Your partner
in progress

What is Cloud standard for ISO/IEC 27017 and ISO/IEC 27018?

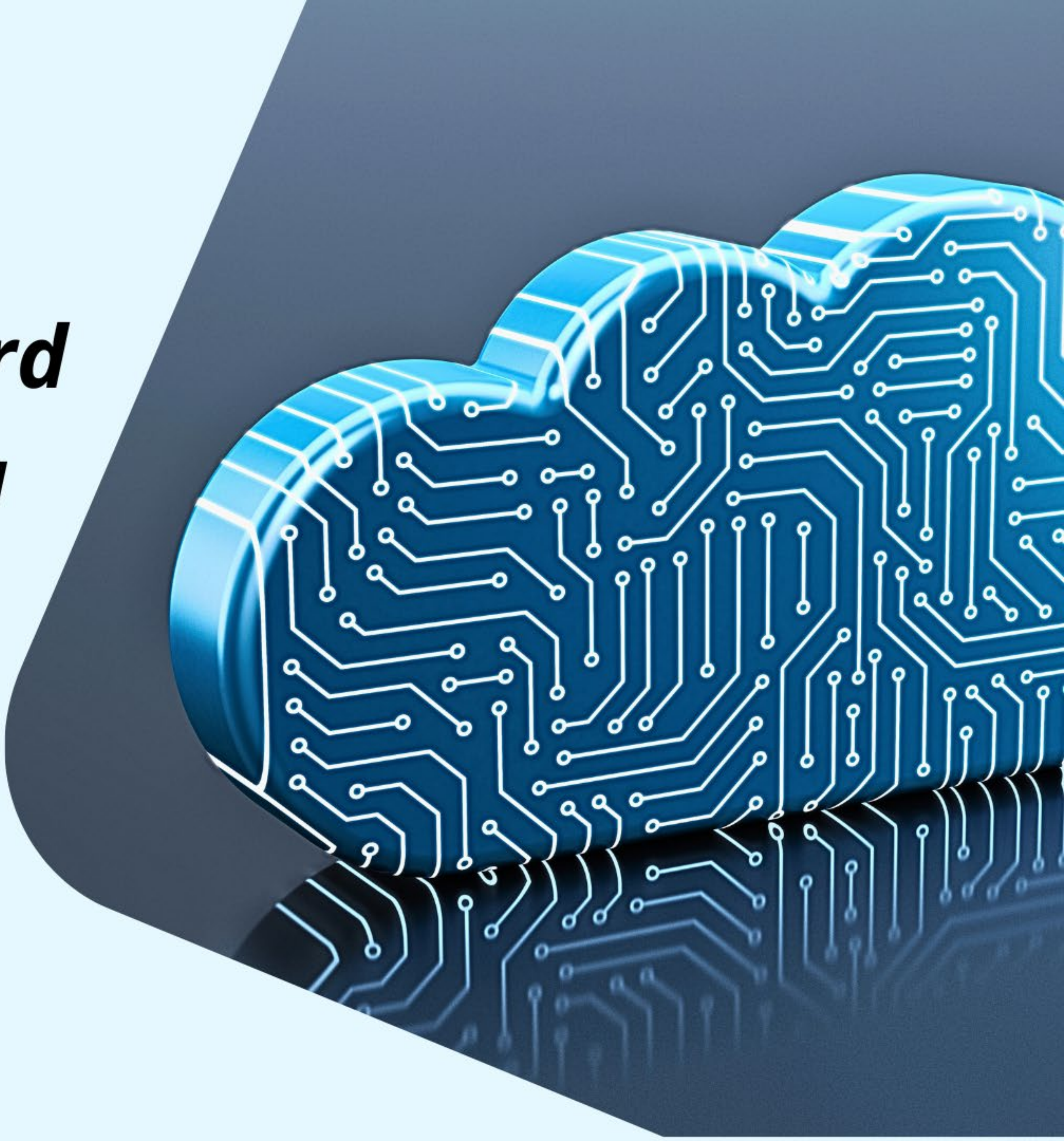
Webinar

บรรยายโดย

อาจารย์กิตติพงษ์ เกียรตินิยมรุ่ง

Product Technical Manager, BSI Thailand

สถาบันมาตรฐานอังกฤษ (BSI)



Agenda

01 ISO/IEC 27017, ISO/IEC 27018 requirement

02 Implement ISO/IEC 27017 and ISO/IEC 27018

03 Certify ISO/IEC 27017 and ISO/IEC 27018

04 Q & A

ISO/IEC 27017

ISO/IEC 27018

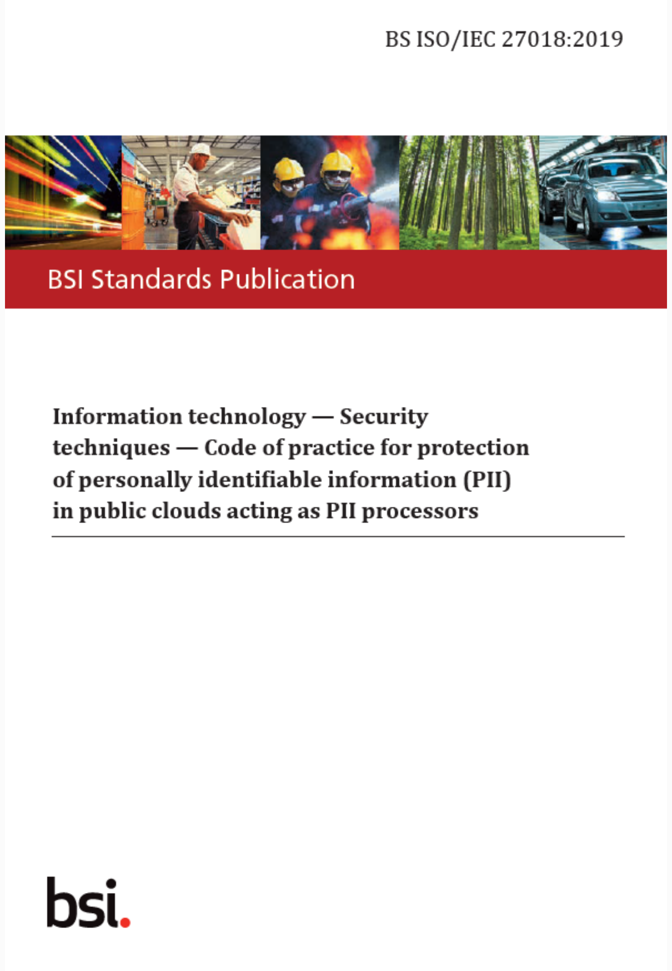
ISO/IEC 27017:2015 and ISO/IEC 27018:2019

