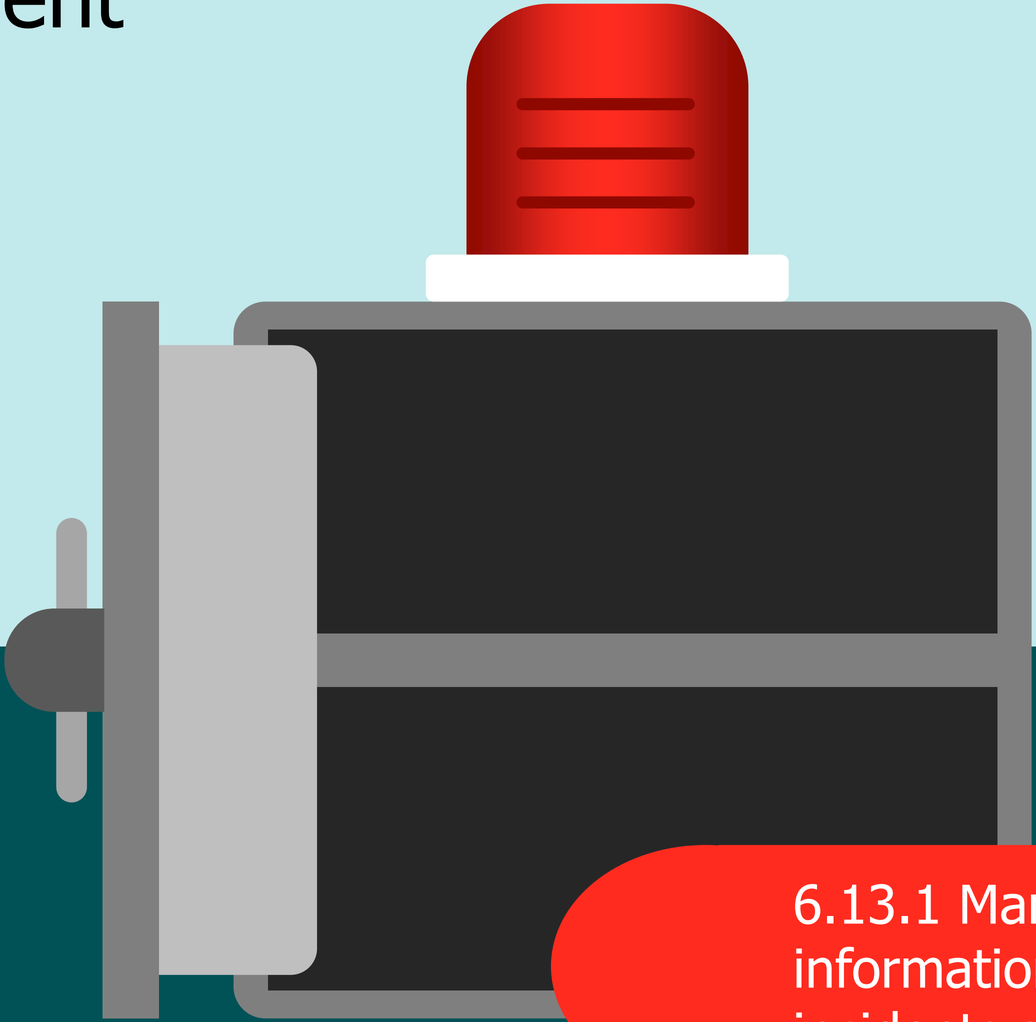
6.7.1 Cryptographic controls

6.8.2.7 Secure disposal or re-use of equipment

6.8.2.9 Clear desk and clear screen policy



Clause 6.13 Information security incident management



6.13.1 Management of information security incidents and improvements

Clause 6.13 Information security incident management

How to recognize a PII breach/ security incident

NEWS TODAY

Friday 25th October 20XX

£0.65

BREACH!

