WEBINAR: INTRODUCTION TO ISO 27017 & ISO 27018

Tim Pinnell

21/07/2021

OUR PURPOSE

IS TO HELP CUSTOMERS DELIVER PRODUCTS THE WORLD CAN

TRUST

NQA is a **world leading certification body** with global operations.

NQA specialises in certification in **high technology** and engineering sectors.

BOSTON
LONDON
BANGALORE
SHANGHAI

AMERICA'S NO.1

Certification body in **Aerospace** sector

TOP 3 IN THE UK

ISO 9001, ISO 14001, ISO 45001, ISO 27001

CHINA'S NO.1

Certification body in **Automotive** sector

GLOBAL NO.1

Certification body in **telecommunications** and **Automotive** sector

GLOBAL NO.3

Certification body in **Aerospace** sector

UK'S NO.2

Certification body in **Aerospace** sector

nqa.

nqa.

NEVER STOP IMPROVING

CERTIFICATION AND TRAINING SERVICES

We specialise in management systems certification for:

QUALITY

AEROSPACE (QUALITY)

AUTOMOTIVE (QUALITY)

ENVIRONMENT

ENERGY

HEALTH AND SAFETY

INFORMATION RESILIENCE

FOOD SAFETY

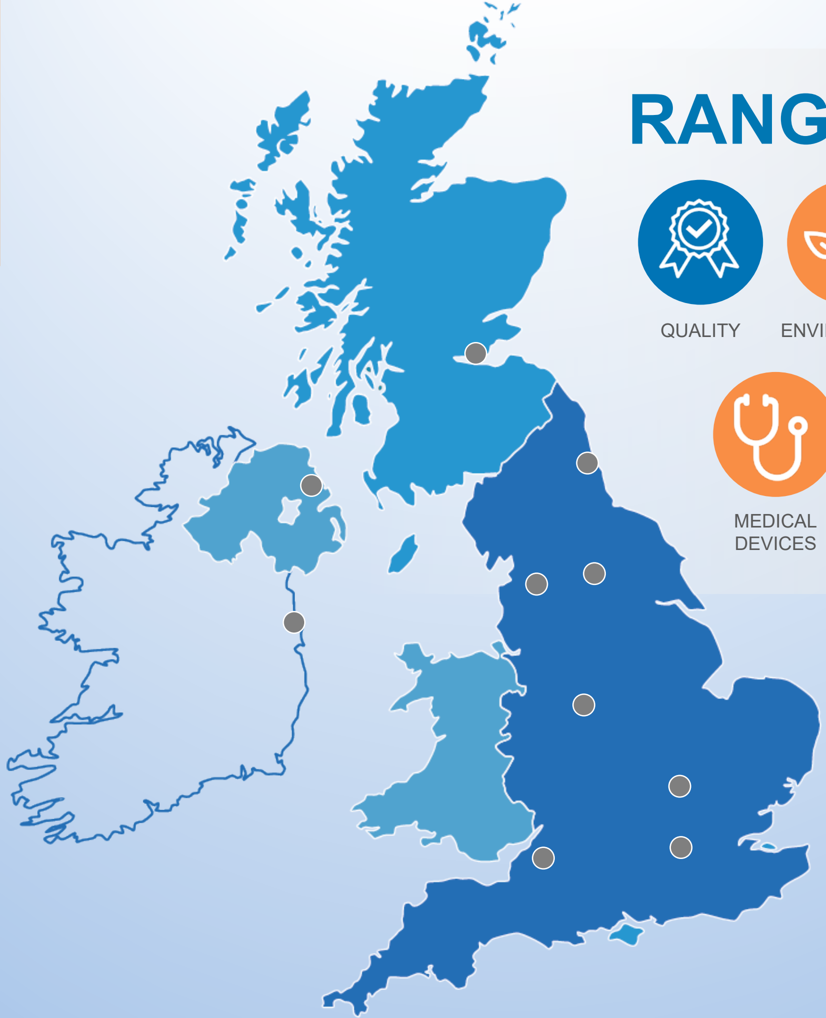
RISK MANAGEMENT

MEDICAL DEVICES

NATIONWIDE TRAINING SERVICES

ACCREDITED COURSES

- Virtual Learning
- e-Learning / Live Webinars
- In-house Training
- Public Training Nationwide Locations



RANGE OF COURSES

- QUALITY
- ENVIRONMENT
- ENERGY
- HEALTH AND SAFETY
- INFORMATION SECURITY
- MEDICAL DEVICES
- BUSINESS CONTINUITY
- AEROSPACE
- INTEGRATED MANAGEMENT

- **e-Learning** Introduction
- **1 day** Introduction Courses
- **2 day** Implementation Courses
- **2 day** Internal Auditor – NQA or IRCA
- **5 day** Lead Auditor – NQA or IRCA
- **Advanced** Training

CQI | IRCA
APPROVED TRAINING PARTNER

nqa.

NEVER STOP IMPROVING

KEY INFO

- 30 minute webinar
- Questions in the chat box
- Q&A at the end
- Recording of webinar circulated shortly

YOUR PRESENTER

Tim Pinnell

BSc, MSc, PCIP, CIPP/E,
CISMP, Information Security

NQA Information Security Assurance Manager

Tim has worked in telecommunications cyber and information security for over twenty years. From the early World Wide Web days to today's globally connected information services, Tim brings a wealth of experience in security, compliance and governance. Throughout his career he has played a leading role in adopting, consulting and implementing information security compliance standards, including ISO 27001, PCIDSS and Cyber Essentials, helping organizations understand the risks facing their businesses and the controls needed to mitigate them.

> “The rigour of a certified management system has sped up the process and ensured that we have been able to deliver what our clients need: an uninterrupted service.”
>
> **E.L.F.S.**

AGENDA FOR WEBINAR

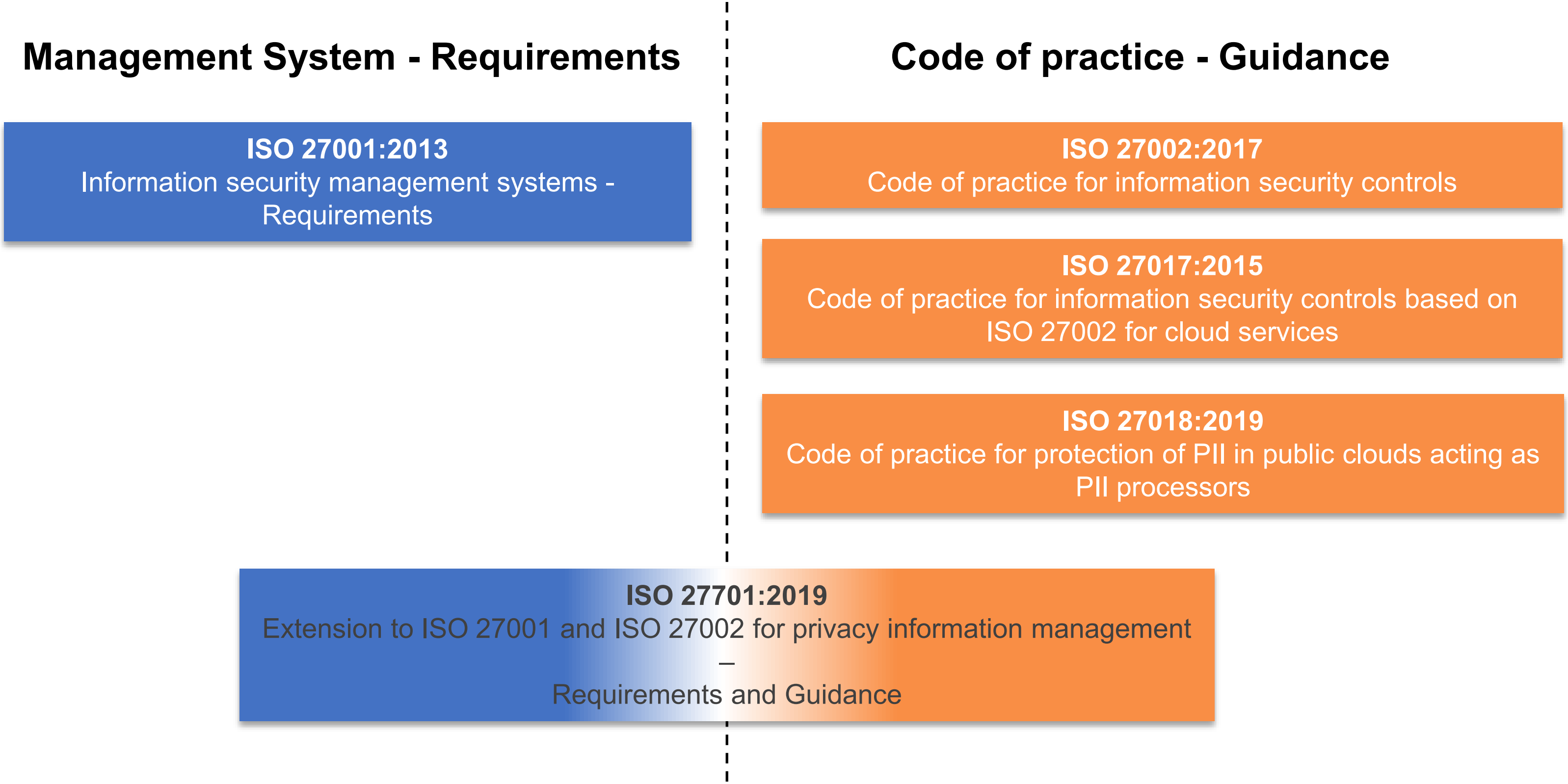
- Extensions to ISO 27002
- ISO 27017 overview
- ISO 27018 overview
- The relationship between ISO 27018 and ISO 27701
- Q&A

nqa.

