



Your partner
in progress

มาตรฐานการจัดการ ของผู้ให้บริการ *Cloud service*

Webinar

บรรยายโดย

อาจารย์กิตติพงษ์ เกียรตินิยมรุ่ง

Product Technical Manager, BSI Thailand



Agenda

- 01 General information – Cloud type
- 02 ข้อกฎหมายไทยที่เกี่ยวข้องกับผู้ให้บริการ Cloud
- 03 มาตรฐานการจัดการของผู้ให้บริการ Cloud service
- 04 การขอการรับรอง



Your partner
in progress

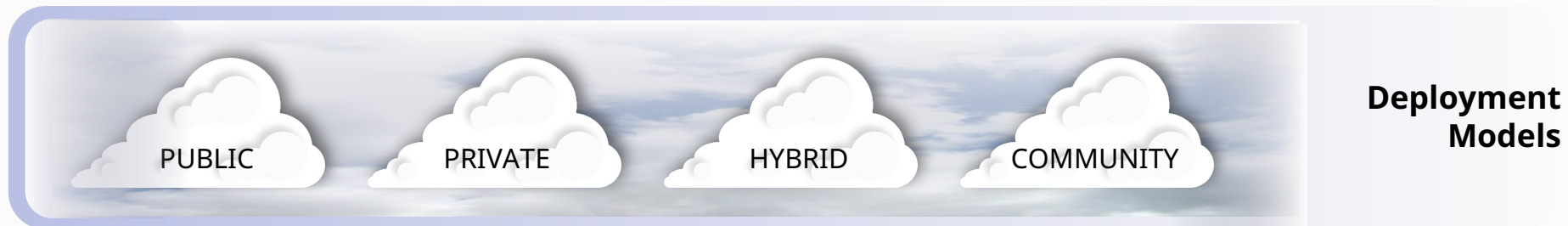
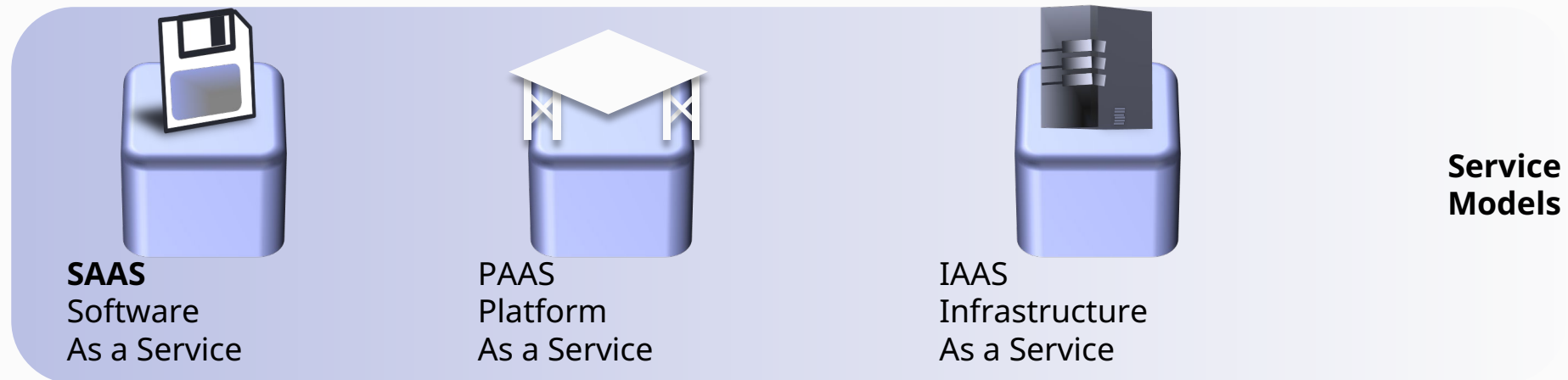
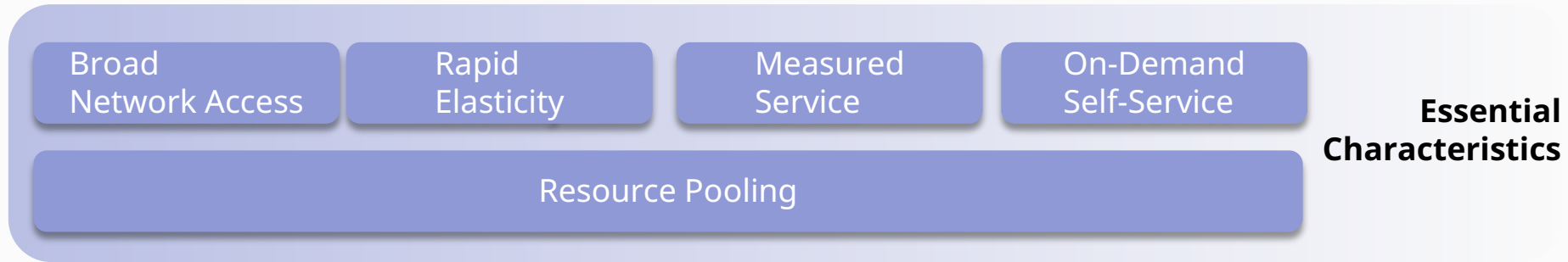
General information