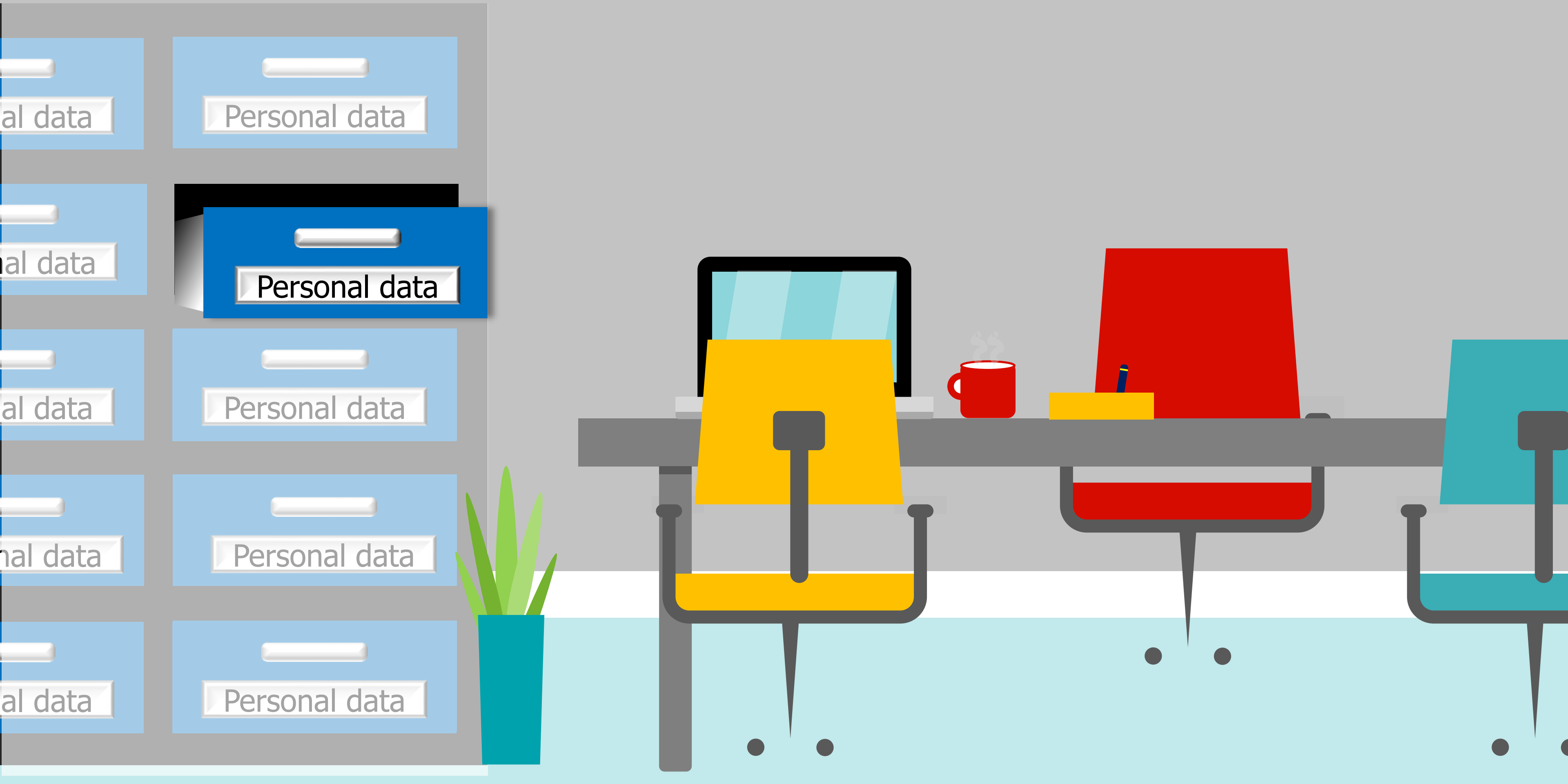
PII leak in top firm

Vivamus venenatis ornare tortor in tempor.

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Quisque id posuere arcu, et convallis justo. Integer sed ex feugiat, accumsan est a, elementum leo.

Sed id lacus a tortor gravida maximus quis sed lacus. Nam sit amet elit vehicula, vestibulum eros ut, hendrerit metus. Phasellus rutrum