NEVER STOP IMPROVING

EXTENSIONS TO ISO 27002

REQUIREMENTS VS. GUIDANCE



Management System - Requirements

ISO 27001:2013
Information security management systems - Requirements

Code of practice - Guidance

ISO 27002:2017
Code of practice for information security controls

ISO 27017:2015
Code of practice for information security controls based on ISO 27002 for cloud services

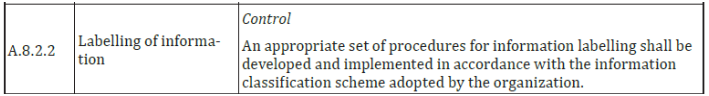
ISO 27018:2019
Code of practice for protection of PII in public clouds acting as PII processors

ISO 27701:2019
Extension to ISO 27001 and ISO 27002 for privacy information management
–
Requirements and Guidance

REQUIREMENTS VS. GUIDANCE

Management System - Requirements

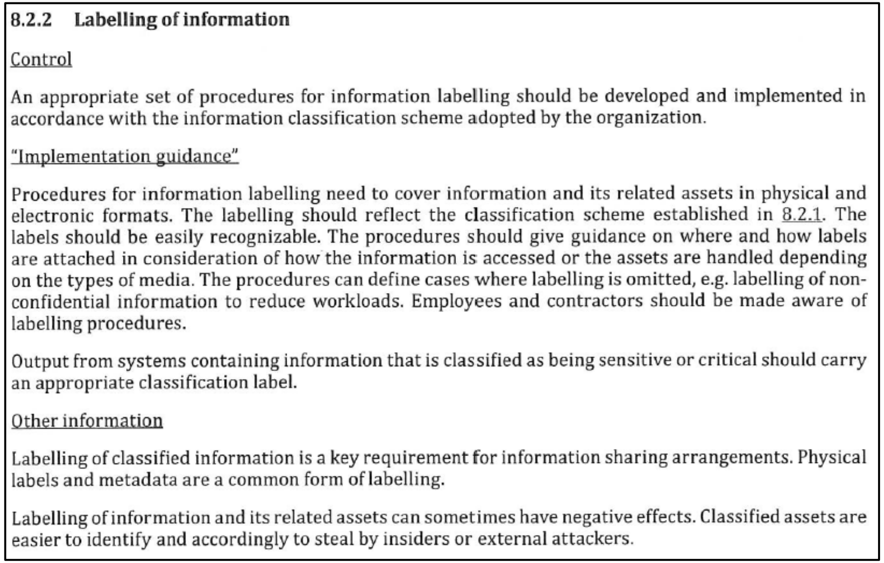
ISO 27001:2013
Information security management systems - Requirements



A.8.2.2	Labelling of information	*Control* An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization.

Code of practice - Guidance

ISO 27002:2017
Code of practice for information security controls



8.2.2 Labelling of information

Control

An appropriate set of procedures for information labelling should be developed and implemented in accordance with the information classification scheme adopted by the organization.

"Implementation guidance"

Procedures for information labelling need to cover information and its related assets in physical and electronic formats. The labelling should reflect the classification scheme established in 8.2.1. The labels should be easily recognizable. The procedures should give guidance on where and how labels are attached in consideration of how the information is accessed or the assets are handled depending on the types of media. The procedures can define cases where labelling is omitted, e.g. labelling of non-confidential information to reduce workloads. Employees and contractors should be made aware of labelling procedures.

Output from systems containing information that is classified as being sensitive or critical should carry an appropriate classification label.

Other information

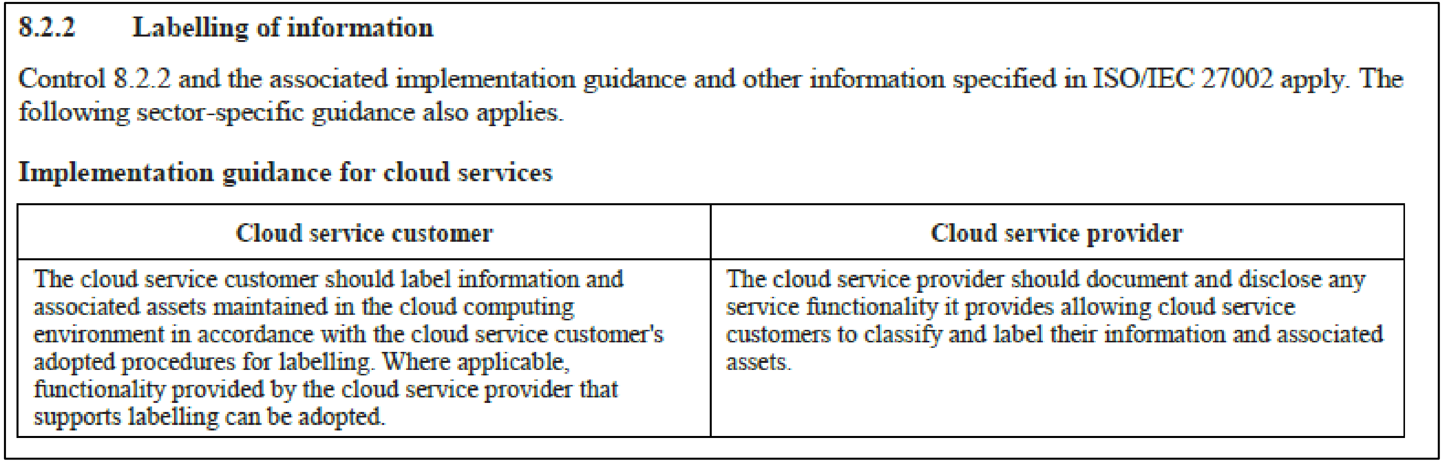
Labelling of classified information is a key requirement for information sharing arrangements. Physical labels and metadata are a common form of labelling.

Labelling of information and its related assets can sometimes have negative effects. Classified assets are easier to identify and accordingly to steal by insiders or external attackers.

REQUIREMENTS VS. GUIDANCE

ISO 27017:2015

Code of practice for information security controls based on ISO 27002 for cloud services



8.2.2 Labelling of information

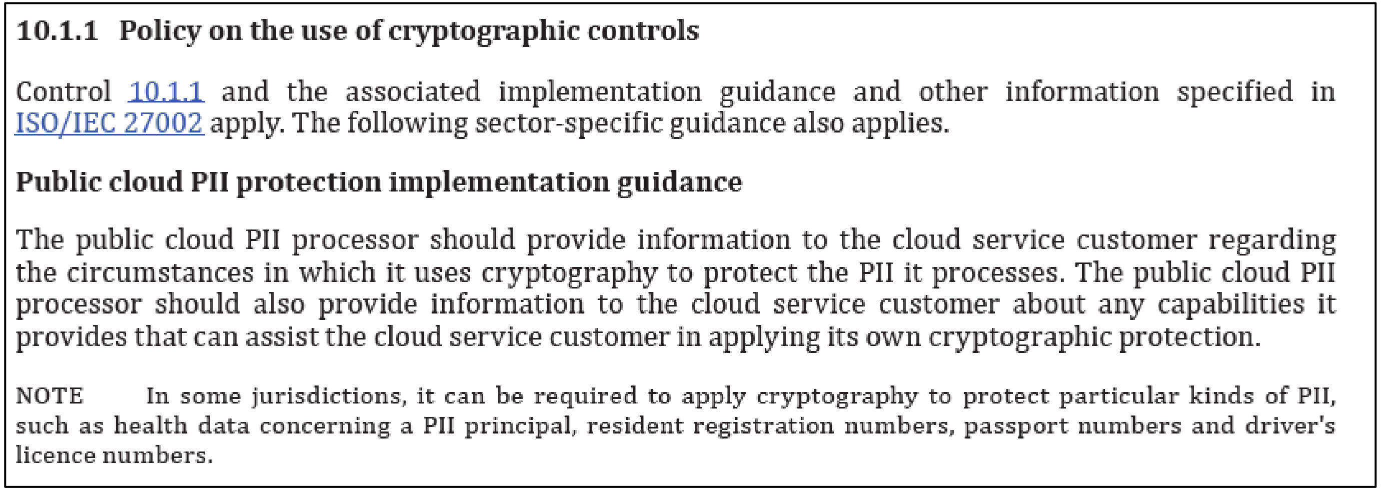
Control 8.2.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Implementation guidance for cloud services

Cloud service customer	Cloud service provider
The cloud service customer should label information and associated assets maintained in the cloud computing environment in accordance with the cloud service customer's adopted procedures for labelling. Where applicable, functionality provided by the cloud service provider that supports labelling can be adopted.	The cloud service provider should document and disclose any service functionality it provides allowing cloud service customers to classify and label their information and associated assets.