Cloud type

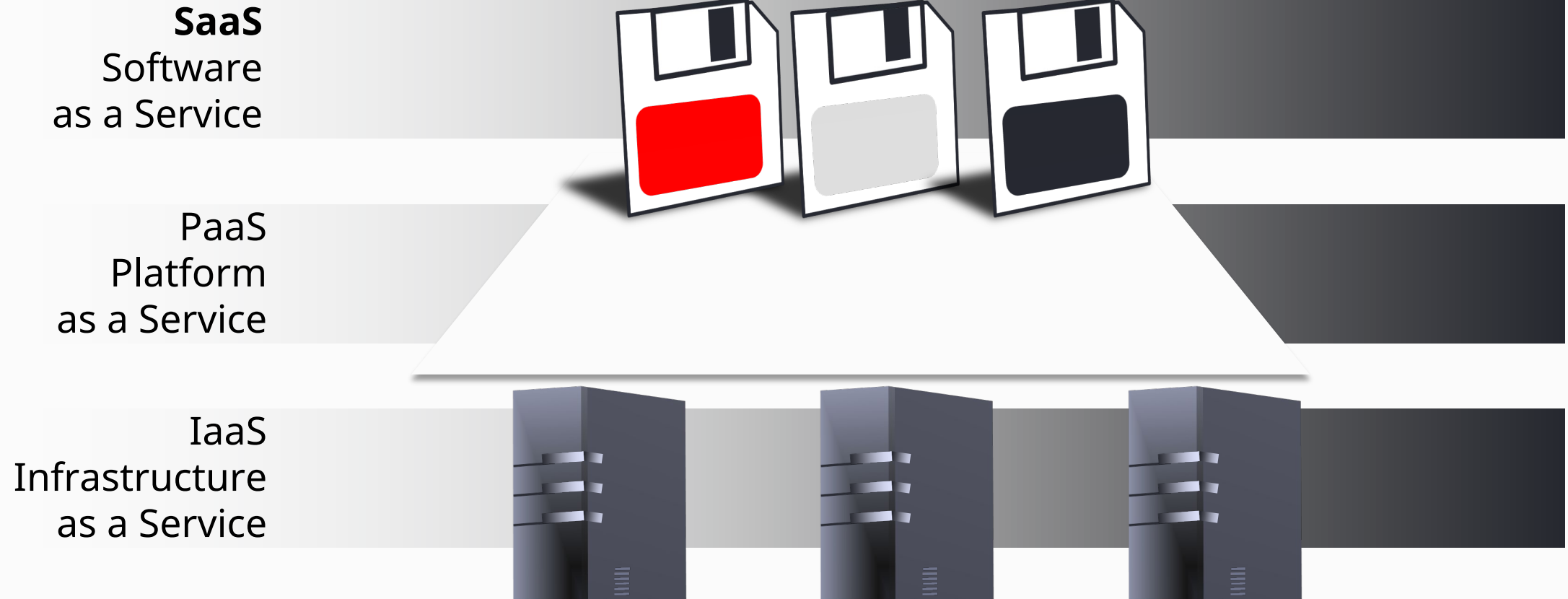
What is the Cloud?