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



Clause 7.2 Conditions for collection and processing

GDPR

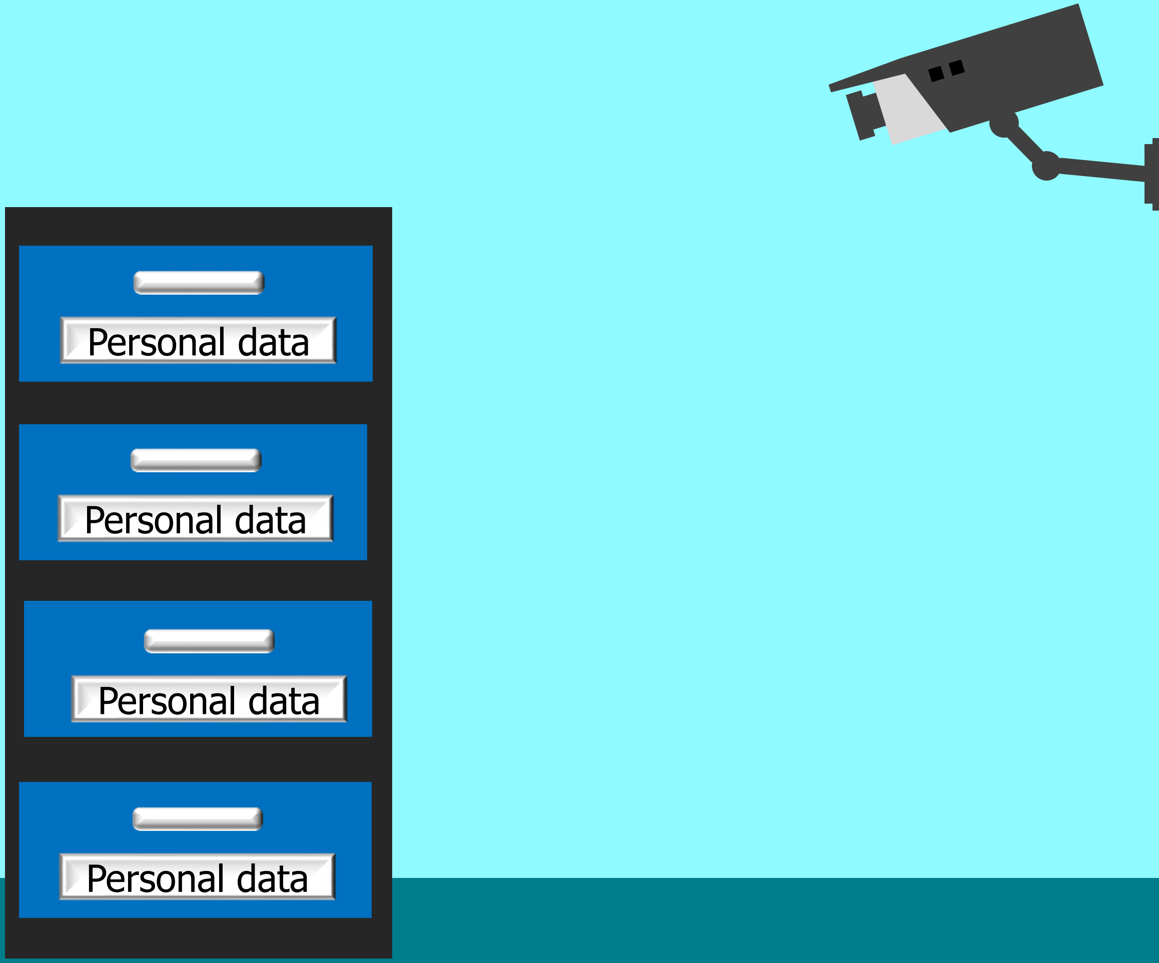
Article 6

7.2.1 Identify and document purpose

7.2.2 Identify lawful basis

Clause 7 Obligations to PII principals

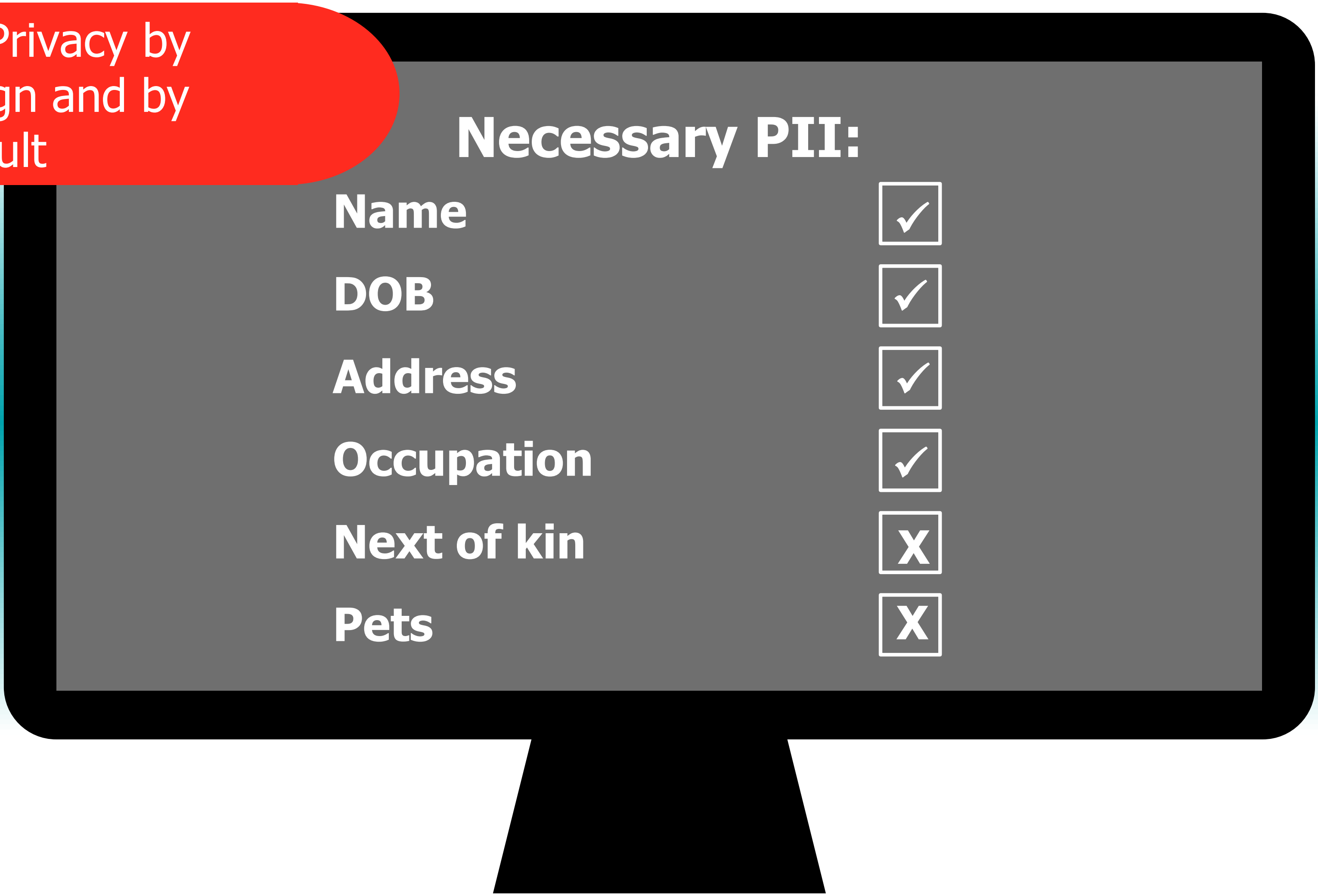
7.3 Obligations to PII principals



Clause 7.4 Privacy by design and by default

Clause 7.4 Privacy by design and by default

7.4 Privacy by design and by default



Necessary PII:

Name	☑
DOB	☑
Address	☑
Occupation	☑
Next of kin	☒
Pets	☒