REQUIREMENTS VS. GUIDANCE

ISO 27018:2019
Code of practice for protection of PII in public clouds acting as PII processors



10.1.1 Policy on the use of cryptographic controls

Control 10.1.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

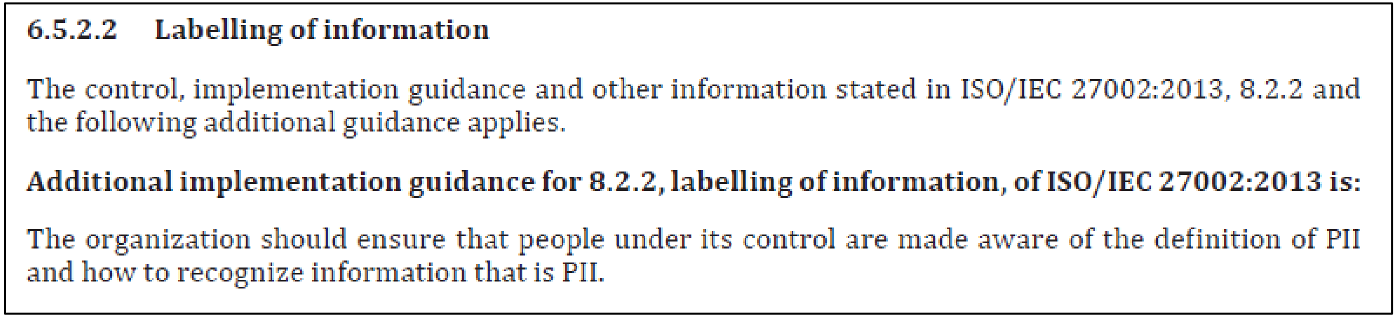
Public cloud PII protection implementation guidance

The public cloud PII processor should provide information to the cloud service customer regarding the circumstances in which it uses cryptography to protect the PII it processes. The public cloud PII processor should also provide information to the cloud service customer about any capabilities it provides that can assist the cloud service customer in applying its own cryptographic protection.

NOTE In some jurisdictions, it can be required to apply cryptography to protect particular kinds of PII, such as health data concerning a PII principal, resident registration numbers, passport numbers and driver's licence numbers.

REQUIREMENTS VS. GUIDANCE

ISO 27701:2019
Extension to ISO 27001 and ISO 27002 for privacy information management –
Requirements and Guidance



6.5.2.2 Labelling of information

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 8.2.2 and the following additional guidance applies.

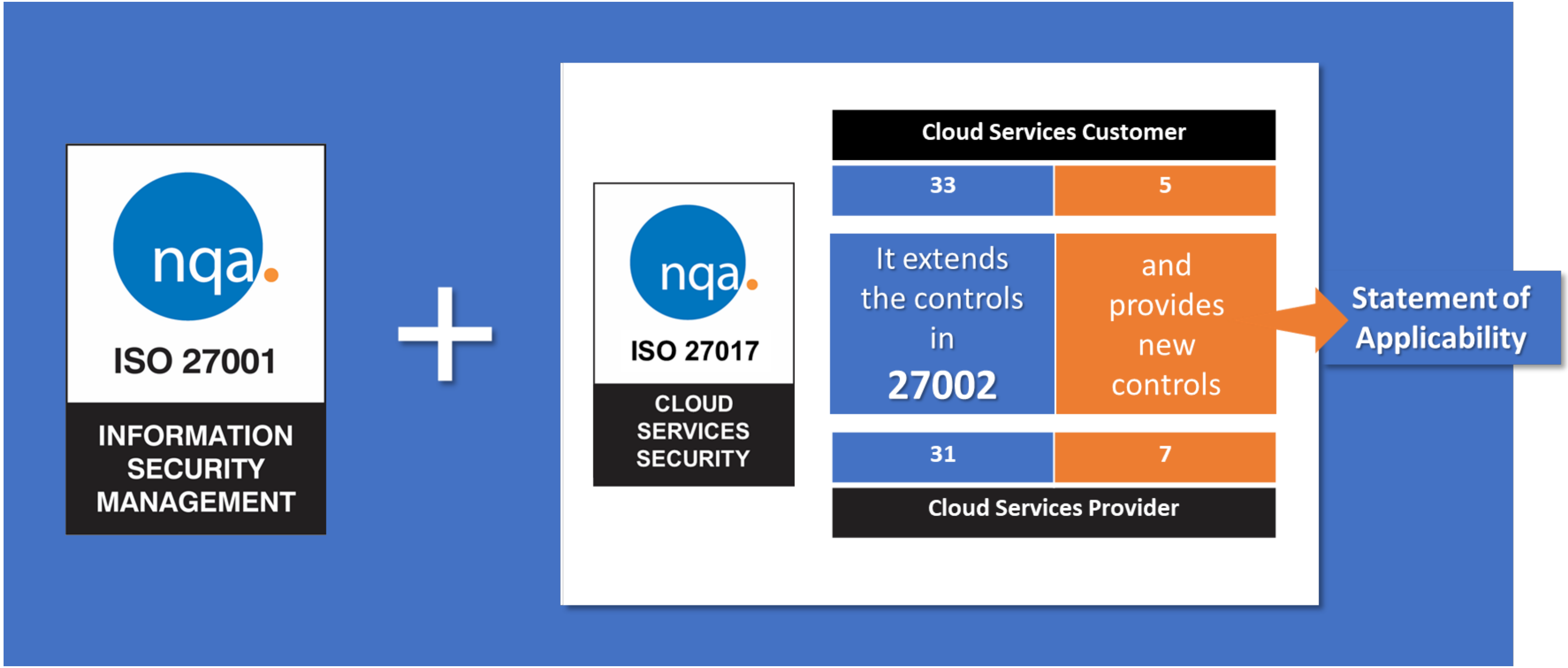
Additional implementation guidance for 8.2.2, labelling of information, of ISO/IEC 27002:2013 is:

The organization should ensure that people under its control are made aware of the definition of PII and how to recognize information that is PII.

ISO 27017

NEVER STOP IMPROVING

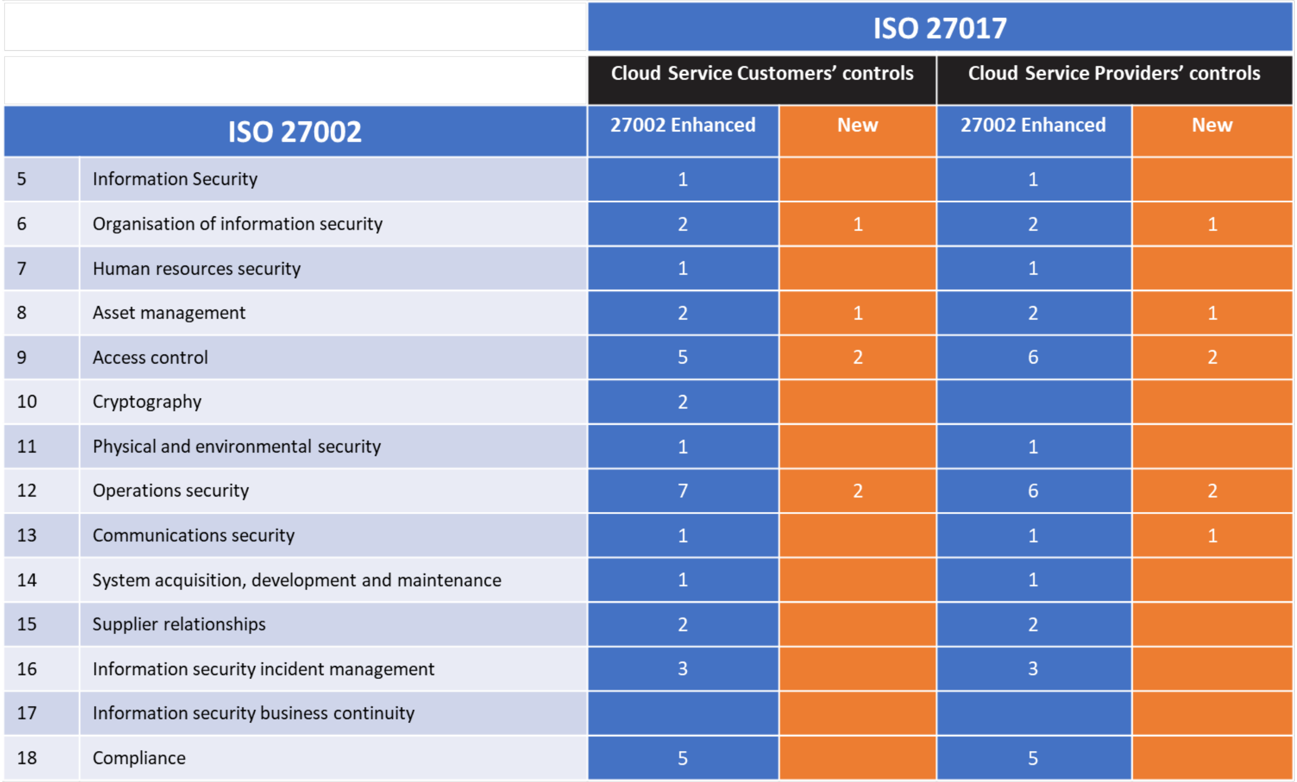
ISO 27017 – INFORMATION SECURITY CONTROLS FOR CLOUD SERVICES



Cloud Services Customer	
33	5
It extends the controls in 27002	and provides new controls
31	7
Cloud Services Provider	