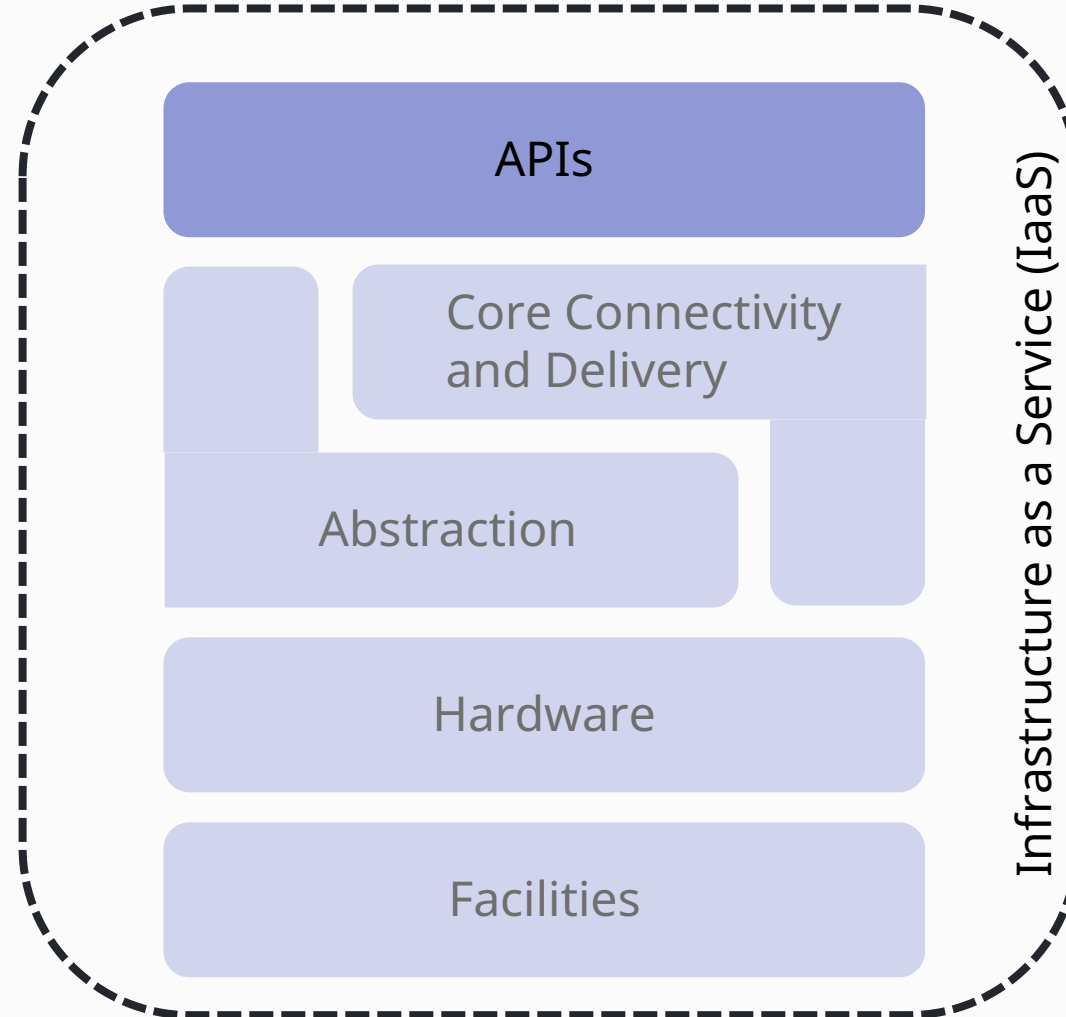
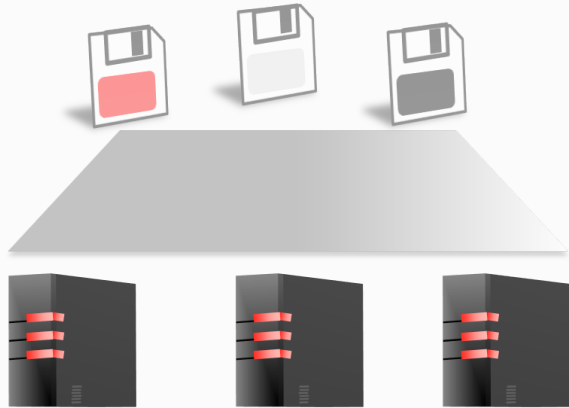
What is the Cloud?