BS ISO/IEC 27017:2015

BSI Standards Publication

Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services

...making excellence a habit.™

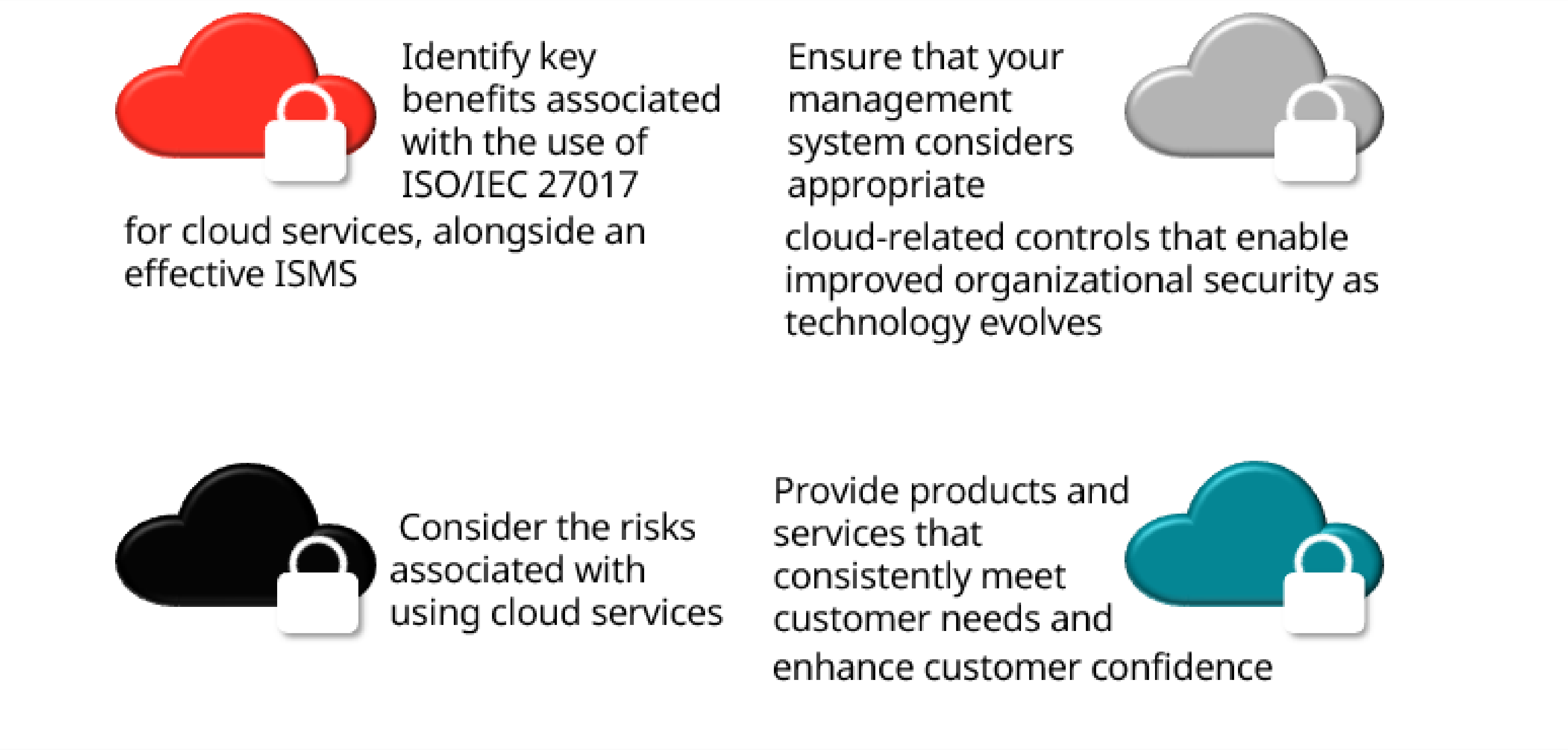


BS ISO/IEC 27018:2019

BSI Standards Publication

Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

Benefits to you ISO/IEC 27017



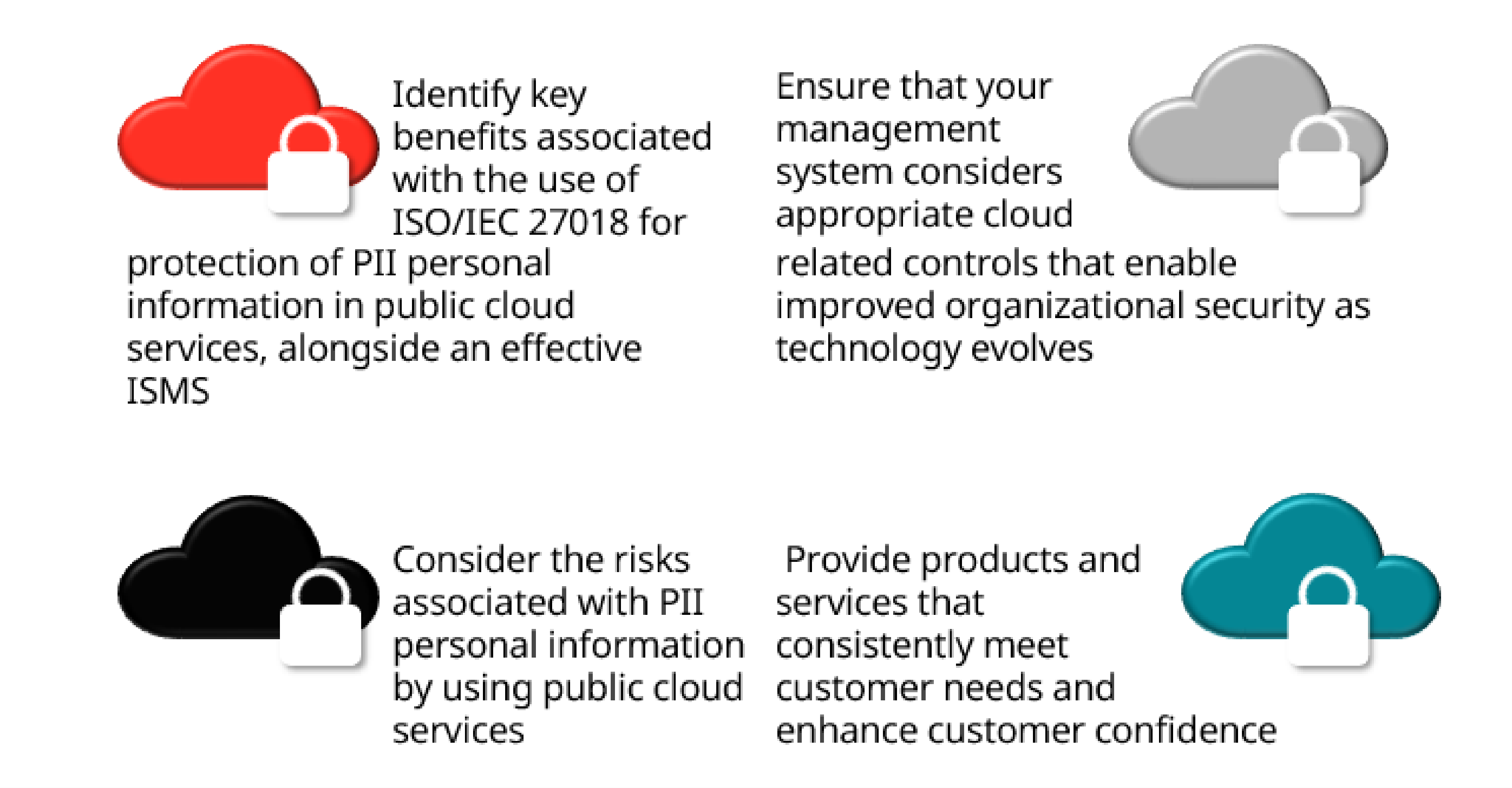
Identify key benefits associated with the use of ISO/IEC 27017 for cloud services, alongside an effective ISMS

Ensure that your management system considers appropriate cloud-related controls that enable improved organizational security as technology evolves

Consider the risks associated with using cloud services

Provide products and services that consistently meet customer needs and enhance customer confidence

Benefits to you ISO/IEC 27018

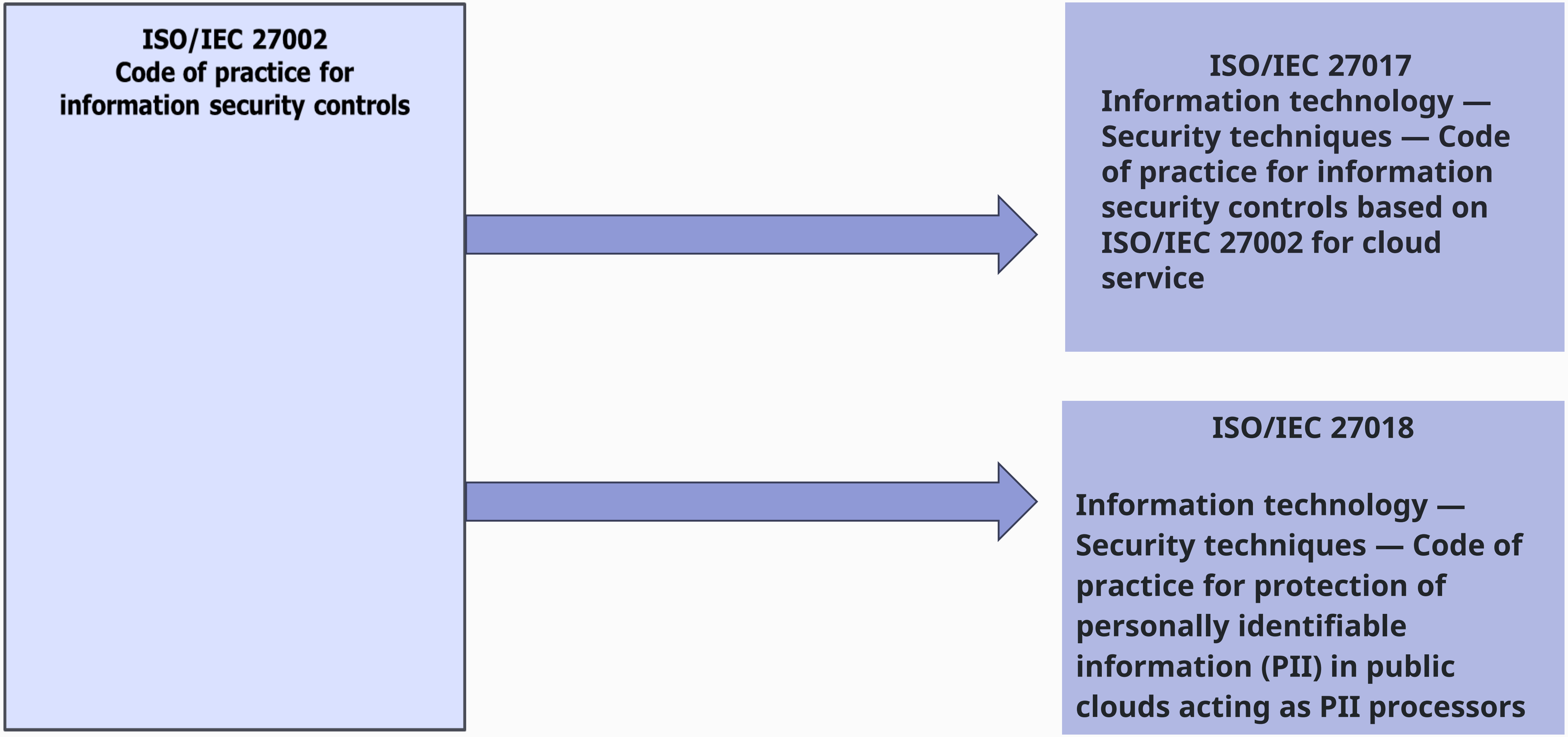


Identify key benefits associated with the use of ISO/IEC 27018 for protection of PII personal information in public cloud services, alongside an effective ISMS

Ensure that your management system considers appropriate cloud related controls that enable improved organizational security as technology evolves

Consider the risks associated with PII personal information by using public cloud services

Provide products and services that consistently meet customer needs and enhance customer confidence



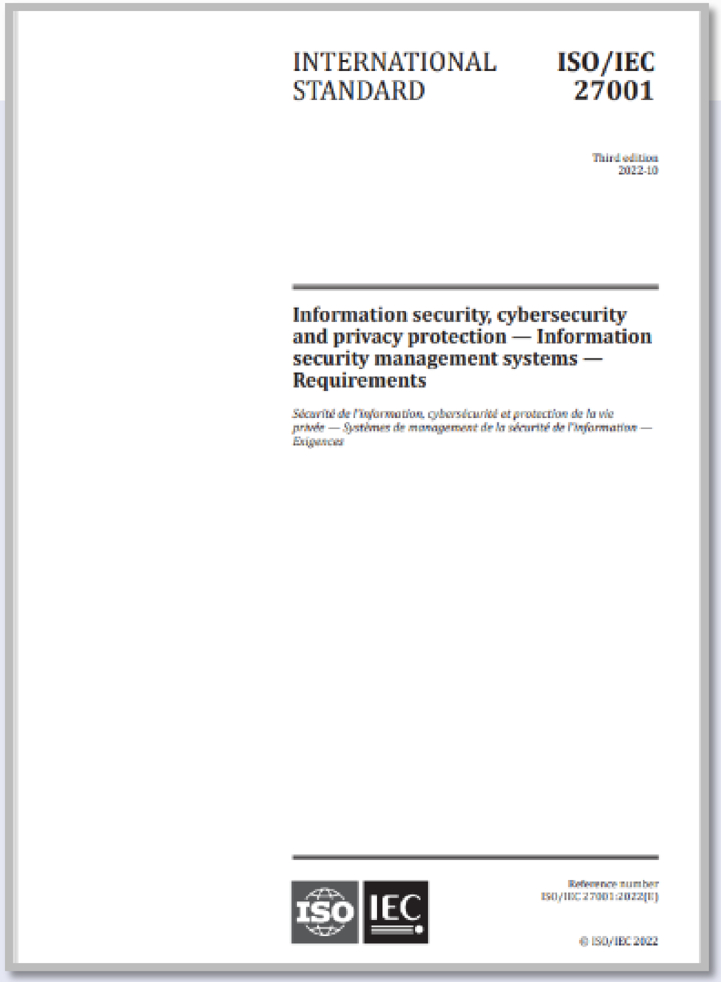
ISO/IEC 27002
Code of practice for information security controls