NEVER STOP IMPROVING

ISO 27017 – INFORMATION SECURITY CONTROLS FOR CLOUD SERVICES



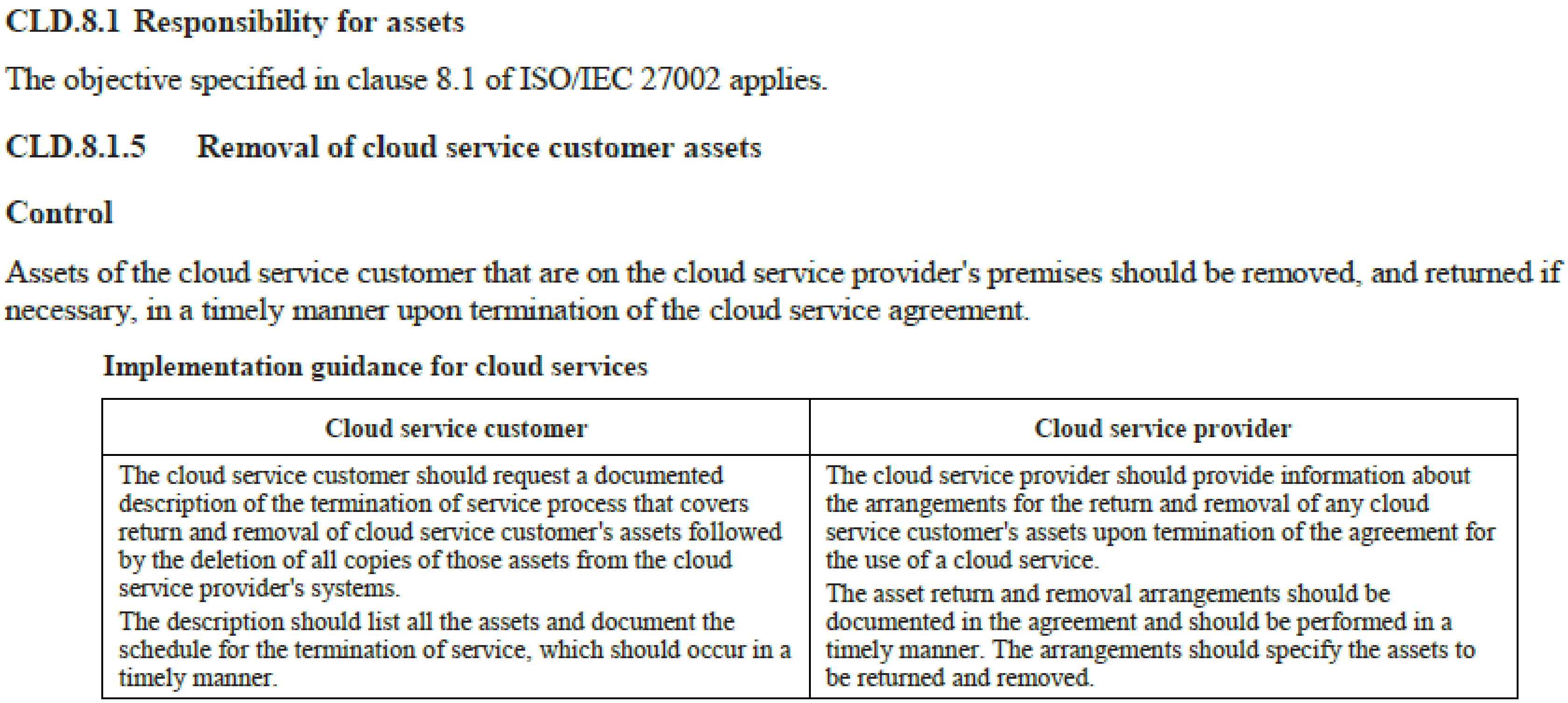
		ISO 27017			
		Cloud Service Customers’ controls		Cloud Service Providers’ controls	
ISO 27002		27002 Enhanced	New	27002 Enhanced	New
5	Information Security	1		1	
6	Organisation of information security	2	1	2	1
7	Human resources security	1		1	
8	Asset management	2	1	2	1
9	Access control	5	2	6	2
10	Cryptography	2			
11	Physical and environmental security	1		1	
12	Operations security	7	2	6	2
13	Communications security	1		1	1
14	System acquisition, development and maintenance	1		1	
15	Supplier relationships	2		2	
16	Information security incident management	3		3	
17	Information security business continuity				
18	Compliance	5		5	

nqa.
NEVER STOP IMPROVING

ISO 27017 – INFORMATION SECURITY CONTROLS FOR CLOUD SERVICES

Annex A – Cloud service extended control set	
CLD.6.3.1	Shared roles and responsibilities within a cloud computing environment
CLD.8.1.5	Removal of cloud service customer assets
CLD.9.5.1	Segregation in virtual computing environments
CLD.9.5.2	Virtual machine hardening
CLD.12.1.5	Administrator's operational security
CLD.12.4.5	Monitoring of Cloud Services
CLD.13.1.4	Alignment of security management for virtual and physical networks

ISO 27017 – INFORMATION SECURITY CONTROLS FOR CLOUD SERVICES



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

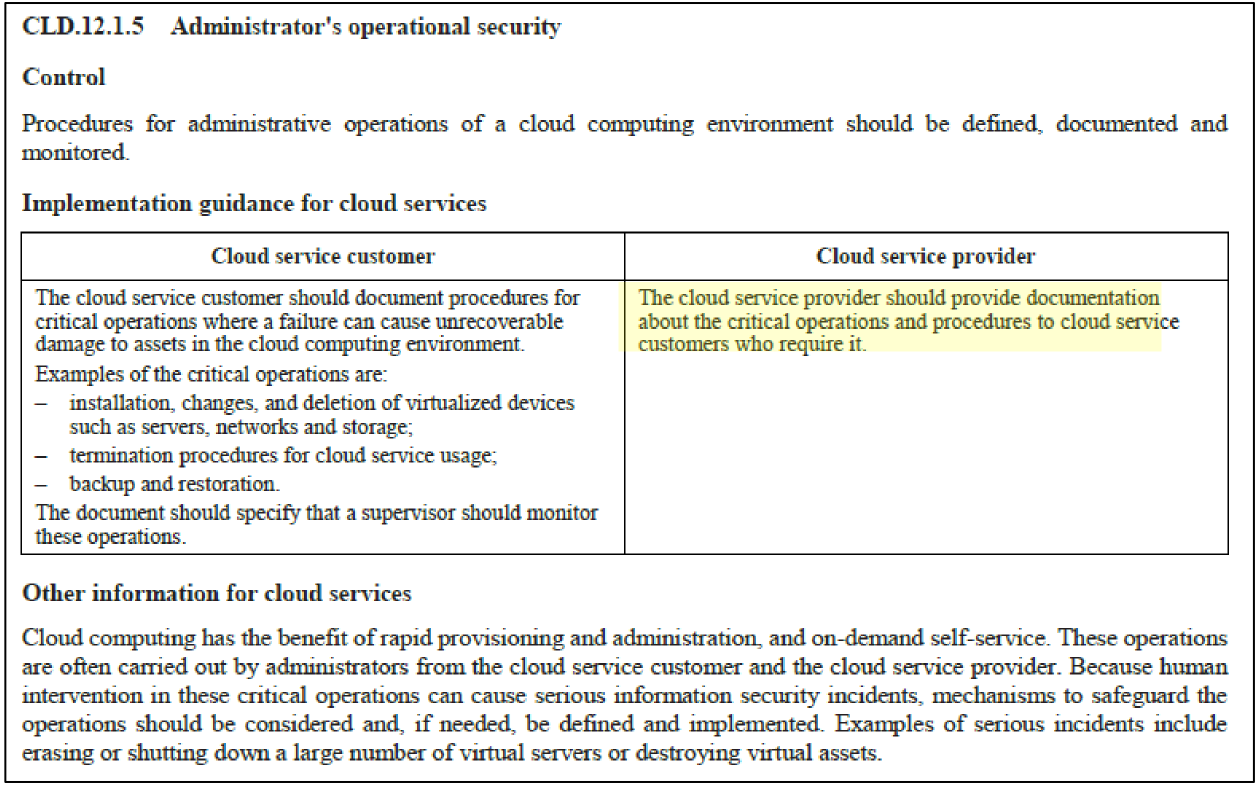
Control

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.

Implementation guidance for cloud services

Cloud service customer	Cloud service provider
The cloud service customer should request a documented description of the termination of service process that covers return and removal of cloud service customer's assets followed by the deletion of all copies of those assets from the cloud service provider's systems. The description should list all the assets and document the schedule for the termination of service, which should occur in a timely manner.	The cloud service provider should provide information about the arrangements for the return and removal of any cloud service customer's assets upon termination of the agreement for the use of a cloud service. The asset return and removal arrangements should be documented in the agreement and should be performed in a timely manner. The arrangements should specify the assets to be returned and removed.

ISO 27017 – INFORMATION SECURITY CONTROLS FOR CLOUD SERVICES



CLD.12.1.5 Administrator's operational security

Control

Procedures for administrative operations of a cloud computing environment should be defined, documented and monitored.