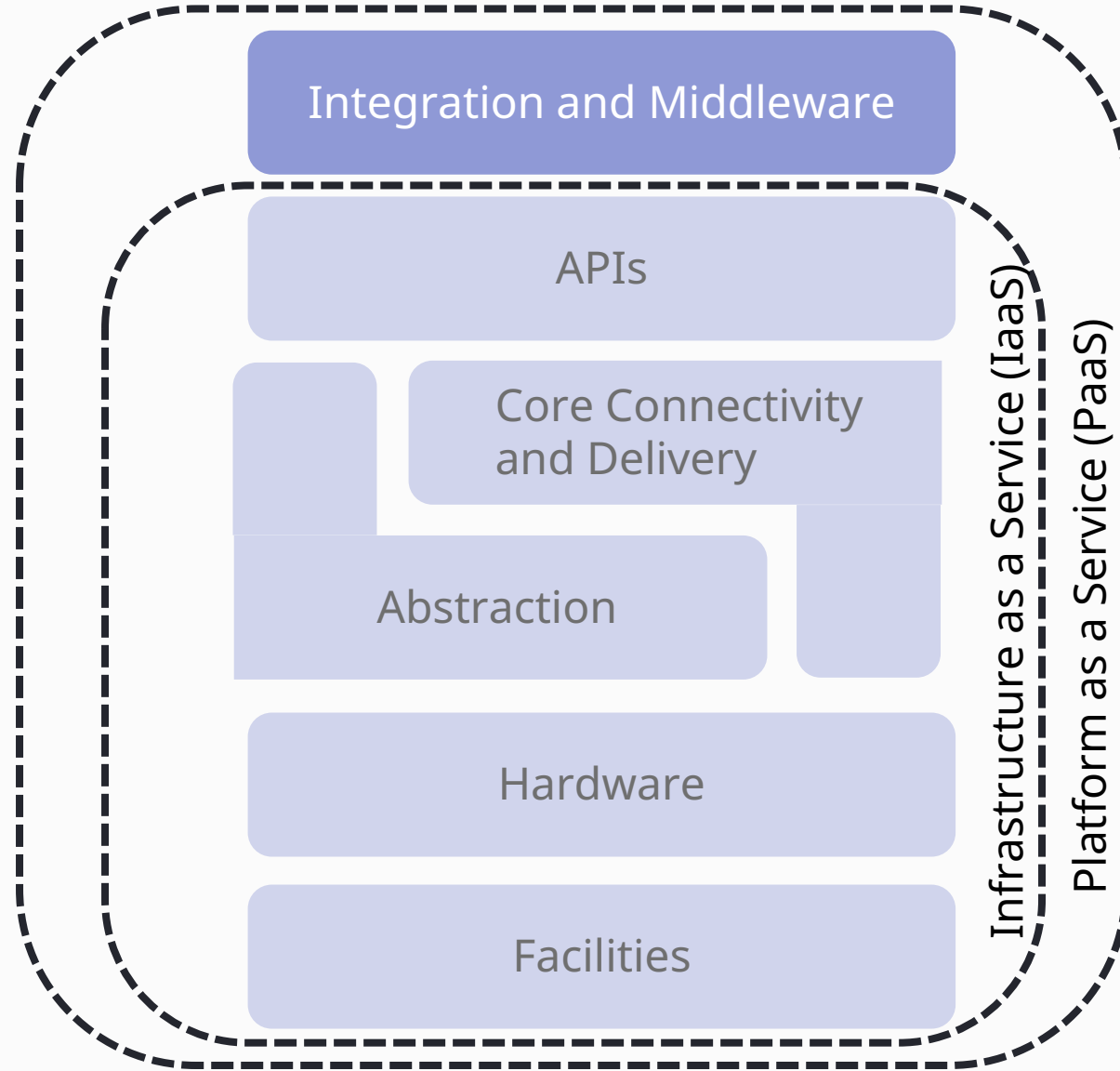
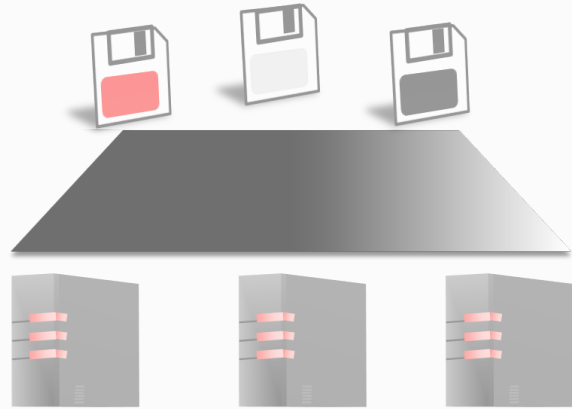
Cloud service models



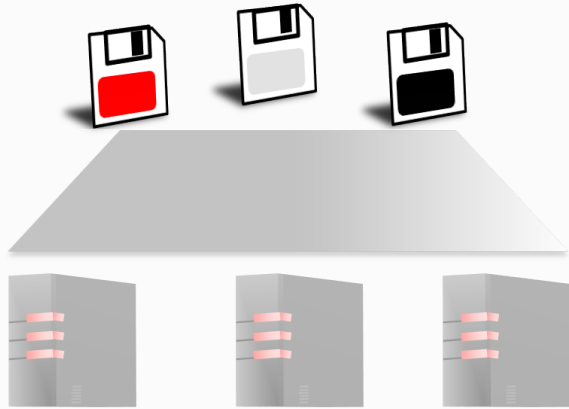
Infrastructure as a Service (IaaS)



Platform as a Service (PaaS)



Software as a Service (SaaS)