ISO/IEC 27017
Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud service

ISO/IEC 27018

Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

ISO/IEC 27001:2022 and ISO/IEC 27002:2022



INTERNATIONAL STANDARD

ISO/IEC 27001

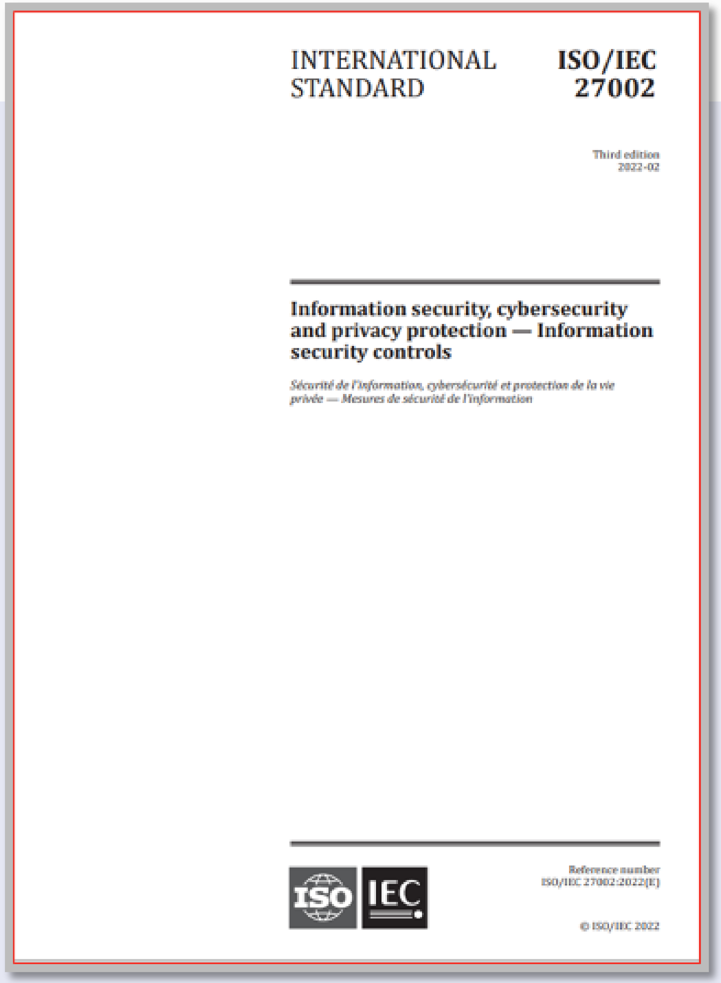
Third edition
2022-10

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



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

Structure of

ISO/IEC 27017:2015

ISO/IEC 27018:2019

Structure of ISO/IEC 27017:2015

Doesn’t repeat all ISO/IEC 27002 control objectives

Type 1

Separate for cloud service customer and provider

Two types of implementation guidance

Type 2

Guidance for both customer and provider

Extended control sets are in Annex A

Structure of ISO/IEC 27018:2019

Doesn’t repeat

all ISO/IEC 27002

control objectives

Guidance for provider

Extended control sets

are in Annex A

(from ISO/IEC 29110)

ISO/IEC 27017:2015

BS ISO/IEC 27017:2015

BSI Standards Publication

Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services

bsi.

...making excellence a habit™

ISO 27017 :2015 Requirement (5-18)

Clause	Main Control	Sub Control	Additional from ISO 27002:2013	Note
5	Information security policies			
5.1	The objective specified in clause 5.1 of ISO/IEC 27002 applies.	5.1.1 Policies for information security	Y	
		5.1.2 Review of the policies for information security	N	
6	Organization of information security			
6.1	Internal organization	6.1.1 Information security roles and responsibilities	Y	
		6.1.2 Segregation of duties	N	
		6.1.3 Contact with authorities	Y	
		6.1.4 Contact with special interest groups	N	
		6.1.5 Information security in project management	N	
6.2	Mobile devices and teleworking	6.2.1 Mobile device policy	N	
		6.2.2 Teleworking	N	
7	Human resource security			
7.1	Prior to employment	7.1.1 Screening	N	
		7.1.2 Terms and conditions of employment	N	
7.2	During employment	7.2.1 Management responsibilities	N	
		7.2.2 Information security awareness, education and training	Y	
		7.2.3 Disciplinary process	N	
7.3	Termination and change of employment	7.3.1 Termination or change of employment responsibilities	N	

ISO 27017 :2015 Requirement (5-18)

Clause	Main Control	Sub Control	Additional from ISO 27002:2013	Note
8	**Asset management**			
8.1	Responsibility for assets	8.1.1 Inventory of assets	Y	
		8.1.2 Ownership of assets	N	
		8.1.3 The acceptable use of assets	N	
		8.1.4 Return of assets	N	
8.2	Information classification	8.2.1 Classification of information	N	
		8.2.2 Labelling of information	Y	
		8.2.3 Handling of assets	N	
8.3	Media handling	8.3.1 Management of removable media	N	
		8.3.2 Disposal of media	N	
		8.3.3 Physical media transfer	N	

ISO 27017 :2015 Requirement (5-18)

Clause	Main Control	Sub Control	Additional from ISO 27002:2013	Note
9	Access control			
9.1	Business requirements of access control	9.1.1 Access control policy	N	
		9.1.2 Access to networks and network services	Y	
9.2	User access management	9.2.1 User registration and deregistration	Y	
		9.2.2 User access provisioning	Y	
		9.2.3 Management of privileged access rights	Y	
		9.2.4 Management of secret authentication information of users	Y	
		9.2.5 Review of user access rights	N	
		9.2.6 Removal or adjustment of access rights	N	
9.3	User responsibilities	9.3.1 Use of secret authentication information	N	
9.4	System and application access control	9.4.1 Information access restriction	Y	
		9.4.2 Secure log-on procedures	N	
		9.4.3 Password management system	N	
		9.4.4 Use of privileged utility programs	y	
		9.4.5 Access control to program source code	N	

ISO 27017 :2015 Requirement (5-18)

Clause	Main Control	Sub Control	Additional from ISO 27002:2013	Note
10	Cryptography			
10.1	Cryptographic controls	10.1.1 Policy on the use of cryptographic controls	Y	
		10.1.2 Key management	Y	
11	Physical and environmental security			
11.1	Secure areas	11.1.1 Physical security perimeter	N	
		11.1.2 Physical entry controls	N	
		11.1.3 Securing offices, rooms and facilities	N	
		11.1.4 Protecting against external and environmental threats	N	
		11.1.5 Working in secure areas	N	
		11.1.6 Delivery and loading areas	N	
11.2	Equipment	11.2.1 Equipment siting and protection	N	
		11.2.2 Supporting utilities	N	
		11.2.3 Cabling security	N	
		11.2.4 Equipment maintenance	N	
		11.2.5 Removal of assets	N	
		11.2.6 Security of equipment and assets off-premises	N	
		11.2.7 Secure disposal or reuse of equipment	Y	
		11.2.8 Unattended user equipment	N	
		11.2.9 Clear desk and clear screen policy	N	

ISO 27017 :2015 Requirement (5-18)

Clause	Main Control	Sub Control	Additional from ISO 27002:2013	Note
12	Operations security			
12.1	Operational procedures and responsibilities	12.1.1 Documented operating procedures	N	
		12.1.2 Change management	Y	
		12.1.3 Capacity management	Y	
		12.1.4 Separation of development, testing and operational environments	N	
12.2	Protection from malware	12.2.1 Controls against malware	N	
12.3	Backup	12.3.1 Information backup	Y	
12.4	Logging and monitoring	12.4.1 Event logging	Y	
		12.4.2 Protection of log information	N	
		12.4.3 Administrator and operator logs	Y	
		12.4.4 Clock synchronization	Y	
12.5	Control of operational software	12.5.1 Installation of software on operational systems	N	
12.6	Technical vulnerability management	12.6.1 Management of technical vulnerabilities	Y	
		12.6.2 Restrictions on software installation	N	
12.7	Information systems audit considerations	12.7.1 Information systems audit controls	N	

ISO 27017 :2015 Requirement (5-18)

Clause	Main Control	Sub Control	Additional from ISO 27002:2013	Note
13	Communications security			
13.1	Network security management	13.1.1 Network controls	N	
		13.1.2 Security of network services	N	
		13.1.3 Segregation in networks	Y	
13.2	Information transfer	13.2.1 Information transfer policies and procedures	N	
		13.2.2 Agreements on information transfer	N	
		13.2.3 Electronic messaging	N	
		13.2.4 Confidentiality or non-disclosure agreements	N	

ISO 27017 :2015 Requirement (5-18)

Clause	Main Control	Sub Control	Additional from ISO 27002:2013	Note
14	System acquisition, development and maintenance			
14.1	Security requirements of information systems	14.1.1 Information security requirements analysis and specification	Y	
		14.1.2 Securing applications services on public networks	N	
		14.1.3 Protecting application services transactions	N	
14.2	Security in development and support processes	14.2.1 Secure development policy	Y	
		14.2.2 System change control procedures	N	
		14.2.3 Technical review of applications after operating platform changes	N	
		14.2.4 Restrictions on changes to software packages	N	
		14.2.5 Secure system engineering principles	N	
		14.2.6 Secure development environment	N	
		14.2.7 Outsourced development	N	
		14.2.8 System security testing	N	
		14.2.9 System acceptance testing	N	
14.3	Test data	14.3.1 Protection of test data	N	

ISO 27017 :2015 Requirement (5-18)

Clause	Main Control	Sub Control	Additional from ISO 27002:2013	Note
15	Supplier relationships			
15.1	Information security in supplier relationships	15.1.1 Information security policy for supplier relationships	Y	
		15.1.2 Addressing security within supplier agreements	Y	
		15.1.3 Information and communication technology supply chain	Y	
15.2	Supplier service delivery management	15.2.1 Monitoring and review of supplier services	N	
		15.2.2 Managing changes to supplier services	N	
16	Information security incident management			
16.1	Management of information security incidents and improvements	16.1.1 Responsibilities and procedures	Y	
		16.1.2 Reporting information security events	Y	
		16.1.3 Reporting information security weaknesses	N	
		16.1.4 Assessment of and decision on information security events	N	
		16.1.5 Response to information security incidents	N	
		16.1.6 Learning from information security incidents	N	
		16.1.7 Collection of evidence	Y	

ISO 27017 :2015 Requirement (5-18)

Clause	Main Control	Sub Control	Additional from ISO 27002:2013	Note
17	Information security aspects of business continuity management			
17.1	Information security continuity	17.1.1 Planning information security continuity	N	
		17.1.2 Implementing information security continuity	N	
		17.1.3 Verify, review and evaluate information security continuity	N	
17.2	Redundancies	17.2.1 Availability of information processing facilities	N	
18	Compliance			
18.1	Compliance with legal and contractual requirements	18.1.1 Identification of applicable legislation and contractual requirements	Y	
		18.1.2 Intellectual property rights	Y	
		18.1.3 Protection of records	Y	
		18.1.4 Privacy and protection of personally identifiable information	N	
		18.1.5 Regulation of cryptographic controls	Y	
18.2	Information security reviews	18.2.1 Independent review of information security	Y	
		18.2.2 Compliance with security policies and standards	N	
		18.2.3 Technical compliance review	N	

ISO 27017 :2015 Requirement (5-18)

Clause	Main Control	Sub Control	Additional from ISO 27002:2013	Note
17	Information security aspects of business continuity management			
17.1	Information security continuity	17.1.1 Planning information security continuity	N	
		17.1.2 Implementing information security continuity	N	
		17.1.3 Verify, review and evaluate information security continuity	N	
17.2	Redundancies	17.2.1 Availability of information processing facilities	N	
18	Compliance			
18.1	Compliance with legal and contractual requirements	18.1.1 Identification of applicable legislation and contractual requirements	Y	
		18.1.2 Intellectual property rights	Y	
		18.1.3 Protection of records	Y	
		18.1.4 Privacy and protection of personally identifiable information	N	
		18.1.5 Regulation of cryptographic controls	Y	
18.2	Information security reviews	18.2.1 Independent review of information security	Y	
		18.2.2 Compliance with security policies and standards	N	
		18.2.3 Technical compliance review	N	

ISO 27017:2015 Requirement

Annex A Cloud service extended control set

CLD.6.3	Relationship between cloud service customer and cloud service provider	**Objective:** To clarify the relationship regarding shared roles and responsibilities between the cloud service customer and the cloud service provider for information security management
	CLD.6.3.1Shared roles and responsibilities within a cloud computing environment	**Control:** Responsibilities for shared information security roles in the use of the cloud service should be allocated to identified parties, documented, communicated and implemented by both the cloud service customer and the cloud service provider.