Implementation guidance for cloud services

Cloud service customer	Cloud service provider
The cloud service customer should document procedures for critical operations where a failure can cause unrecoverable damage to assets in the cloud computing environment. Examples of the critical operations are: – installation, changes, and deletion of virtualized devices such as servers, networks and storage; – termination procedures for cloud service usage; – backup and restoration. The document should specify that a supervisor should monitor these operations.	The cloud service provider should provide documentation about the critical operations and procedures to cloud service customers who require it.

Other information for cloud services

Cloud computing has the benefit of rapid provisioning and administration, and on-demand self-service. These operations are often carried out by administrators from the cloud service customer and the cloud service provider. Because human intervention in these critical operations can cause serious information security incidents, mechanisms to safeguard the operations should be considered and, if needed, be defined and implemented. Examples of serious incidents include erasing or shutting down a large number of virtual servers or destroying virtual assets.

ISO 27017 – INFORMATION SECURITY CONTROLS FOR CLOUD SERVICES

What are the benefits?

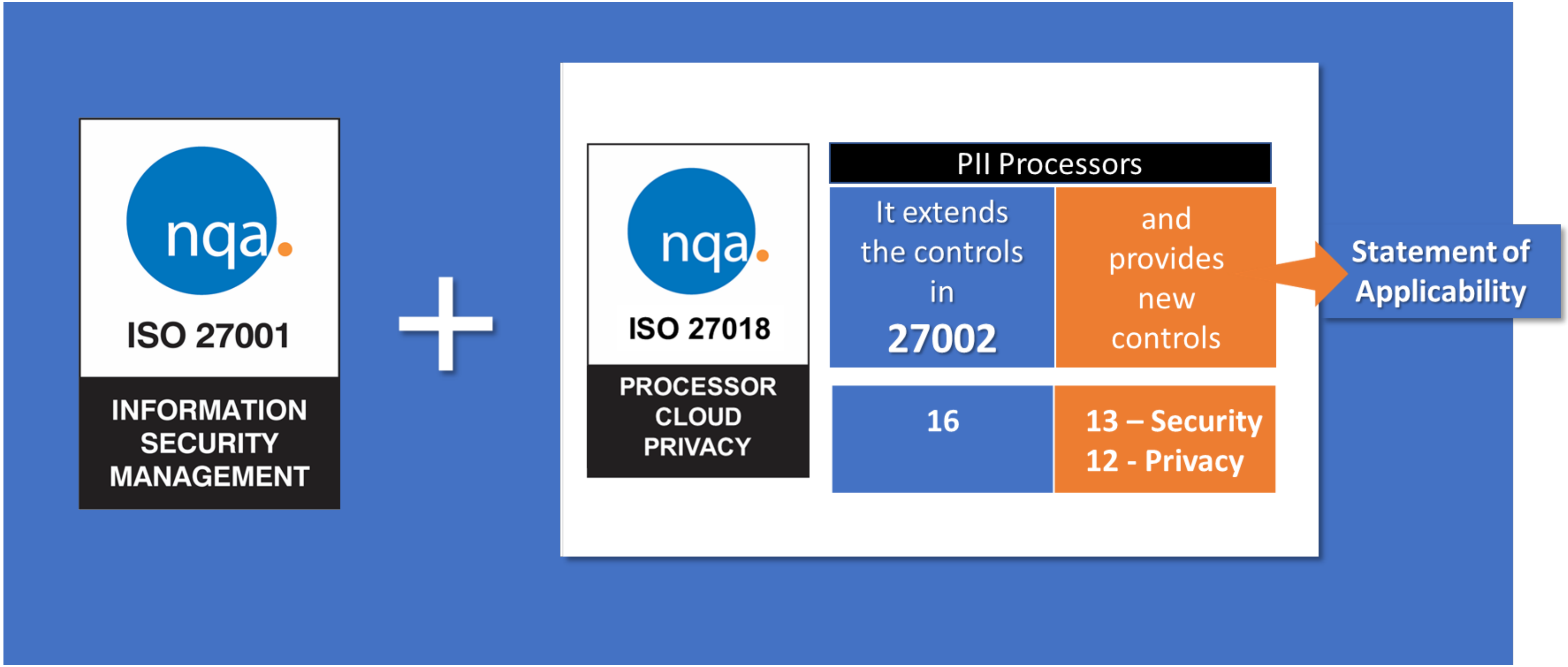
- It provides a comprehensive information security management framework for **cloud service providers** who want increased assurance on the security of their operations and of customers' information.
- It provides external assurance to customers that information processed in the cloud by the **cloud service provider** is secure.
- It provides a comprehensive information security management framework for **cloud services customers** and in so doing it holds their providers to account.
- It helps reduce the risk of a security breach.
- It extends and enhances a clients ISO 27001 certification.

NEVER STOP IMPROVING

ISO 27018

NEVER STOP IMPROVING

ISO 27018 – PROTECTION OF PII IN PUBLIC CLOUDS ACTING AS PII PROCESSORS



ISO 27001

INFORMATION SECURITY MANAGEMENT

+

ISO 27018

PROCESSOR CLOUD PRIVACY

PII Processors	
It extends the controls in **27002**	and provides new controls
16	**13 – Security** **12 - Privacy**

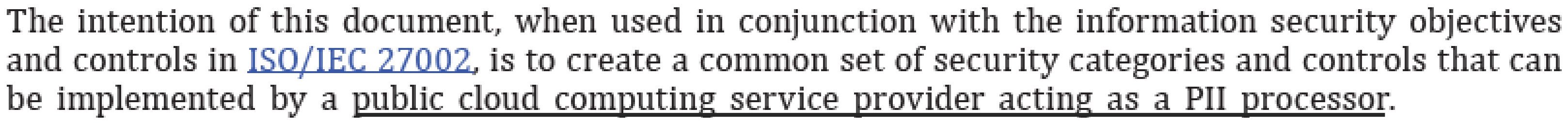
Statement of Applicability

ISO 27018 – INTENDED USE

Controller: determines the means and purposes of the processing of personal data

Processor: processes personal data on behalf of the controller

Who can use the standard?



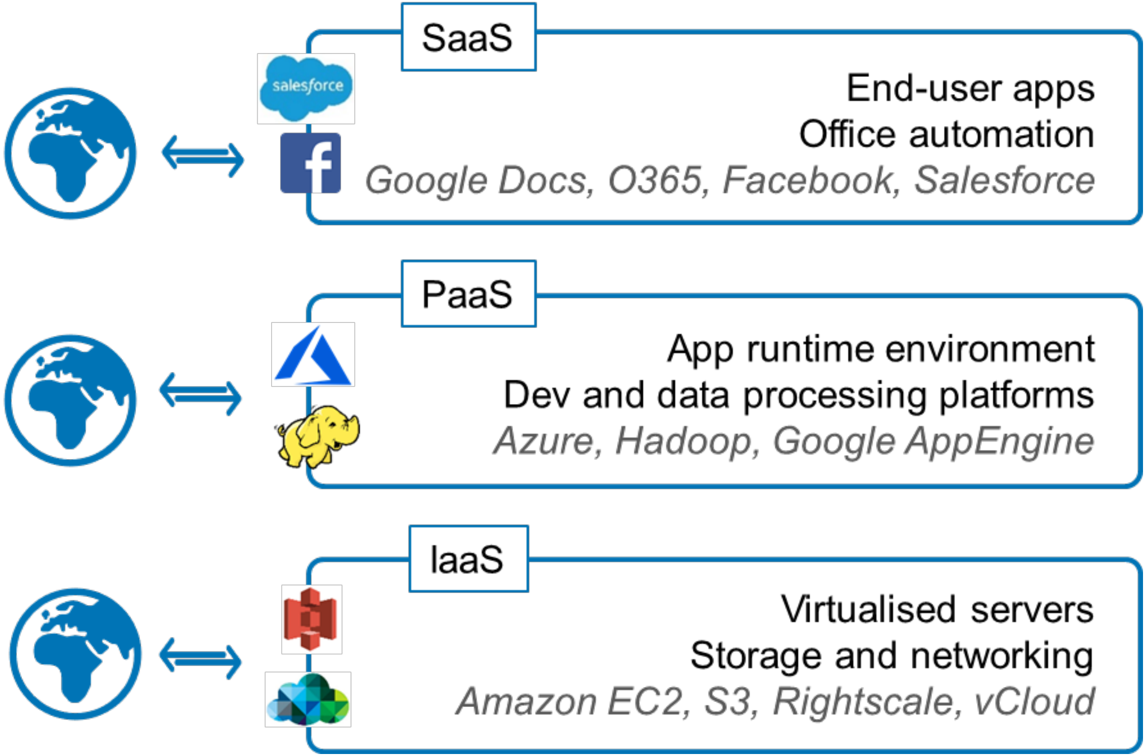
The intention of this document, when used in conjunction with the information security objectives and controls in ISO/IEC 27002, is to create a common set of security categories and controls that can be implemented by a public cloud computing service provider acting as a PII processor.