Presentation
Modality

Presentation
Platform

APIs

Applications

Data

Metadata

Content

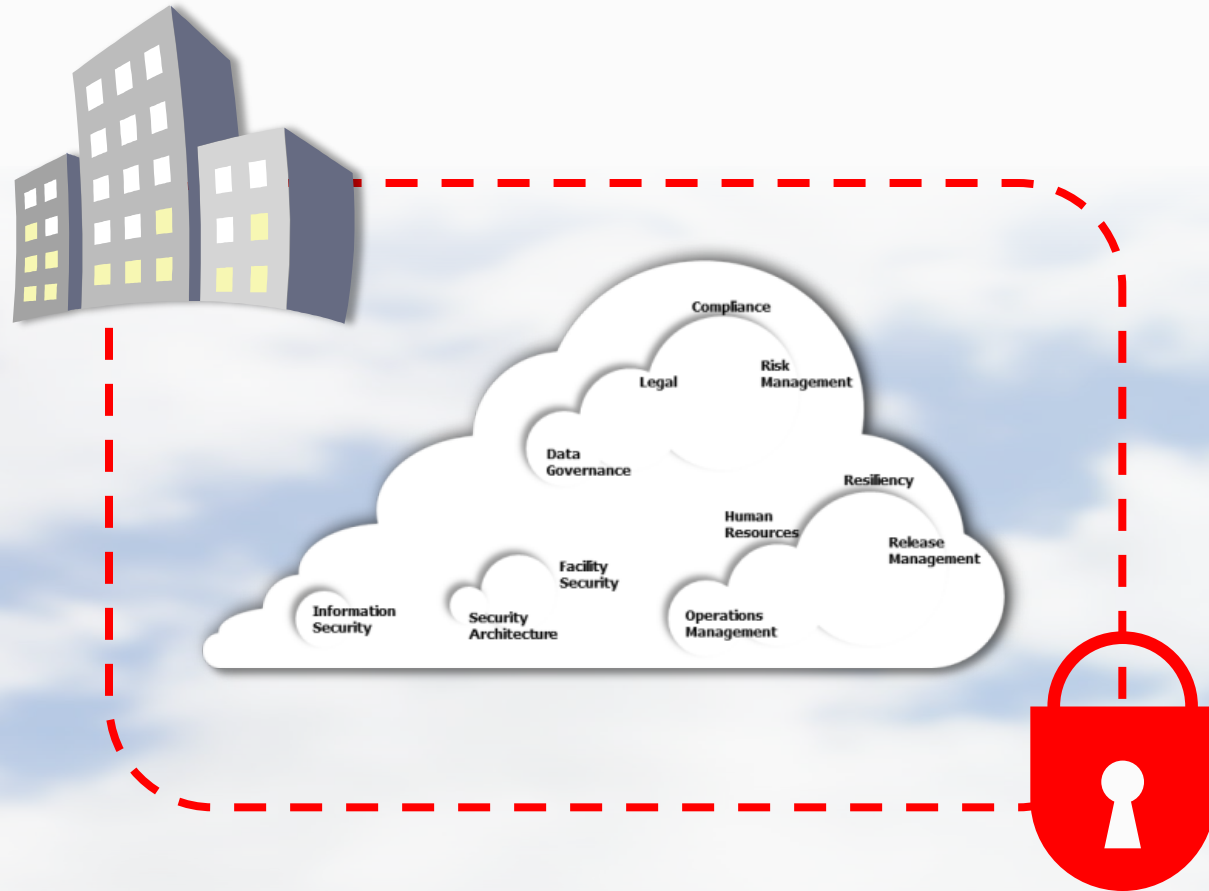
Public Cloud

- Available to anyone over the Internet
- Multiple locations and countries
- Potential legal and regulatory issues?