CLD.8.1	Responsibility for assets	The objective specified in clause 8.1 of ISO/IEC 27002 applies.
	CLD.8.1.5 Removal of cloud service customer assets	**Control:** Assets of the cloud service customer that are on the cloud service provider's premises should be removed, and returned if necessary, in a timely manner upon termination of the cloud service agreement.

ISO 27017:2015 Requirement

Annex A Cloud service extended control set

CLD.9.5	Access control of cloud service customer data in shared virtual environment	**Objective:** To mitigate information security risks when using the shared virtual environment of cloud computing.
	CLD.9.5.1 Segregation in virtual computing environments	**Control :** A cloud service customer's virtual environment running on a cloud service should be protected from other cloud service customers and unauthorized persons.
	CLD.9.5.2 Virtual machine hardening	**Control** Virtual machines in a cloud computing environment should be hardened to meet business needs.

CLD.12.1	Operational procedures and responsibilities	The objective specified in clause 12.1 of ISO/IEC 27002 applies.
	CLD.12.1.5 Administrator's operational security	**Control** Procedures for administrative operations of a cloud computing environment should be defined, documented and monitored.

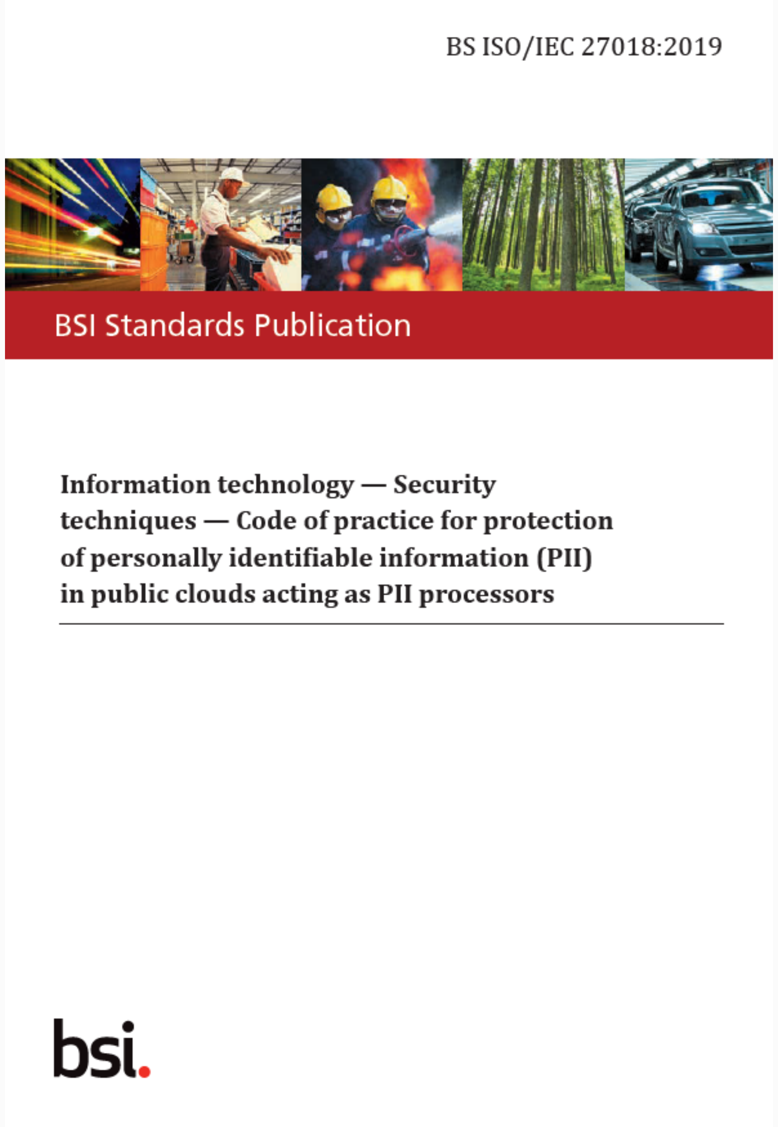
ISO 27017:2015 Requirement

Annex A Cloud service extended control set

CLD.12.4	Logging and monitoring	The objective specified in clause 12.4 of ISO/IEC 27002 applies.
	CLD.12.4.5 Monitoring of Cloud Services	**Control** The cloud service customer should have the capability to monitor specified aspects of the operation of the cloud services that the cloud service customer uses.

CLD.13.1	Network security management	The objective specified in clause 13.1 of ISO/IEC 27002 applies.
	CLD.13.1.4 Alignment of security management for virtual and physical networks	**Control** Upon configuration of virtual networks, consistency of configurations between virtual and physical networks should be verified based on the cloud service provider's network security policy.

ISO/IEC 27018:2019

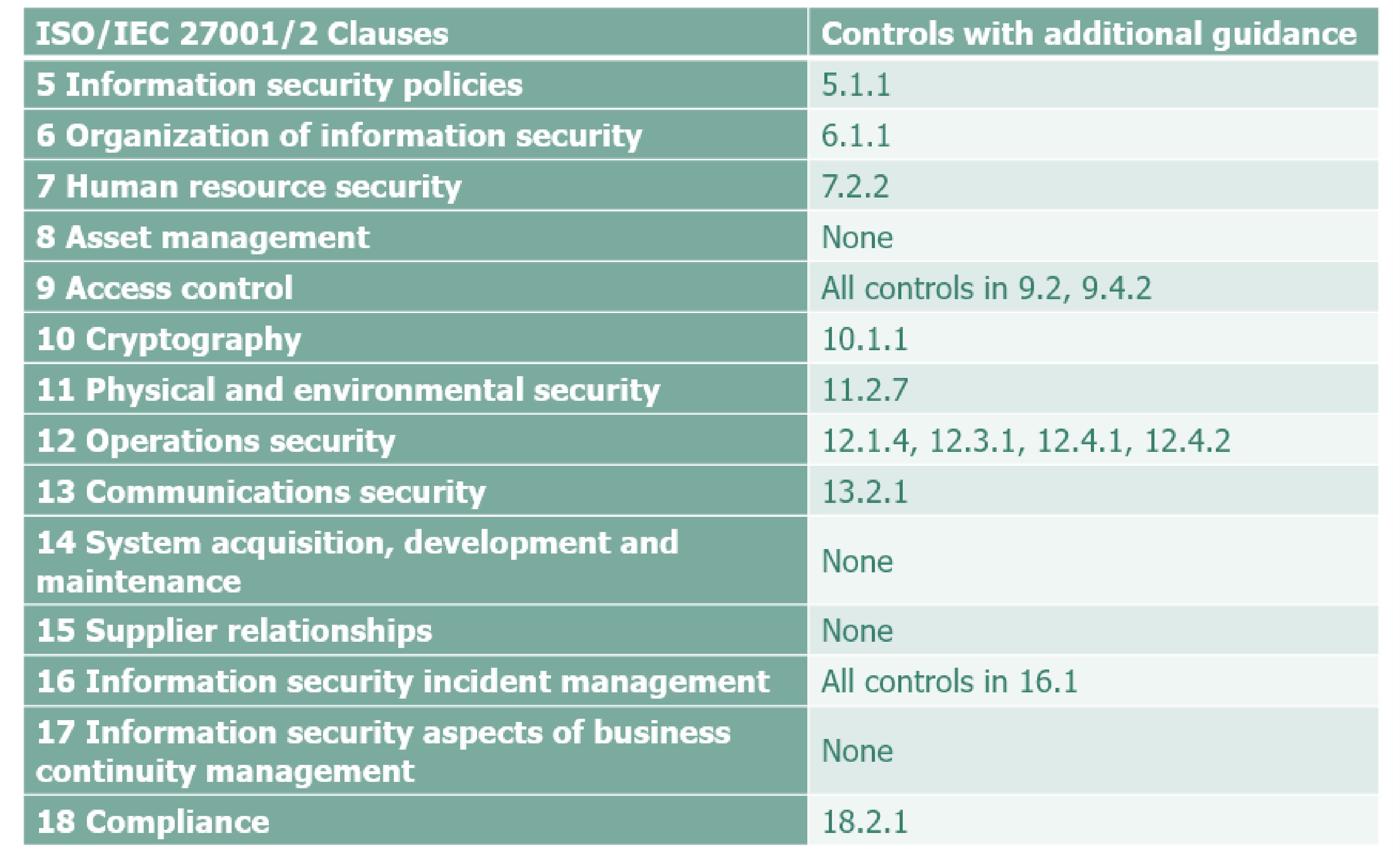


BS ISO/IEC 27018:2019

BSI Standards Publication

Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

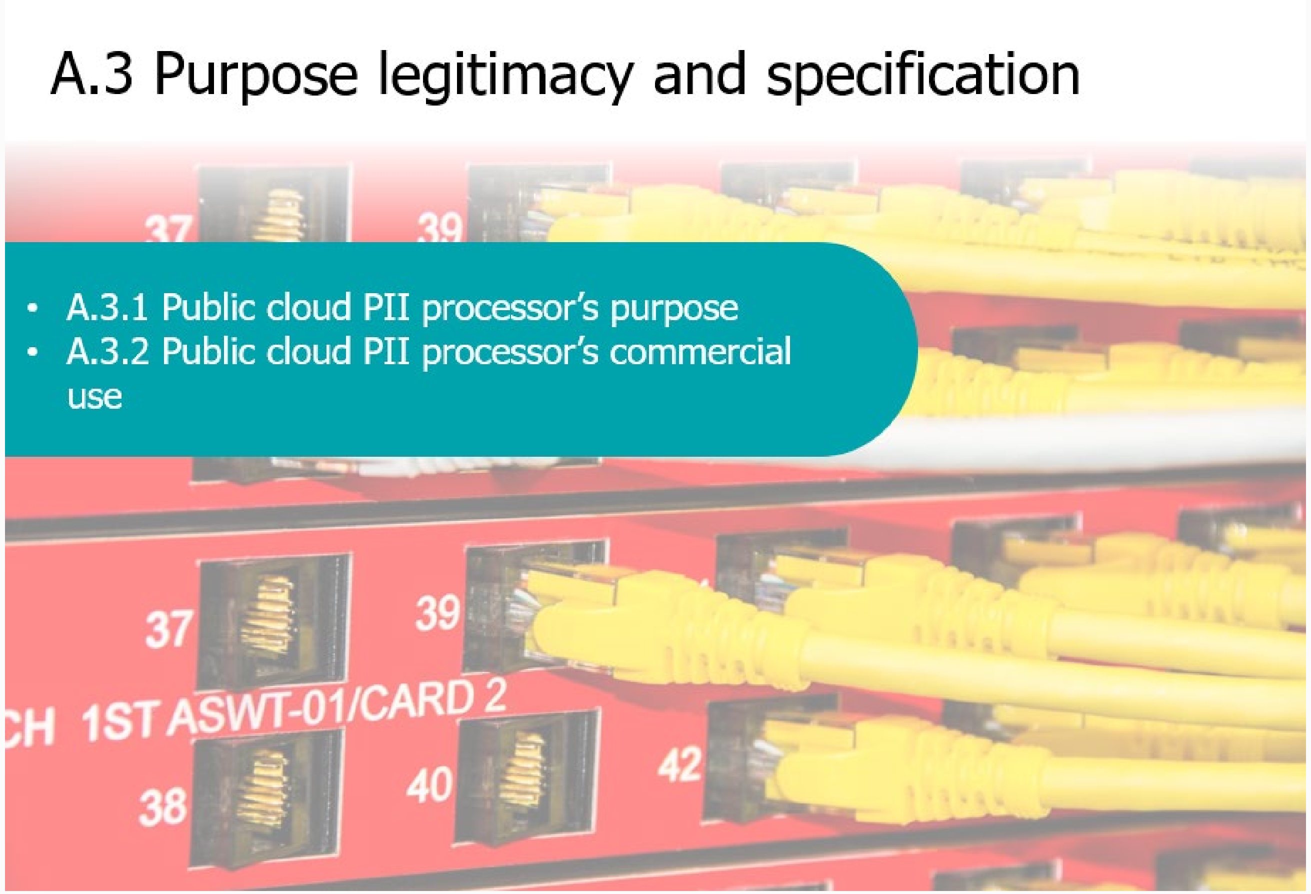
ISO 27018:2019 Requirement (5-18)