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

Clause 8 Conditions for collection and processing

8.2.1 Cooperation agreement

Clause 8.4 Privacy by design and privacy by default

8.4.2 Return, transfer or disposal of PII (1)

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

Summary
Contents in ISO/IEC 27701

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

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

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

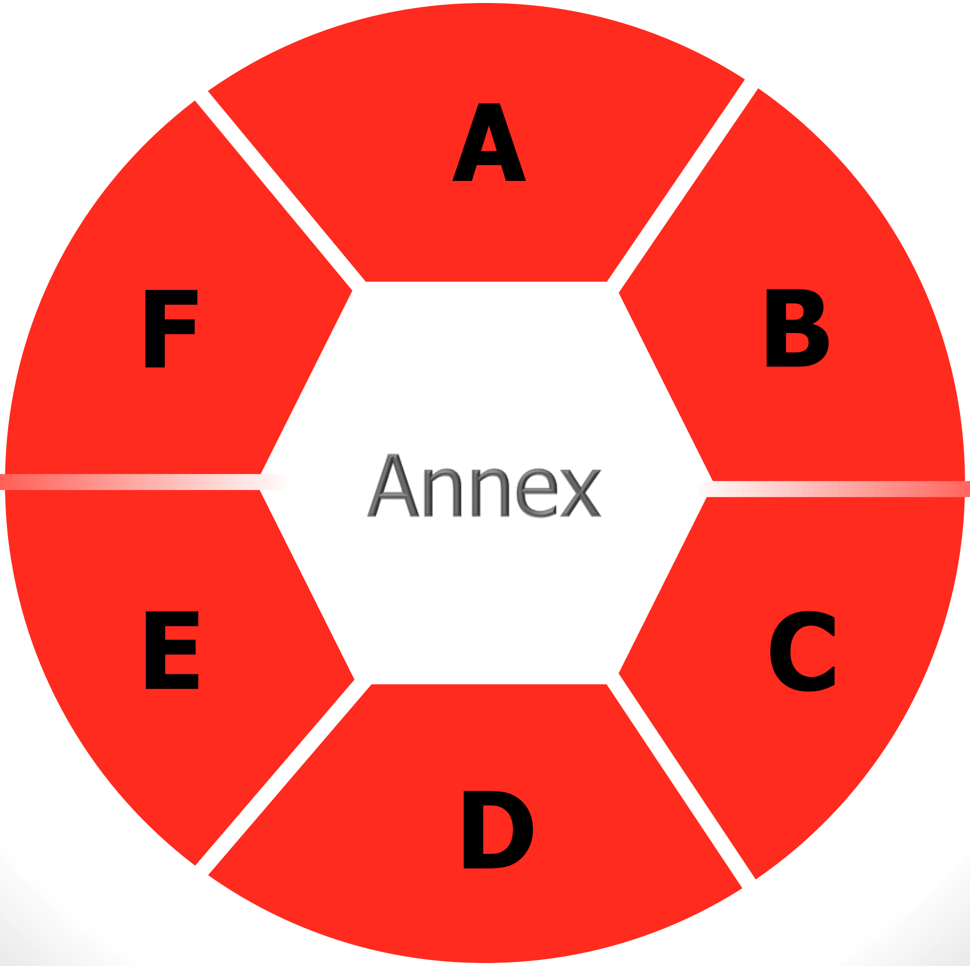
Clause 6: PIMS-specific guidance related to ISO/IEC 27002