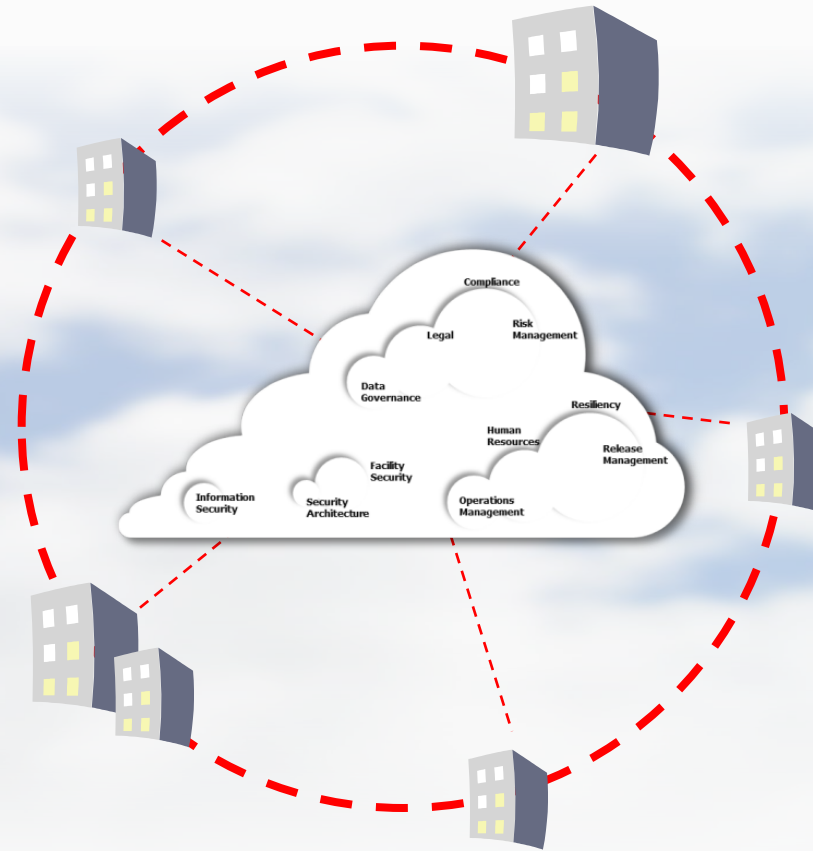
Private Cloud

- “Internal Cloud”
- Built to serve one group or company
- Best of both worlds
- First step to full cloud computing