ISO/IEC 27001/2 Clauses	Controls with additional guidance
5 Information security policies	5.1.1
6 Organization of information security	6.1.1
7 Human resource security	7.2.2
8 Asset management	None
9 Access control	All controls in 9.2, 9.4.2
10 Cryptography	10.1.1
11 Physical and environmental security	11.2.7
12 Operations security	12.1.4, 12.3.1, 12.4.1, 12.4.2
13 Communications security	13.2.1
14 System acquisition, development and maintenance	None
15 Supplier relationships	None
16 Information security incident management	All controls in 16.1
17 Information security aspects of business continuity management	None
18 Compliance	18.2.1

ISO 27018:2019 Requirement

Annex A: Public cloud PII processor extended control set for PII protection (ISO/IEC 29100)



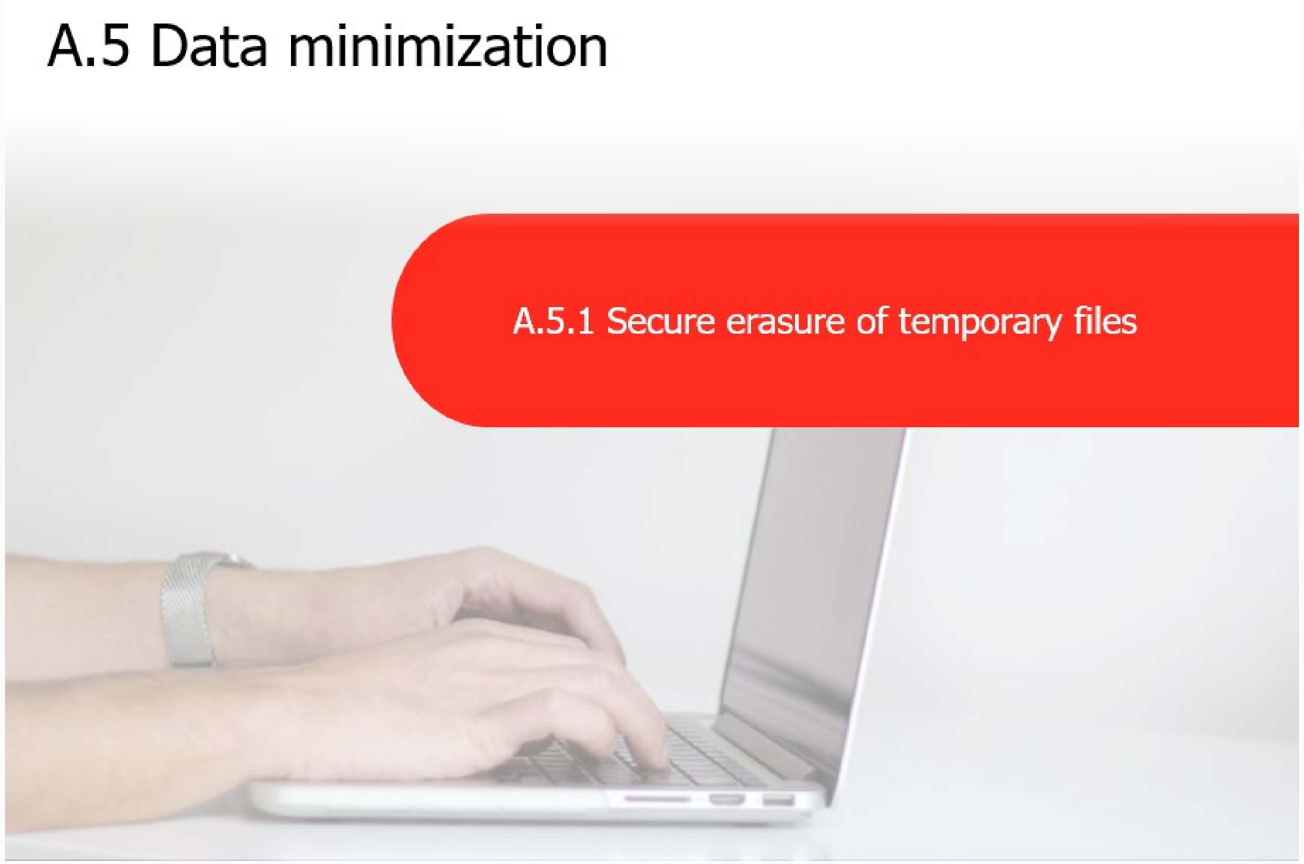
A.3 Purpose legitimacy and specification

- A.3.1 Public cloud PII processor's purpose
- A.3.2 Public cloud PII processor's commercial use

37
39
37
39
CH 1ST ASWT-01/CARD 2
38
40
42

ISO 27018:2019 Requirement

Annex A: Public cloud PII processor extended control set for PII protection (ISO/IEC 29100)

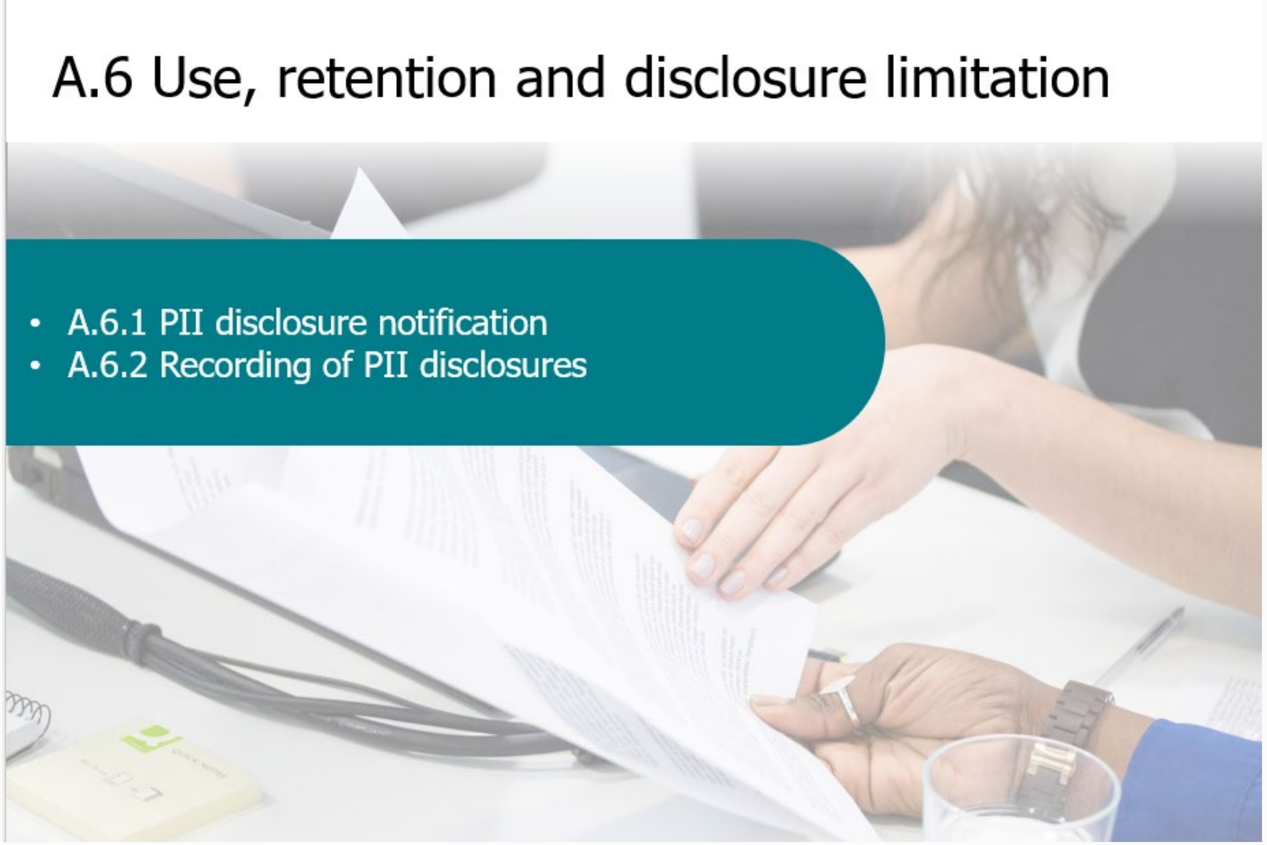


A.5 Data minimization

A.5.1 Secure erasure of temporary files

ISO 27018:2019 Requirement

Annex A: Public cloud PII processor extended control set for PII protection (ISO/IEC 29100)