It is not for a processor who is using public cloud services

NEVER STOP IMPROVING

ISO 27018 – CONTROL SELECTION

1. Criteria for risk acceptance
2. Risk treatment options
3. Contractual arrangements
4. National and international legislation
5. **Dependent on provider's role in the cloud computing architecture when processing controller's PII**



SaaS

End-user apps

Office automation

Google Docs, O365, Facebook, Salesforce

PaaS

App runtime environment

Dev and data processing platforms

Azure, Hadoop, Google AppEngine

IaaS

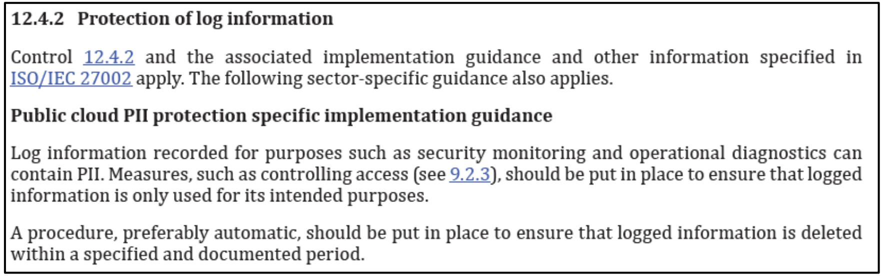
Virtualised servers

Storage and networking

Amazon EC2, S3, Rightscale, vCloud

ISO 27018 – 27002 ENHANCED CONTROLS

		ISO 27018
ISO 27002		27002 Enhanced
5	Information Security	1
6	Organisation of information security	1
7	Human resources security	1
8	Asset management	
9	Access control	3
10	Cryptography	1
11	Physical and environmental security	1
12	Operations security	4
13	Communications security	1
14	System acquisition, development and maintenance	
15	Supplier relationships	2
16	Information security incident management	2
17	Information security business continuity	
18	Compliance	1



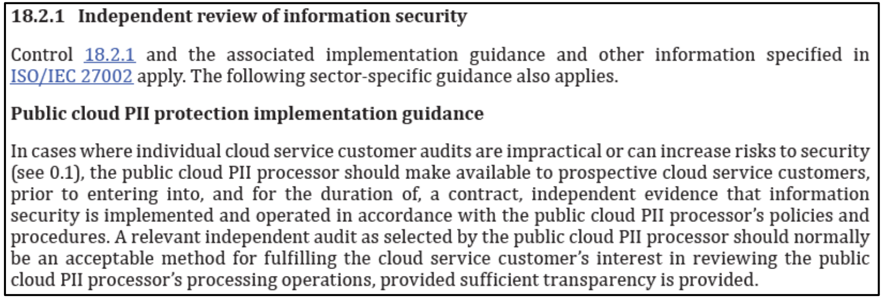
12.4.2 Protection of log information

Control 12.4.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Public cloud PII protection specific implementation guidance

Log information recorded for purposes such as security monitoring and operational diagnostics can contain PII. Measures, such as controlling access (see 9.2.3), should be put in place to ensure that logged information is only used for its intended purposes.

A procedure, preferably automatic, should be put in place to ensure that logged information is deleted within a specified and documented period.



18.2.1 Independent review of information security

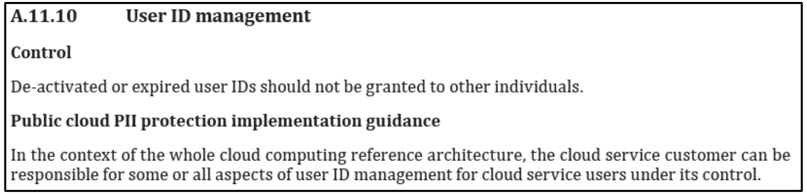
Control 18.2.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Public cloud PII protection implementation guidance

In cases where individual cloud service customer audits are impractical or can increase risks to security (see 0.1), the public cloud PII processor should make available to prospective cloud service customers, prior to entering into, and for the duration of, a contract, independent evidence that information security is implemented and operated in accordance with the public cloud PII processor's policies and procedures. A relevant independent audit as selected by the public cloud PII processor should normally be an acceptable method for fulfilling the cloud service customer's interest in reviewing the public cloud PII processor's processing operations, provided sufficient transparency is provided.

ISO 27018 – ANNEX A INFORMATION SECURITY CONTROLS

A.11	Information security
A.11.1	Confidentiality or non-disclosure agreements
A.11.2	Restriction of the creation of hardcopy material
A.11.3	Control of logging and data restoration
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
A.11.7	Secure disposal of hardcopy materials
A.11.8	Unique use of user IDs
A.11.9	Records of authorised users
A.11.10	User ID management
A.11.11	Contract measures
A.11.12	Sub-contract PII processing
A.11.13	Access to data on pre-used data storage space



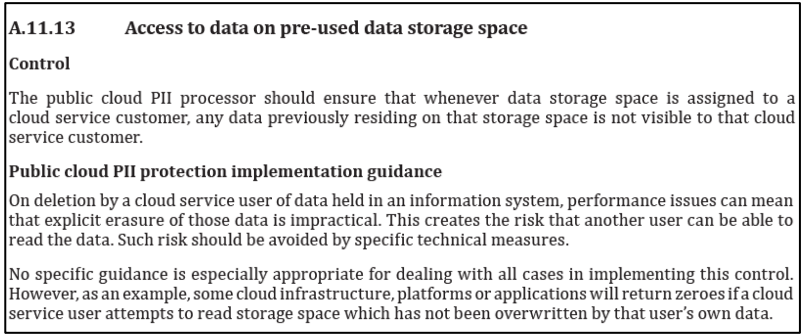
A.11.10 User ID management

Control

De-activated or expired user IDs should not be granted to other individuals.

Public cloud PII protection implementation guidance

In the context of the whole cloud computing reference architecture, the cloud service customer can be responsible for some or all aspects of user ID management for cloud service users under its control.



A.11.13 Access to data on pre-used data storage space

Control

The public cloud PII processor should ensure that whenever data storage space is assigned to a cloud service customer, any data previously residing on that storage space is not visible to that cloud service customer.

Public cloud PII protection implementation guidance

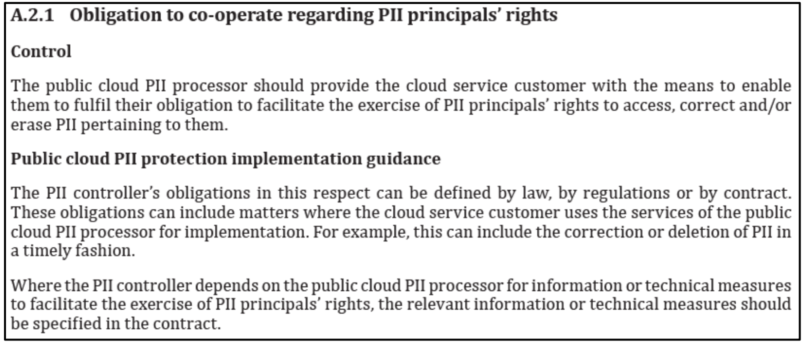
On deletion by a cloud service user of data held in an information system, performance issues can mean that explicit erasure of those data is impractical. This creates the risk that another user can be able to read the data. Such risk should be avoided by specific technical measures.

No specific guidance is especially appropriate for dealing with all cases in implementing this control. However, as an example, some cloud infrastructure, platforms or applications will return zeroes if a cloud service user attempts to read storage space which has not been overwritten by that user's own data.

Aligned to ISO 29100 – Security Techniques – Privacy framework

ISO 27018 – ANNEX A PRIVACY CONTROLS

A.2	Consent and choice
A.2.1	Obligation to cooperate regarding PII principles' rights
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
A.4	Collection limitation
A.5	Data minimisation
A.5.1	Secure erasure of temporary files
A.6	Use, retention and disclosure limitation
A.6.1	PII disclosure notification
A.6.2	Recording of PII disclosures
A.7	Accuracy and quality
A.8	Openness, transparency and notice
A.8.1	Disclosure of sub-contracted processing



A.2.1 Obligation to co-operate regarding PII principals' rights

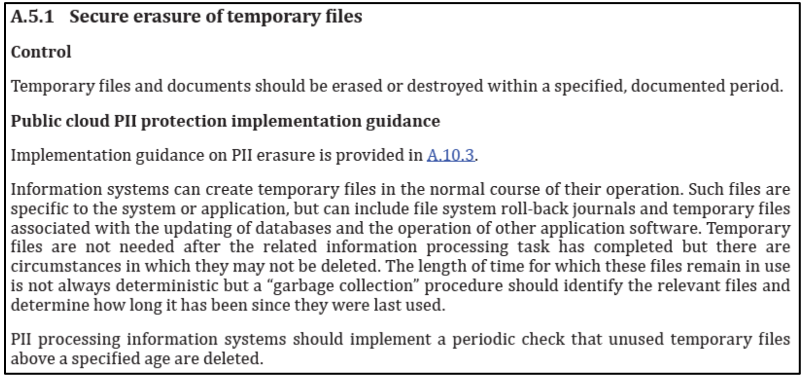
Control

The public cloud PII processor should provide the cloud service customer with the means to enable them to fulfil their obligation to facilitate the exercise of PII principals' rights to access, correct and/or erase PII pertaining to them.

Public cloud PII protection implementation guidance

The PII controller's obligations in this respect can be defined by law, by regulations or by contract. These obligations can include matters where the cloud service customer uses the services of the public cloud PII processor for implementation. For example, this can include the correction or deletion of PII in a timely fashion.

Where the PII controller depends on the public cloud PII processor for information or technical measures to facilitate the exercise of PII principals' rights, the relevant information or technical measures should be specified in the contract.



A.5.1 Secure erasure of temporary files

Control

Temporary files and documents should be erased or destroyed within a specified, documented period.