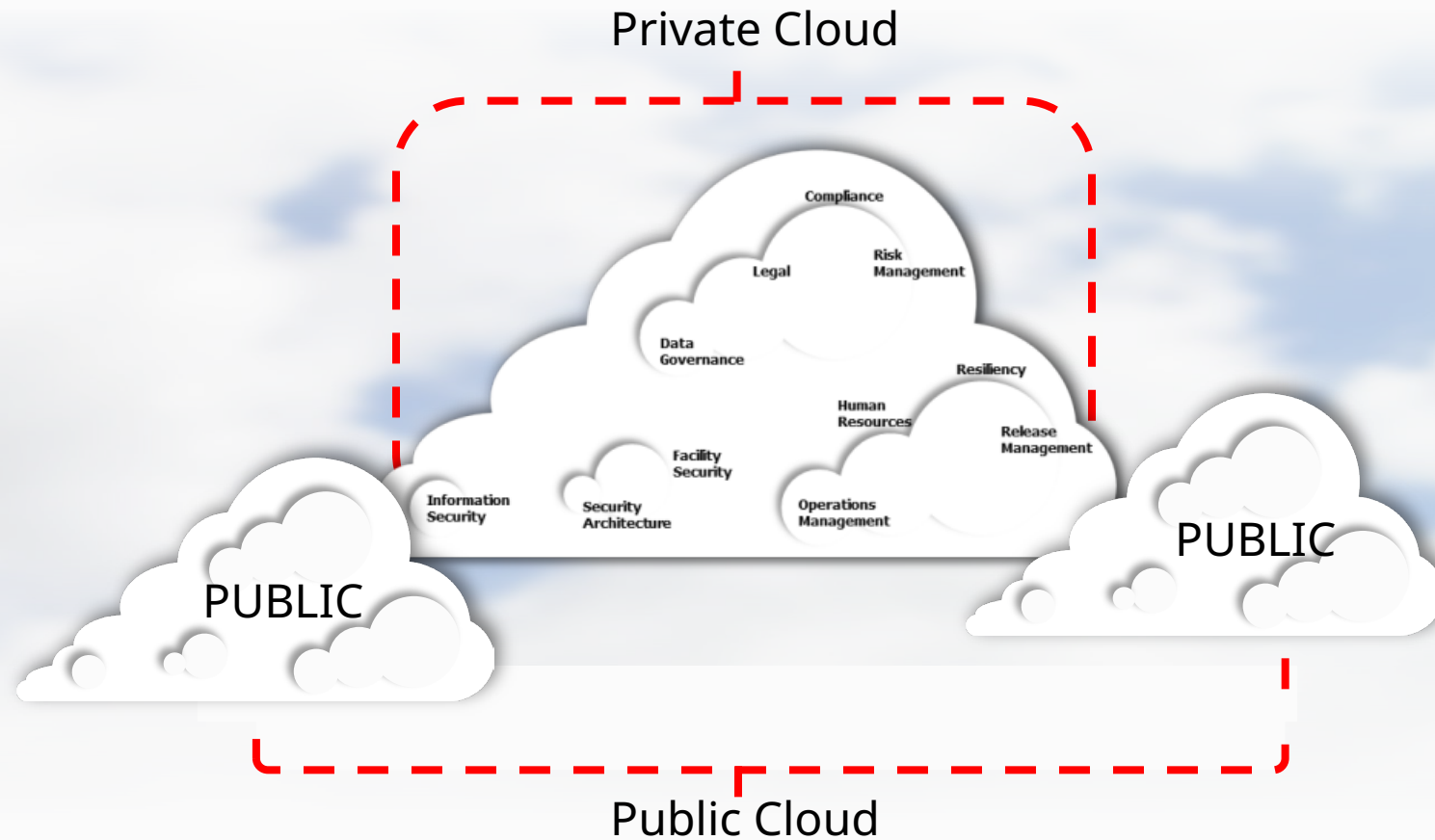
Community Cloud

- Used by a group of companies or organizations



Hybrid Cloud

Public and Private Cloud amalgamation

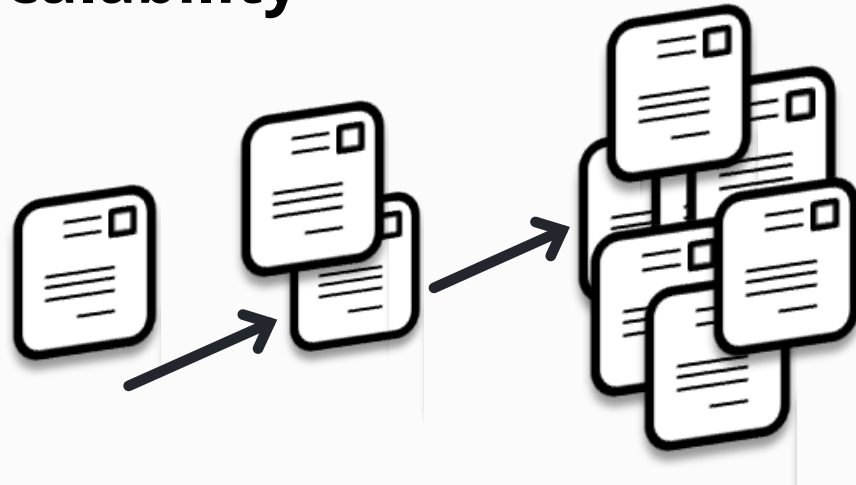


Cloud pros

Cost savings



Scalability



Flexibility



What laws apply to the Cloud?



What laws apply to the Cloud?

It is impossible to say which laws will be applicable to each organization, as there are many permutations that need to be taken into consideration.





ข้อกำหนดไทยที่เกี่ยวข้อง
กับผู้ให้บริการ

Cloud



ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของระบบคลาวด์ 2567

หน้า ๑๖

เล่ม ๑๔๑ ตอนพิเศษ ๒๔๘ ง

ราชกิจจานุเบกษา

๑๐ กันยายน ๒๕๖๗

ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. ๒๕๖๗

โดยที่พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กำหนดให้ คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ มีหน้าที่และอำนาจสร้างมาตรฐาน เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ และกำหนดมาตรฐานขั้นต่ำที่เกี่ยวข้องกับคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือโปรแกรมคอมพิวเตอร์ จึงสมควรมีมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ระบบคลาวด์ เพื่อให้การดำเนินงานเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์เป็นไปอย่างมีประสิทธิภาพ

อาศัยอำนาจตามความในมาตรา ๙ (๔) แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ประกอบกับมติที่ประชุมคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ในคราวการประชุมครั้งที่ ๒/๒๕๖๗ เมื่อวันที่ ๓๑ กรกฎาคม ๒๕๖๗ คณะกรรมการการรักษา ความมั่นคงปลอดภัยไซเบอร์แห่งชาติจึงออกประกาศไว้ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ แห่งชาติ เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. ๒๕๖๗”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับเมื่อพ้นกำหนดสองปีนับแต่วันประกาศในราชกิจจานุเบกษา เป็นต้นไป

ข้อ ๓ ในประกาศนี้

ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของระบบคลาวด์ 2567

ตารางข้อกำหนดขั้นต่ำและการตรวจรับรองสำหรับผู้ให้บริการคลาวด์และผู้ให้บริการคลาวด์