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

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

Annexes

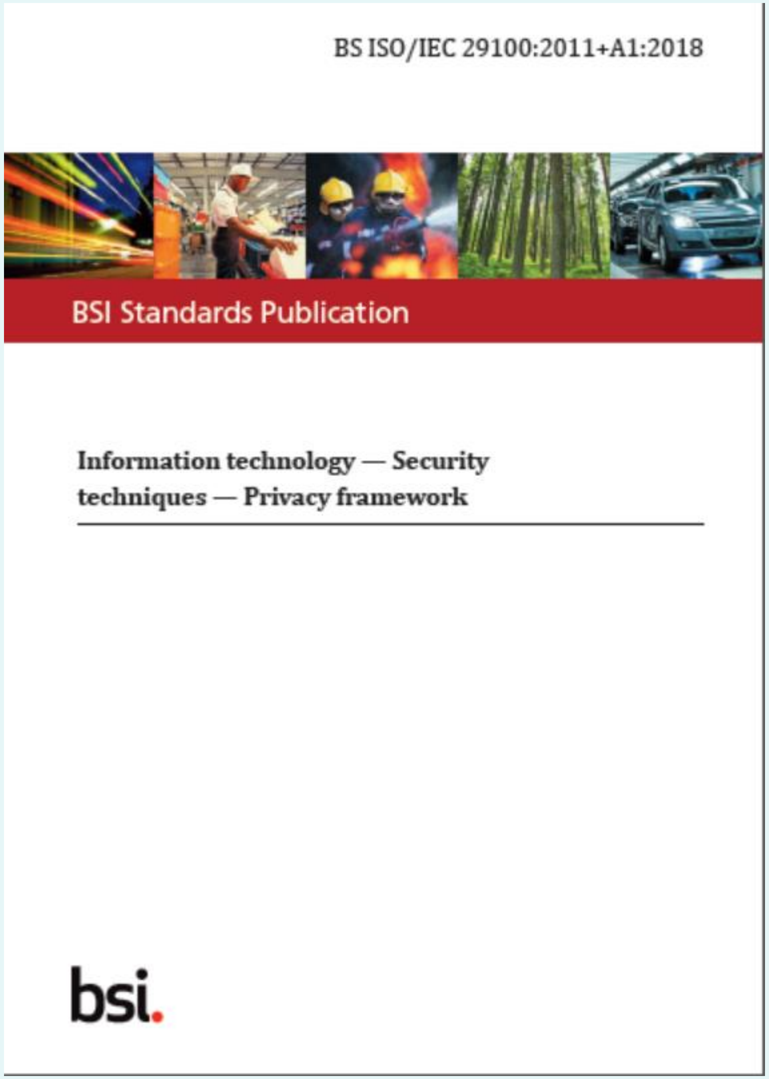
Annexes A-F



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 Table C.1 — Mapping of controls for PII controllers and ISO/IEC 29100 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