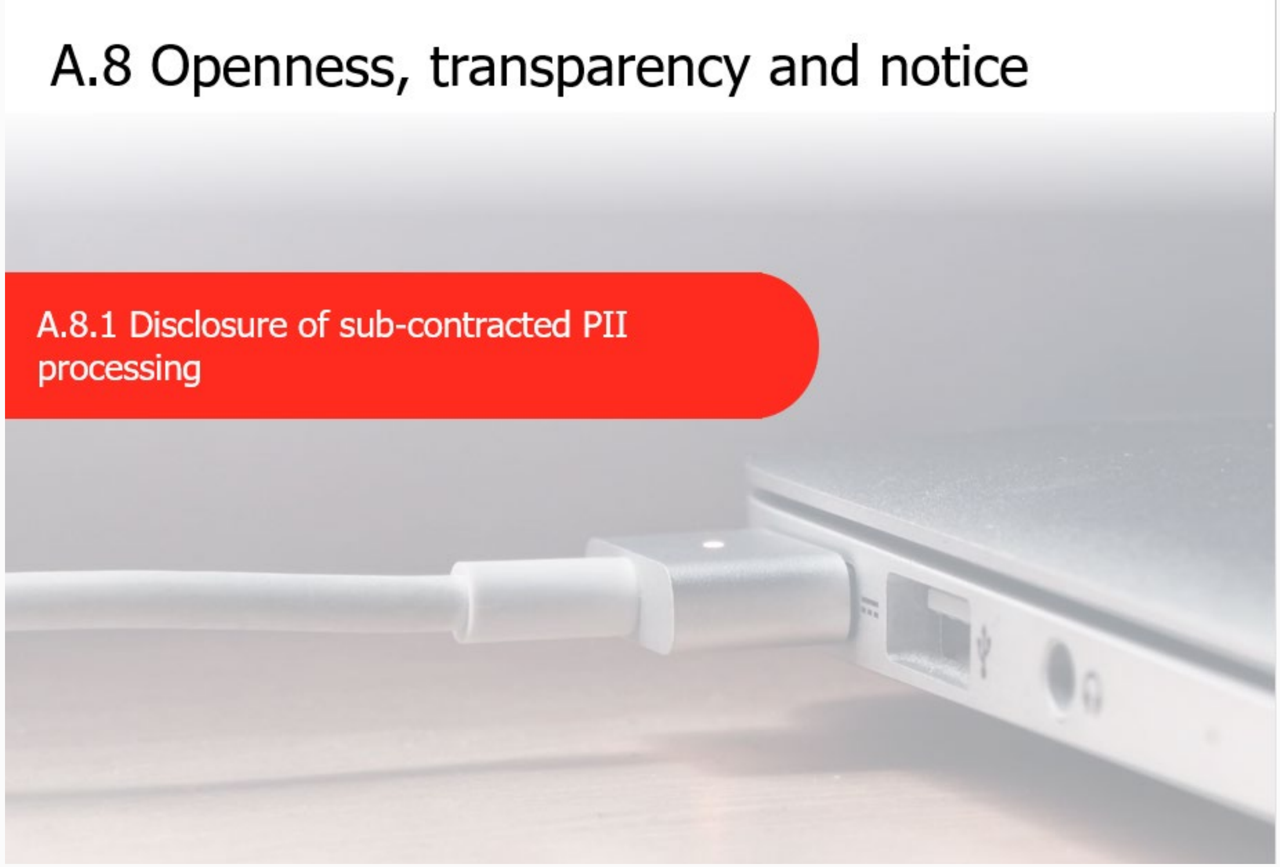


A.6 Use, retention and disclosure limitation

- A.6.1 PII disclosure notification
- A.6.2 Recording of PII disclosures

ISO 27018:2019 Requirement

Annex A: Public cloud PII processor extended control set for PII protection (ISO/IEC 29100)

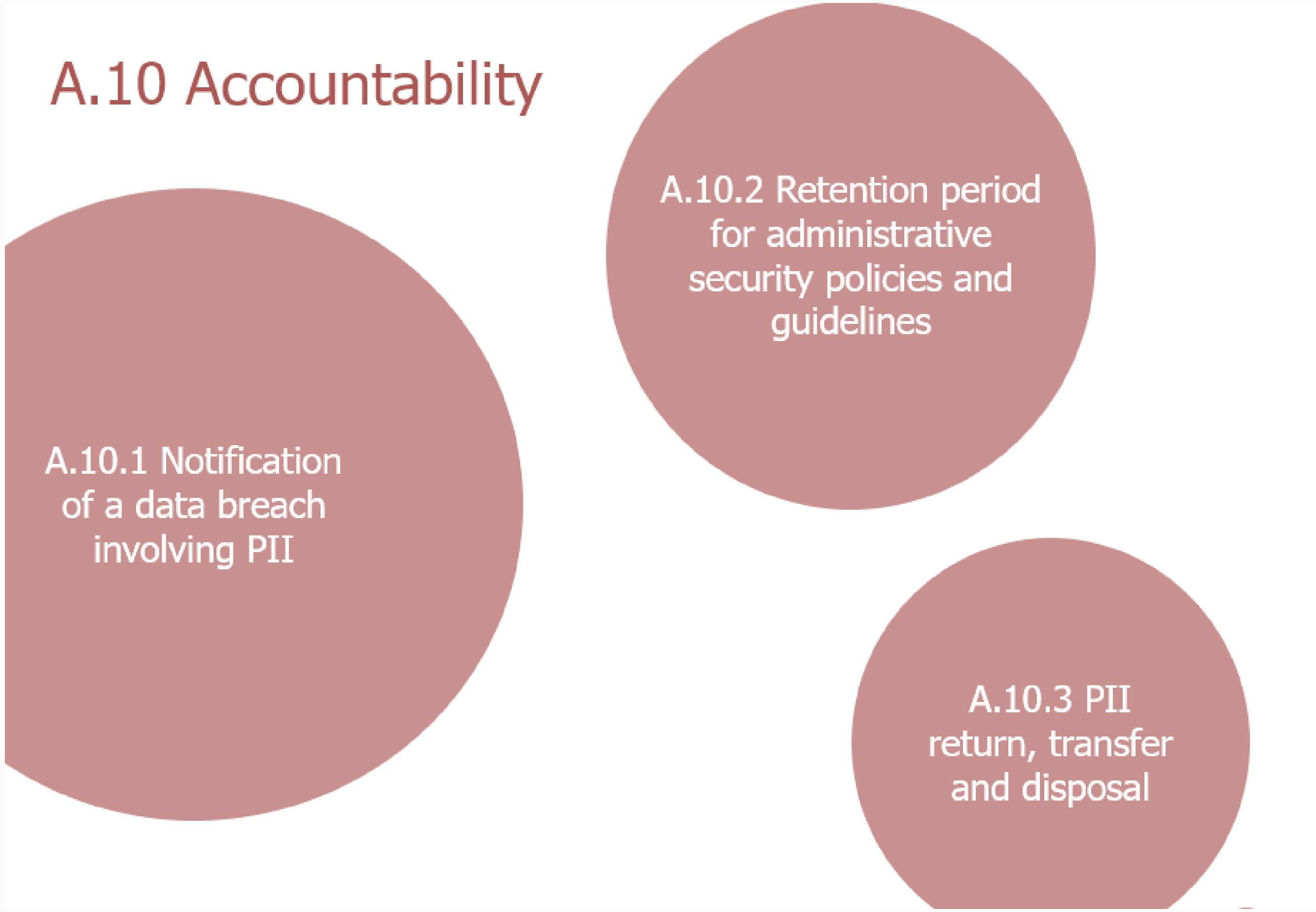


A.8 Openness, transparency and notice

A.8.1 Disclosure of sub-contracted PII processing

ISO 27018:2019 Requirement

Annex A: Public cloud PII processor extended control set for PII protection (ISO/IEC 29100)



A.10 Accountability

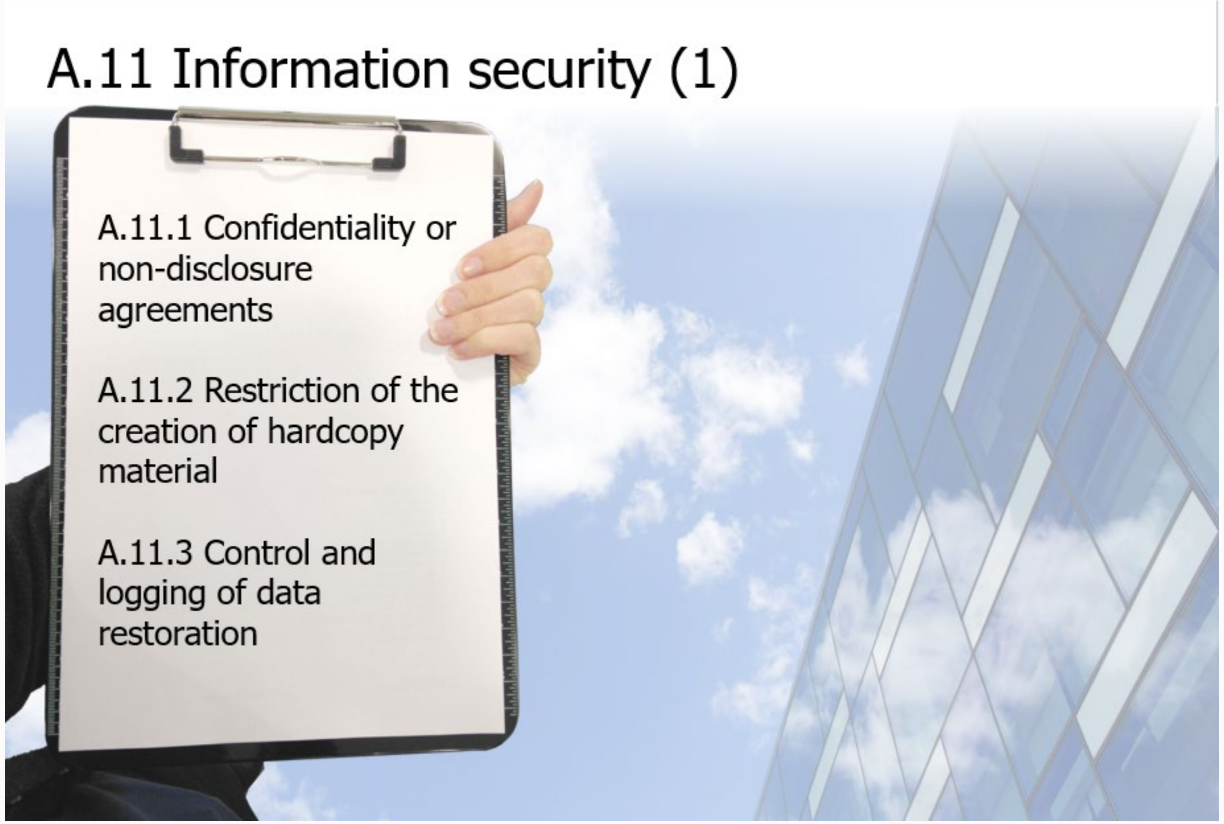
A.10.1 Notification of a data breach involving PII

A.10.2 Retention period for administrative security policies and guidelines

A.10.3 PII return, transfer and disposal

ISO 27018:2019 Requirement

Annex A: Public cloud PII processor extended control set for PII protection (ISO/IEC 29100)



A.11 Information security (1)