Public cloud PII protection implementation guidance

Implementation guidance on PII erasure is provided in A.10.3.

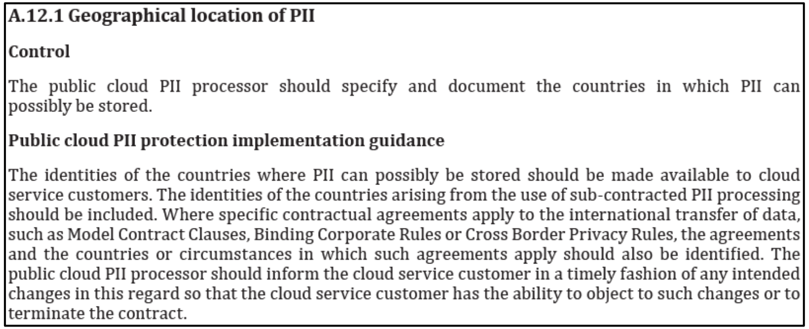
Information systems can create temporary files in the normal course of their operation. Such files are specific to the system or application, but can include file system roll-back journals and temporary files associated with the updating of databases and the operation of other application software. Temporary files are not needed after the related information processing task has completed but there are circumstances in which they may not be deleted. The length of time for which these files remain in use is not always deterministic but a "garbage collection" procedure should identify the relevant files and determine how long it has been since they were last used.

PII processing information systems should implement a periodic check that unused temporary files above a specified age are deleted.

Aligned to ISO 29100 – Security Techniques – Privacy framework

ISO 27018 – ANNEX A PRIVACY CONTROLS

A.9	Individual participation and access
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
A.12	Privacy compliance
A.12.1	Geographical location of PII
A.12.2	Intended destination of PII



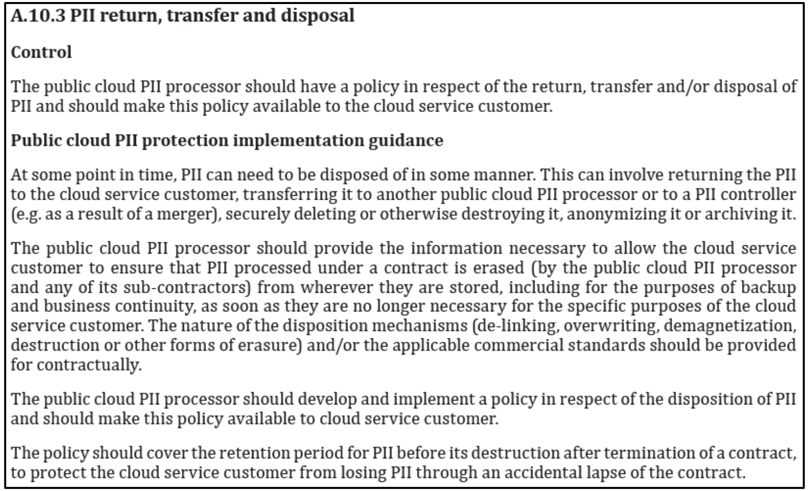
A.12.1 Geographical location of PII

Control

The public cloud PII processor should specify and document the countries in which PII can possibly be stored.

Public cloud PII protection implementation guidance

The identities of the countries where PII can possibly be stored should be made available to cloud service customers. The identities of the countries arising from the use of sub-contracted PII processing should be included. Where specific contractual agreements apply to the international transfer of data, such as Model Contract Clauses, Binding Corporate Rules or Cross Border Privacy Rules, the agreements and the countries or circumstances in which such agreements apply should also be identified. The public cloud PII processor should inform the cloud service customer in a timely fashion of any intended changes in this regard so that the cloud service customer has the ability to object to such changes or to terminate the contract.



A.10.3 PII return, transfer and disposal

Control

The public cloud PII processor should have a policy in respect of the return, transfer and/or disposal of PII and should make this policy available to the cloud service customer.

Public cloud PII protection implementation guidance

At some point in time, PII can need to be disposed of in some manner. This can involve returning the PII to the cloud service customer, transferring it to another public cloud PII processor or to a PII controller (e.g. as a result of a merger), securely deleting or otherwise destroying it, anonymizing it or archiving it.

The public cloud PII processor should provide the information necessary to allow the cloud service customer to ensure that PII processed under a contract is erased (by the public cloud PII processor and any of its sub-contractors) from wherever they are stored, including for the purposes of backup and business continuity, as soon as they are no longer necessary for the specific purposes of the cloud service customer. The nature of the disposition mechanisms (de-linking, overwriting, demagnetization, destruction or other forms of erasure) and/or the applicable commercial standards should be provided for contractually.

The public cloud PII processor should develop and implement a policy in respect of the disposition of PII and should make this policy available to cloud service customer.

The policy should cover the retention period for PII before its destruction after termination of a contract, to protect the cloud service customer from losing PII through an accidental lapse of the contract.

Aligned to ISO 29100 – Security Techniques – Privacy framework

ISO 27018 – PROTECTION OF PII IN PUBLIC CLOUDS ACTING AS PII PROCESSORS

What are the benefits?

- It provides a comprehensive privacy framework for cloud service providers who want increased assurance on the privacy compliance of their cloud services.
- It provides external assurance to customers that personal information processed in the cloud by the cloud service provider is managed in a compliant manner.
- It helps reduce the risk of a privacy breach and fines from the ICO.
- It extends and enhances a client’s ISO 27001 certification.
- It may be considered an appropriate alternative to ISO 27701 where the client only requires external assurance of the cloud services provision of their business.

NEVER STOP IMPROVING

ISO 27018 VS ISO 27701

NEVER STOP IMPROVING

ISO 27701 – EXTENSION TO 27001 AND 27002 FOR PRIVACY INFORMATION MANAGEMENT

27701 Chapter	27001 Annex SL Clause extension	27002 Guidance enhancements	27001 Annex A additions
Clause 5	6 (clauses 4 and 6)		
Clause 6		37	
Clause 7		Guidance for 27701 Annex A	
Clause 8		Guidance for 27701 Annex B	
Annex A			31 (Controllers)
Annex B			18 (Processors)
Annex C	Maps 27701 to ISO 29100		
Annex D	Maps 27701 to GDPR		
Annex E	Maps 27701 to 27018 and 29151		
Annex F	Provides guidance for applying 27701 to 27001 and 27002		

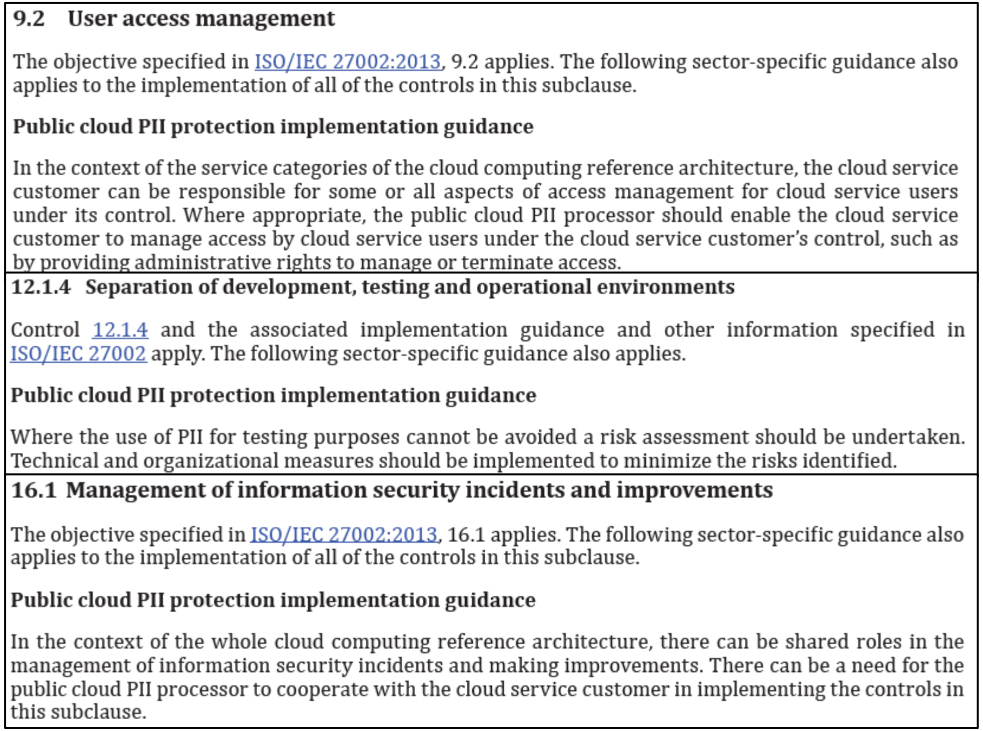
CNIL Press Release 2019

‘The standard was drafted at an international level with contributions from experts from all continents and the participation of several data protection authorities. Experts from the CNIL actively contributed to this standard, with the support of the European Data Protection Board. It represents the state of the art in terms of privacy protection and will allow organisations adopting it to increase their maturity and demonstrate an active approach to data protection.’