Related Standard

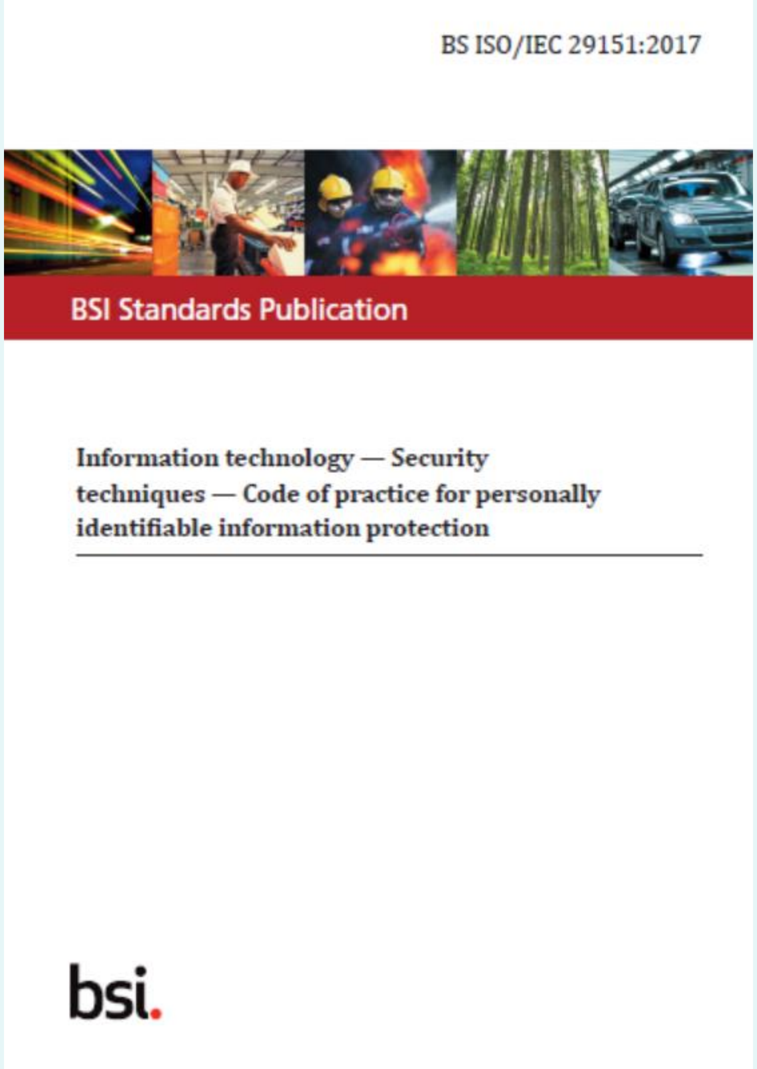


BS ISO/IEC 29100:2011+A1:2018

BSI Standards Publication

Information technology — Security techniques — Privacy framework

bsi.