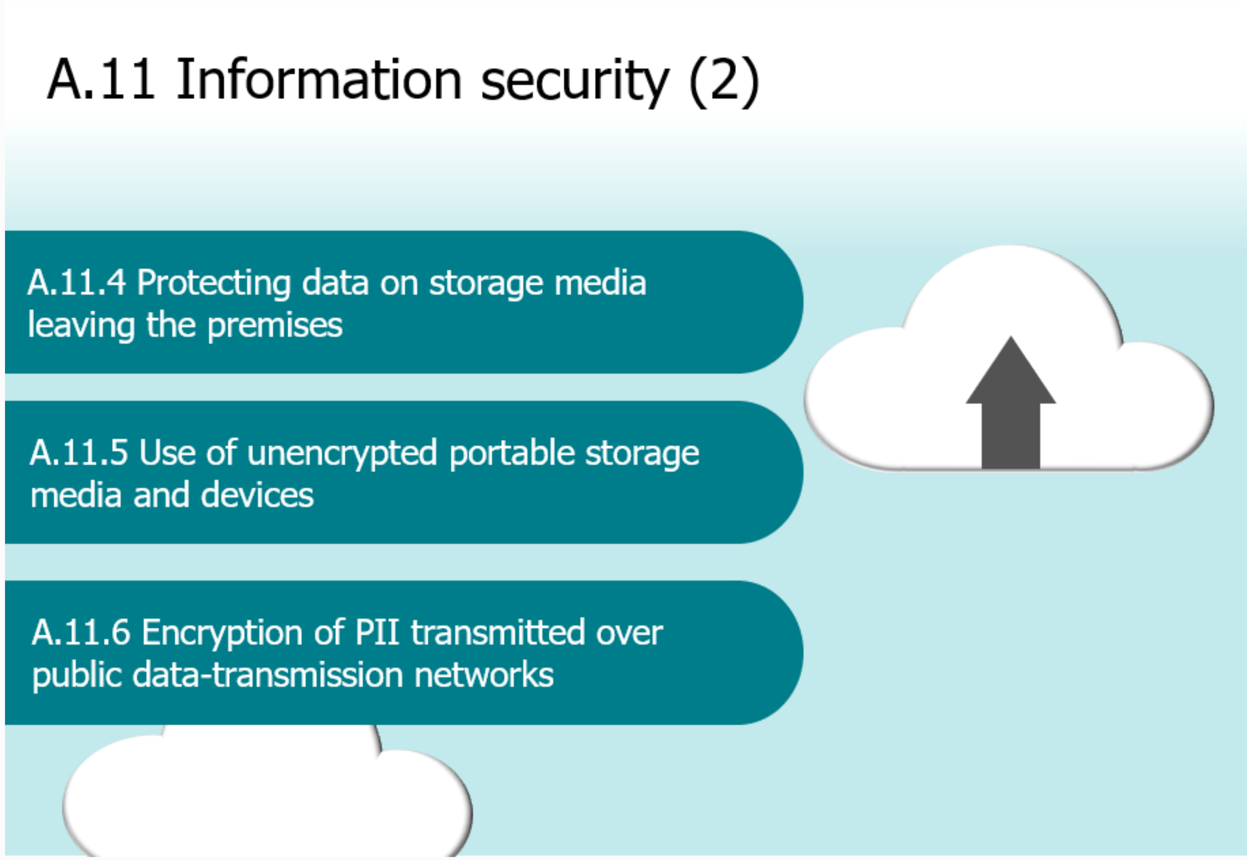
A.11.1 Confidentiality or non-disclosure agreements

A.11.2 Restriction of the creation of hardcopy material

A.11.3 Control and logging of data restoration

ISO 27018:2019 Requirement

Annex A: Public cloud PII processor extended control set for PII protection (ISO/IEC 29100)



A.11 Information security (2)

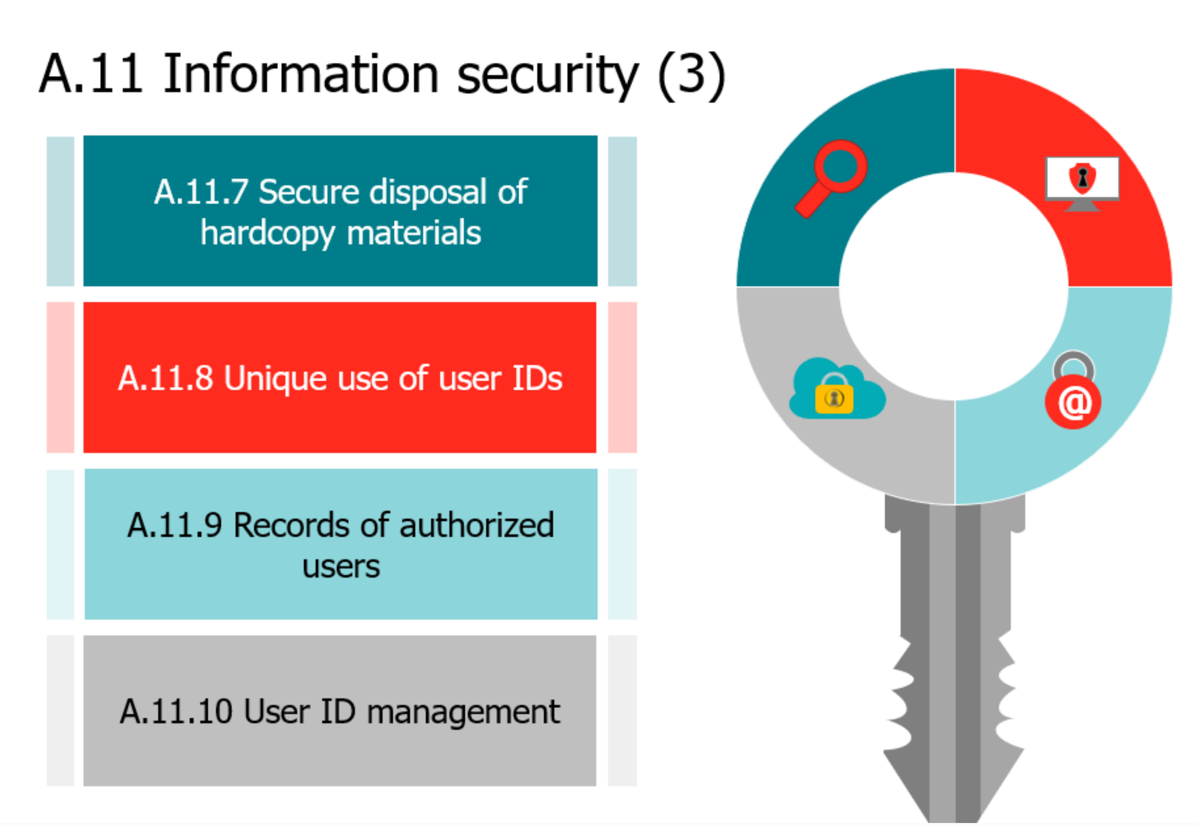
A.11.4 Protecting data on storage media leaving the premises

A.11.5 Use of unencrypted portable storage media and devices

A.11.6 Encryption of PII transmitted over public data-transmission networks

ISO 27018:2019 Requirement

Annex A: Public cloud PII processor extended control set for PII protection (ISO/IEC 29100)

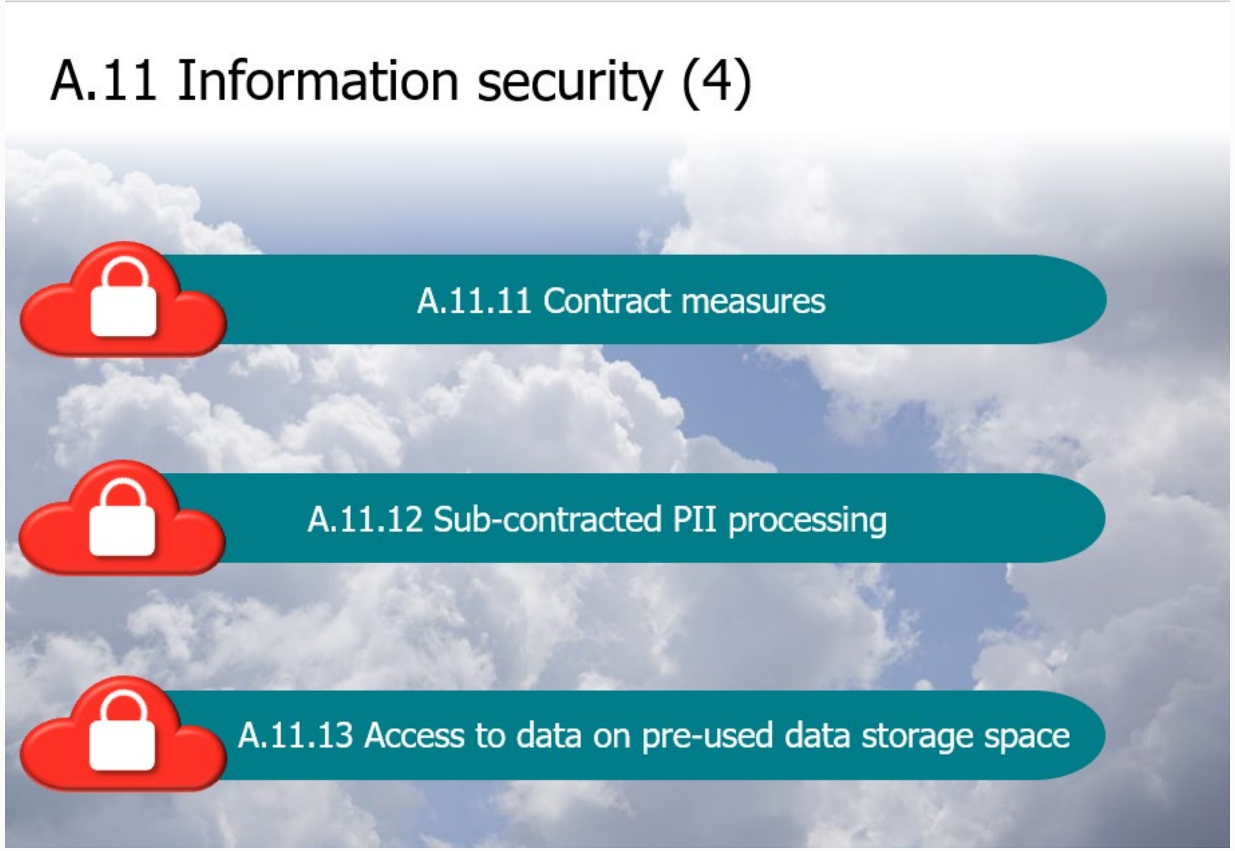


A.11 Information security (3)

- A.11.7 Secure disposal of hardcopy materials
- A.11.8 Unique use of user IDs
- A.11.9 Records of authorized users
- A.11.10 User ID management

ISO 27018:2019 Requirement

Annex A: Public cloud PII processor extended control set for PII protection (ISO/IEC 29100)