NEVER STOP IMPROVING

ISO 27018 – 27701 MAPPING

27018		27701
5.1.1	Policies for Information Security	X
6.1.1	Information security roles and responsibilities	X
7.2.2	Information security awareness, education and training	X
9.2	User access management	
9.2.1	User registration and de-registration	X
9.4.2	Secure log-on procedures	X
10.1.1	Policy on the use of cryptographic controls	
11.2.7	Secure disposal or re-use of equipment	X
12.1.4	Separation of development and operational environments	
12.3.1	Information backup	
12.4.1	Event logging	X
12.4.2	Protection of log information	X
13.2.1	Information exchange policies and procedures	X
16.1	Management of information security incidents and improvements	
16.1.1	Responsibilities and procedures	X
18.2.1	Independent review of information security	X



9.2 User access management

The objective specified in ISO/IEC 27002:2013, 9.2 applies. The following sector-specific guidance also applies to the implementation of all of the controls in this subclause.

Public cloud PII protection implementation guidance

In the context of the service categories of the cloud computing reference architecture, the cloud service customer can be responsible for some or all aspects of access management for cloud service users under its control. Where appropriate, the public cloud PII processor should enable the cloud service customer to manage access by cloud service users under the cloud service customer's control, such as by providing administrative rights to manage or terminate access.

12.1.4 Separation of development, testing and operational environments

Control 12.1.4 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Public cloud PII protection implementation guidance

Where the use of PII for testing purposes cannot be avoided a risk assessment should be undertaken. Technical and organizational measures should be implemented to minimize the risks identified.

16.1 Management of information security incidents and improvements

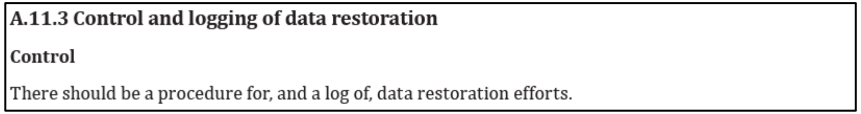
The objective specified in ISO/IEC 27002:2013, 16.1 applies. The following sector-specific guidance also applies to the implementation of all of the controls in this subclause.

Public cloud PII protection implementation guidance

In the context of the whole cloud computing reference architecture, there can be shared roles in the management of information security incidents and making improvements. There can be a need for the public cloud PII processor to cooperate with the cloud service customer in implementing the controls in this subclause.

ISO 27018 – 27701 MAPPING

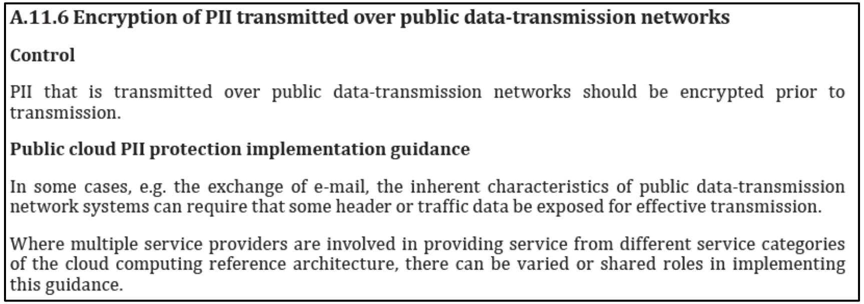
27018 Annex A		27701
A.2.1	Obligation to cooperate regarding PII principles' rights	X
A.3.1	Public cloud PII processor's purpose	X
A.3.2	Public cloud PII processor's commercial use	X
A.5.1	Secure erasure of temporary files	X
A.6.1	PII disclosure notification	X
A.6.2	Recording of PII disclosures	X
A.8.1	Disclosure of sub-contracted processing	X
A.10.1	Notification of a data breach involving PII	X
A.10.2	Retention period for administrative security policies and guidelines	X
A.10.3	PII return, transfer and disposal	X
A.11.1	Confidentiality or non-disclosure agreements	X
A.11.2	Restriction of the creation of hardcopy material	X
A.11.3	Control of logging and data restoration	
A.11.4	Protecting data on storage media leaving the premises	X
A.11.5	Use of unencrypted portable storage media and devices	X
A.11.6	Encryption of PII transmitted over public data-transmission networks	
A.11.7	Secure disposal of hardcopy materials	
A.11.8	Unique use of user IDs	X
A.11.9	Records of authorised users	X
A.11.10	User ID management	X
A.11.11	Contract measures	X
A.11.12	Sub-contract PII processing	
A.11.13	Access to data on pre-used data storage space	X
A.12.1	Geographical location of PII	X
A.12.2	Intended destination of PII	X



A.11.3 Control and logging of data restoration

Control

There should be a procedure for, and a log of, data restoration efforts.



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

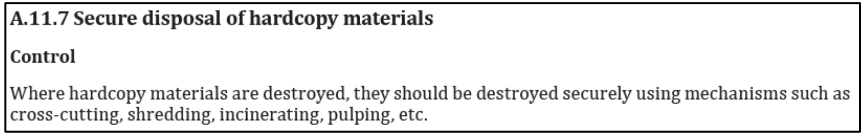
Control

PII that is transmitted over public data-transmission networks should be encrypted prior to transmission.

Public cloud PII protection implementation guidance

In some cases, e.g. the exchange of e-mail, the inherent characteristics of public data-transmission network systems can require that some header or traffic data be exposed for effective transmission.

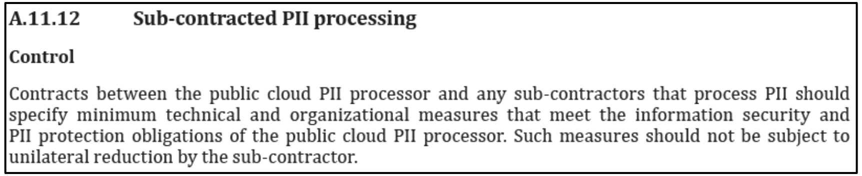
Where multiple service providers are involved in providing service from different service categories of the cloud computing reference architecture, there can be varied or shared roles in implementing this guidance.



A.11.7 Secure disposal of hardcopy materials

Control

Where hardcopy materials are destroyed, they should be destroyed securely using mechanisms such as cross-cutting, shredding, incinerating, pulping, etc.



A.11.12 Sub-contracted PII processing

Control

Contracts between the public cloud PII processor and any sub-contractors that process PII should specify minimum technical and organizational measures that meet the information security and PII protection obligations of the public cloud PII processor. Such measures should not be subject to unilateral reduction by the sub-contractor.

NEVER STOP IMPROVING

SUMMARY

ANNEX A SUMMARY OF CONTROLS

ISO 27017
CLOUD SERVICES SECURITY

Cloud Services Customer	
33	5
It extends the controls in **27002**	and provides new controls
31	7
Cloud Services Provider	

ISO 27018
PROCESSOR CLOUD PRIVACY

PII Processors	
It extends the controls in **27002**	and provides new controls
16	13 – Security 12 - Privacy

8 Annex A controls extended 4 times

ISO 27701
PRIVACY INFORMATION MANAGEMENT

PII Controllers		
6	37	31
It extends the clauses in **27001**	It extends the controls in **27002**	and provides new controls
6	37	18
PII Processors		

NEVER STOP IMPROVING

SUMMARY OF CONTROLS

- ✓ **ISO 27001** is a management system with Annex A containing 114 security controls
- ✓ **ISO 27002** is code of practice with guidance on the 114 security controls in ISO 27001 Annex A
- ✓ **ISO 27017 is a code of practice with:**
  - Guidance for cloud service customers on 33 of the 114 security controls in ISO 27002
  - Guidance for cloud service providers on 31 of the 114 security controls in ISO 27002
  - Annex A with 5 controls *and* guidance for cloud service customers and 7 controls *and* guidance for cloud service providers. These are in addition to the 114 controls in ISO 27002 and should be considered in addition to the 114 controls in 27001 Annex A for inclusion in the SoA.
- ✓ **ISO 27018 is a code of practice with:**
  - Guidance on 16 of the 114 security controls in 27002
  - Annex A with 25 controls *and* guidance. These are in addition to the 114 controls in ISO 27002 and should be considered in addition to the 114 controls in 27001 Annex A for inclusion in the SoA.

NEVER STOP IMPROVING

SUMMARY OF CONTROLS

✓ **ISO 27701 is a management system and a code of practice with:**

- Clause 5 that contains 6 PIMS-specific refinements to ISO 27001 Annex SL clauses
- Clause 6 that contains guidance on 37 of the 114 security controls in ISO 27002
- Clause 7 that contains guidance on the 31 controls for controllers in ISO 27701 Annex A
- Clause 8 that contains guidance on the 18 controls for processors in ISO 27701 Annex B
- Annex A containing 31 privacy controls for controllers which must be considered in addition to the 114 controls in ISO 27001 Annex A for inclusion in the SoA.
- Annex B containing 18 privacy controls for processors which must be considered in addition to the 114 controls in ISO 27001 Annex A for inclusion in the SoA.

> *“The rigour of a certified management system has sped up the process and ensured that we have been able to deliver what our clients need: an uninterrupted service.”*
>
> **E.L.F.S.**

WHAT WE COVERED

- Extensions to ISO 27002
- ISO 27017 overview
- ISO 27018 overview
- The relationship between ISO 27018 and ISO 27701
- Q&A

NEVER STOP IMPROVING

Q&A

nqa.

NEVER STOP IMPROVING

THANK YOU

Warwick House | Houghton Hall Park | Houghton Regis | Dunstable | LU5 5ZX | United Kingdom
0800 052 2424 | | www.nqa.com