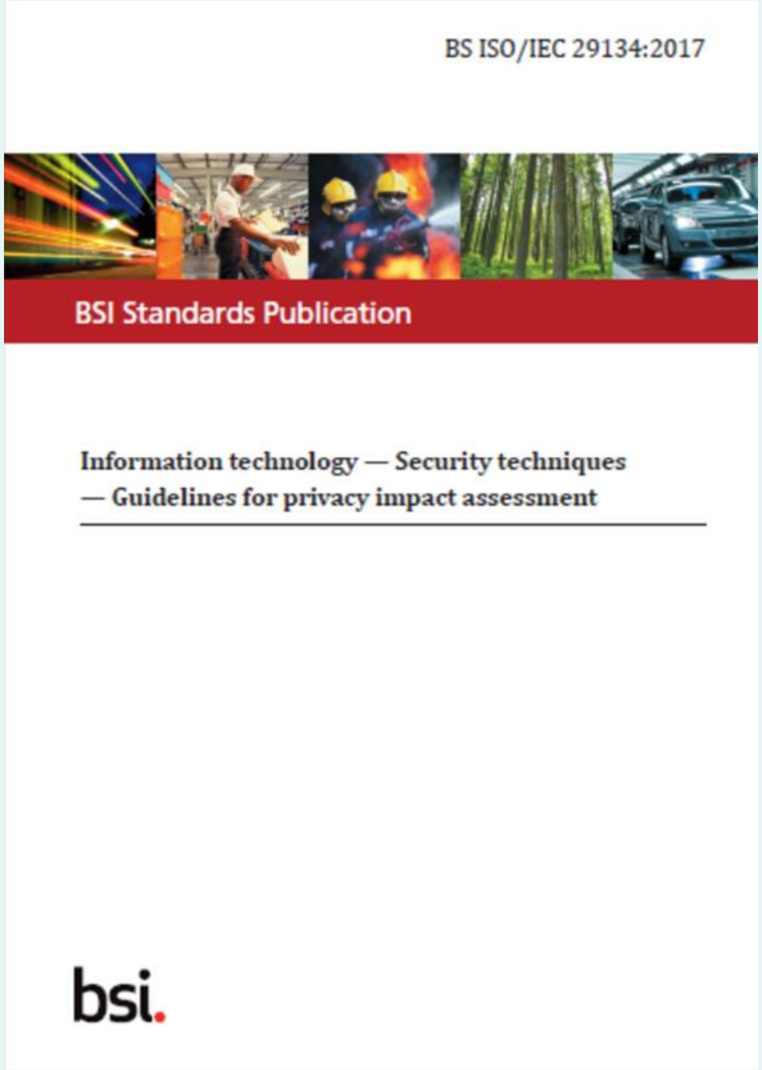
BS ISO/IEC 29151:2017

BSI Standards Publication

Information technology — Security techniques — Code of practice for personally identifiable information protection

bsi.

Related Standard

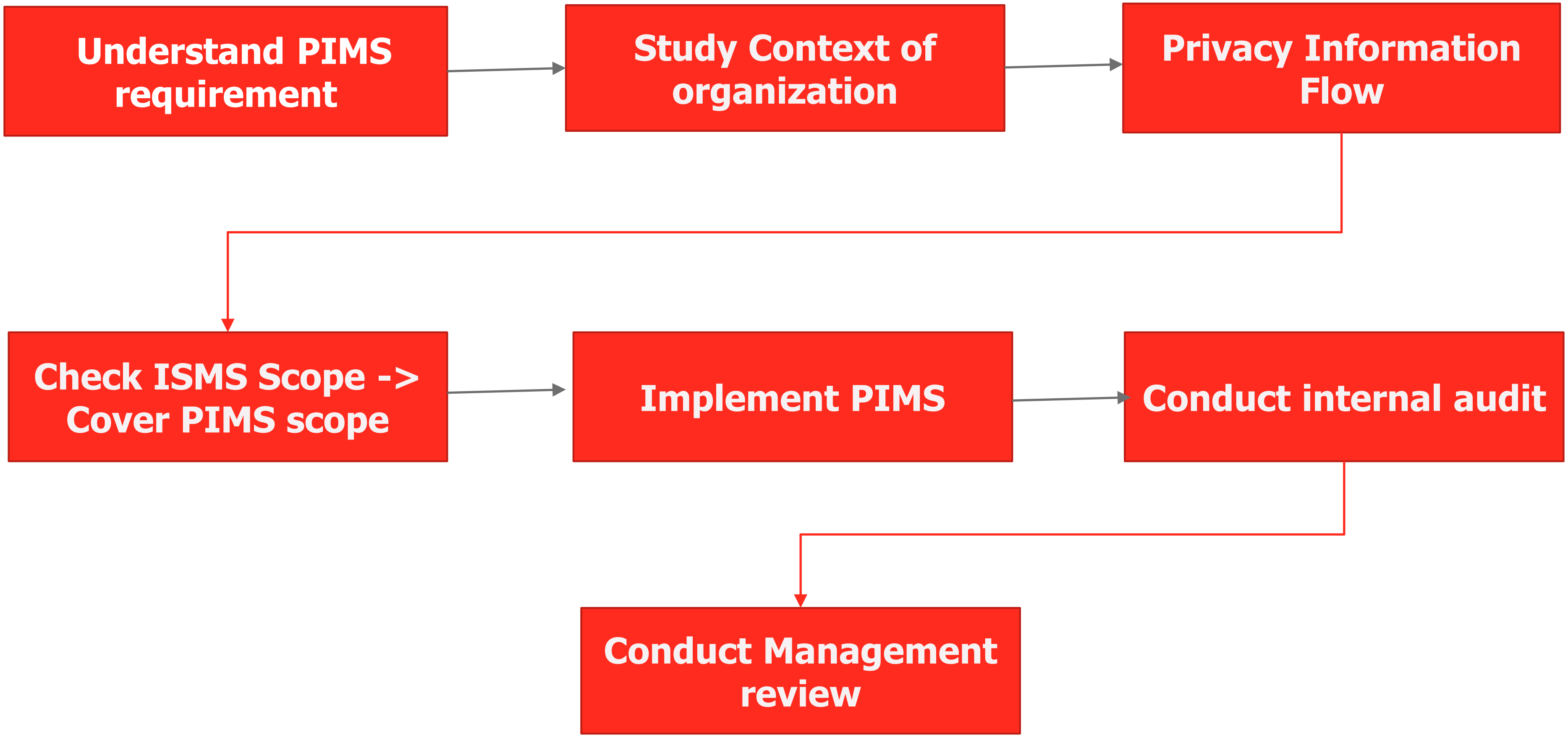


BS ISO/IEC 29134:2017

BSI Standards Publication

Information technology — Security techniques
— Guidelines for privacy impact assessment