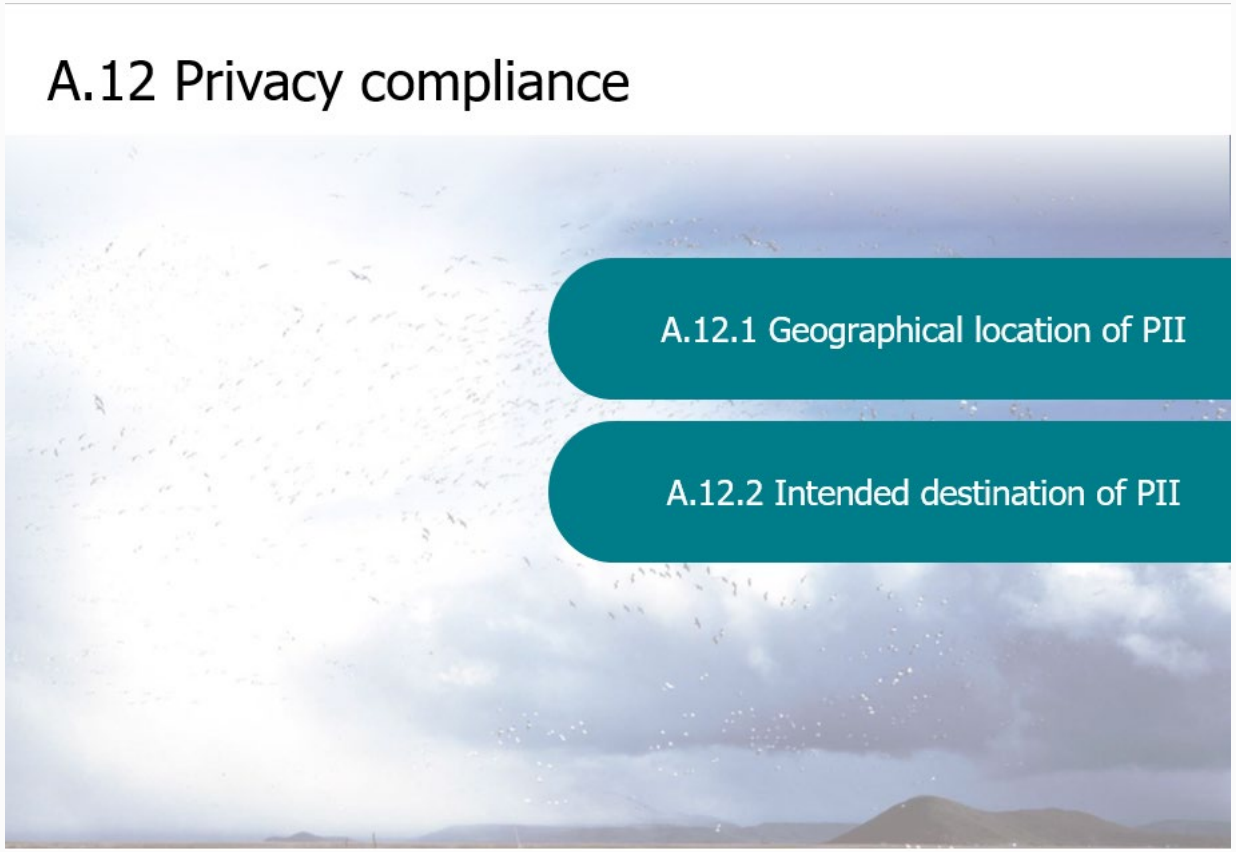


A.11 Information security (4)

- A.11.11 Contract measures
- A.11.12 Sub-contracted PII processing
- A.11.13 Access to data on pre-used data storage space

ISO 27018:2019 Requirement

Annex A: Public cloud PII processor extended control set for PII protection (ISO/IEC 29100)



A.12 Privacy compliance

- A.12.1 Geographical location of PII
- A.12.2 Intended destination of PII

ISO 27018:2019 Requirement

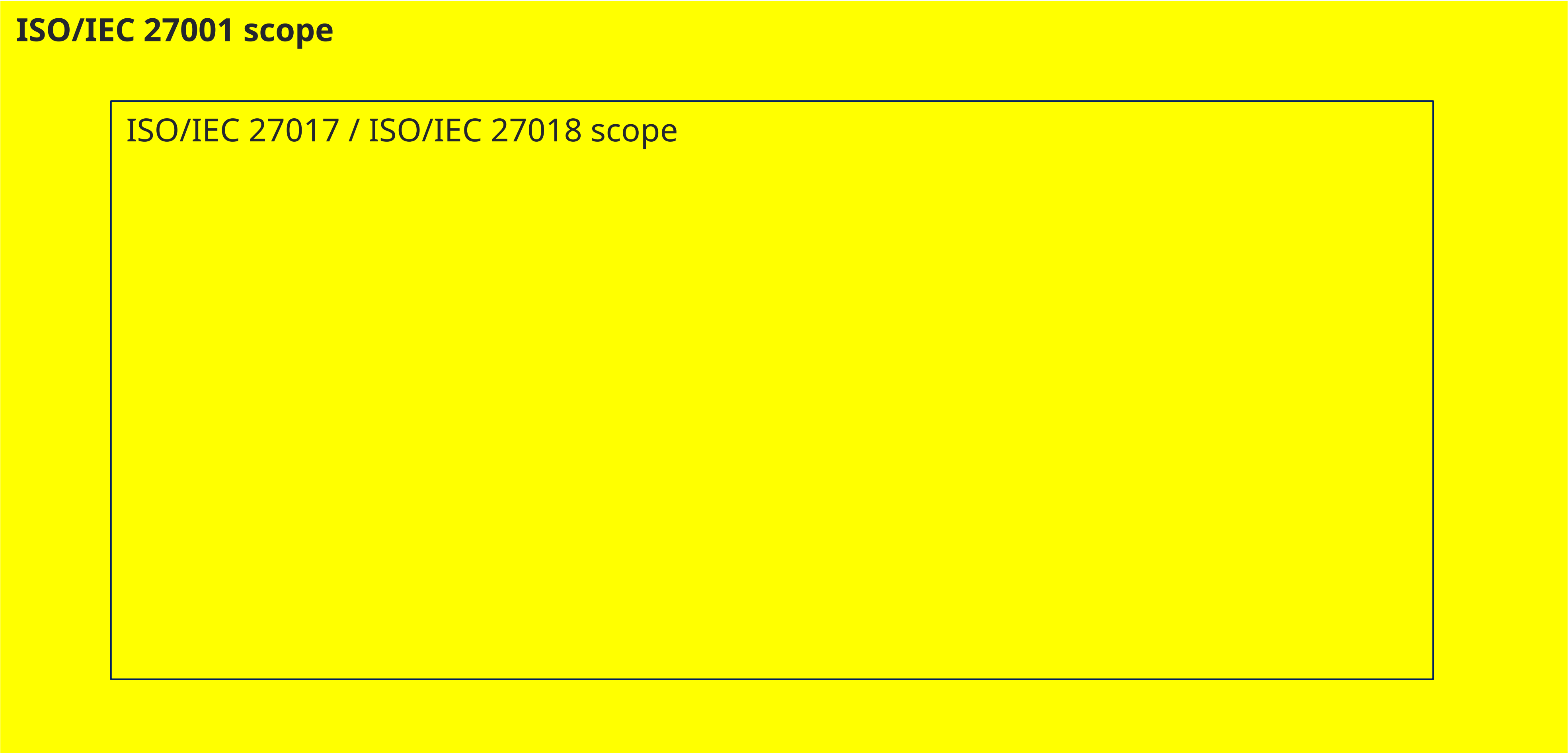
Annex A: Public cloud PII processor extended control set for PII protection
 (ISO/IEC 29100)

ISO 27018:2019 Requirement

Annex A: Public cloud PII processor extended control set for PII protection
 (ISO/IEC 29100)

การขอการรับรอง

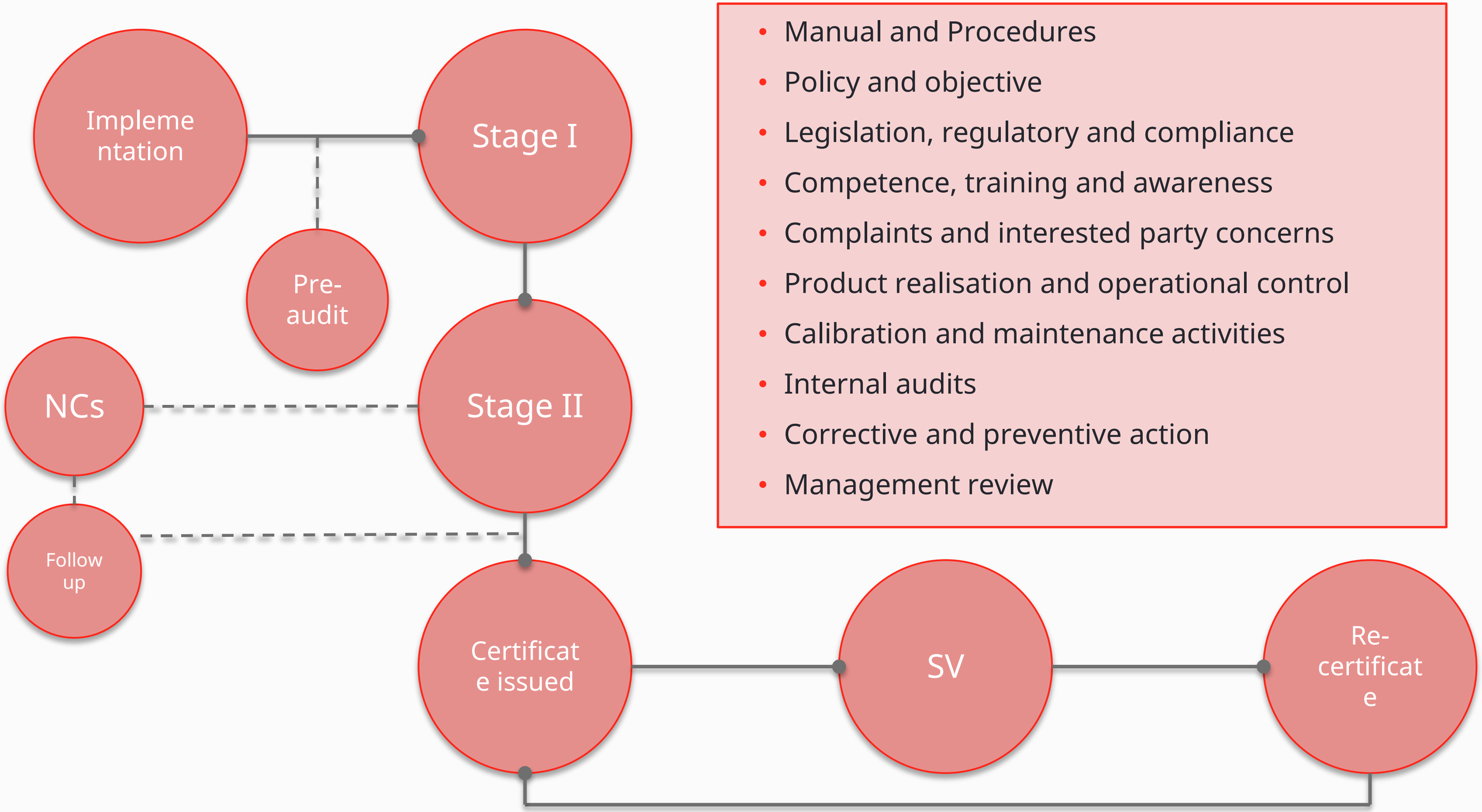
Certification Process



ISO/IEC 27001 scope

ISO/IEC 27017 / ISO/IEC 27018 scope

Certification Process



- Manual and Procedures
- Policy and objective
- Legislation, regulatory and compliance
- Competence, training and awareness
- Complaints and interested party concerns
- Product realisation and operational control
- Calibration and maintenance activities
- Internal audits
- Corrective and preventive action
- Management review

" Q&A

ทบทวนและถามคำถาม

สแกน QR code เป็นเพื่อนกับเราใน Line official ของ BSI

เพื่อไม่ให้พลาดข่าวสารข้อมูลที่เป็นประโยชน์ในสายอาชีพของท่าน

- Free webinars
- Tool และบทความดีๆ

bsi