Implement for PIMS



Understand PIMS requirement

Study Context of organization

Privacy Information Flow

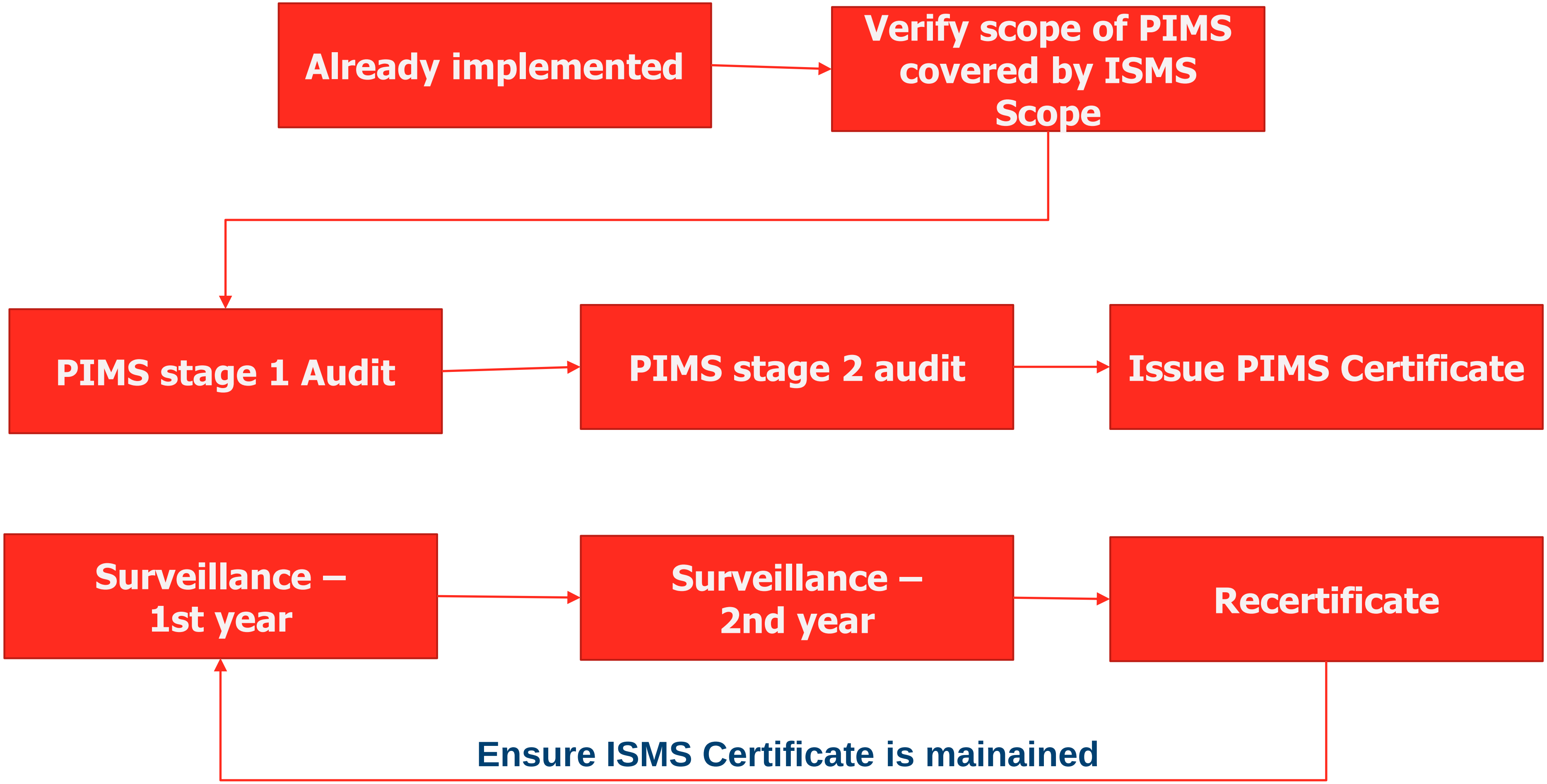
Check ISMS Scope -> Cover PIMS scope

Implement PIMS

Conduct internal audit

Conduct Management review

Certify for PIMS



Already implemented

Verify scope of PIMS covered by ISMS Scope

PIMS stage 1 Audit

PIMS stage 2 audit

Issue PIMS Certificate

Surveillance – 1st year

Surveillance – 2nd year

Recertificate

Ensure ISMS Certificate is mainained

Course review and final questions

?

bsi.

...making excellence a habit.™