ประเภทของข้อมูลหรือระบบสารสนเทศ*	ข้อกำหนดขั้นต่ำ	การตรวจรับรองสำหรับผู้ให้บริการคลาวด์	การตรวจรับรองสำหรับผู้ให้บริการคลาวด์
ผลกระทบระดับต่ำ	ข้อกำหนดส่วนที่ ๑ - เฉพาะข้อ ๕.๑.๑, ๕.๑.๒ ข้อกำหนดส่วนที่ ๒ - เฉพาะข้อ ๕.๒.๑, ๕.๒.๒, ๕.๒.๓, ๕.๒.๔, ๕.๒.๘, ๕.๒.๙	ประเมินตนเอง (Self-assessment) พร้อมแนบหลักฐานและขออนุมัติไปยังผู้บริหารสูงสุดของหน่วยงาน โดยเก็บรักษาไว้ที่หน่วยงาน และส่งให้สำนักงานด้วย	ได้รับการรับรองโดยหน่วยงานให้บริการตรวจรับรอง (Certify Body) ตามวงรอบ ๓ ปี ประกอบด้วย การตรวจรับรองในปีที่ ๑ และการตรวจสอบในปีที่ ๒ และ ๓ และได้รับการรับรองตามมาตรฐาน ISO/IEC 27001 Certification และ CSA STAR Level 1/CCM Lite เป็นอย่างน้อย
ผลกระทบระดับกลาง	ข้อกำหนดส่วนที่ ๑ - ทุกข้อ ข้อกำหนดส่วนที่ ๒ - เฉพาะข้อ ๕.๒.๑, ๕.๒.๒, ๕.๒.๓, ๕.๒.๔, ๕.๒.๗, ๕.๒.๘, ๕.๒.๙, ๕.๒.๑๐	ได้รับการรับรองโดยหน่วยงานความคุ้มหรือกำกับดูแล (Attestation) หรือ ได้รับการรับรองโดยหน่วยงานให้บริการตรวจรับรอง (Certify Body) ตามวงรอบ ๓ ปี ประกอบด้วย การตรวจรับรองในปีที่ ๑ และการตรวจสอบในปีที่ ๒ และ ๓	ได้รับการรับรองโดยหน่วยงานให้บริการตรวจรับรอง (Certify Body) ตามวงรอบ ๓ ปี ประกอบด้วย การตรวจรับรองในปีที่ ๑ และการตรวจสอบในปีที่ ๒ และ ๓ และได้รับการรับรองตามมาตรฐาน CSA STAR Level 2/CCM และ ISO/IEC 27701 Certification เป็นอย่างน้อย

ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของระบบคลาวด์ 2567

ผลกระทประดับสูง	ข้อกำหนดส่วนที่ ๑ - ทุกข้อ ข้อกำหนดส่วนที่ ๒ - ทุกข้อ	ได้รับการรับรองโดยหน่วยงาน ให้บริการตรวจรับรอง (Certify Body) ตามวงรอบ ๓ ปี ประกอบด้วย การตรวจรับรองในปีที่ ๑ และการ ตรวจสอบในปีที่ ๒ และ ๓	ได้รับการรับรองโดยหน่วยงาน ให้บริการตรวจรับรอง (Certify Body) ตามวงรอบ ๓ ปี ประกอบด้วย การตรวจรับรองในปีที่ ๑ และการตรวจสอบ ในปีที่ ๒ และ ๓ และได้รับการ รับรองตามมาตรฐาน ISO/IEC 27017 Certification หรือ CSA STAR Level 2/CCM และ ISO/IEC 27018 Certification และ ISO/IEC 27701 Certification เป็นอย่างน้อย



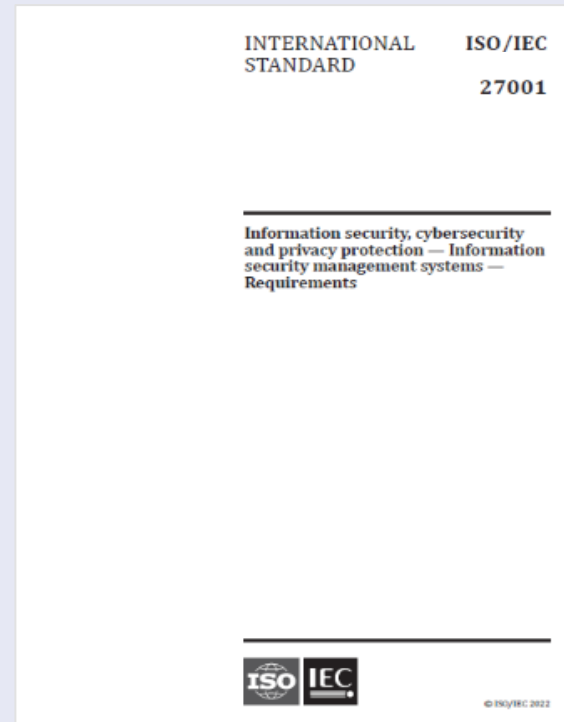
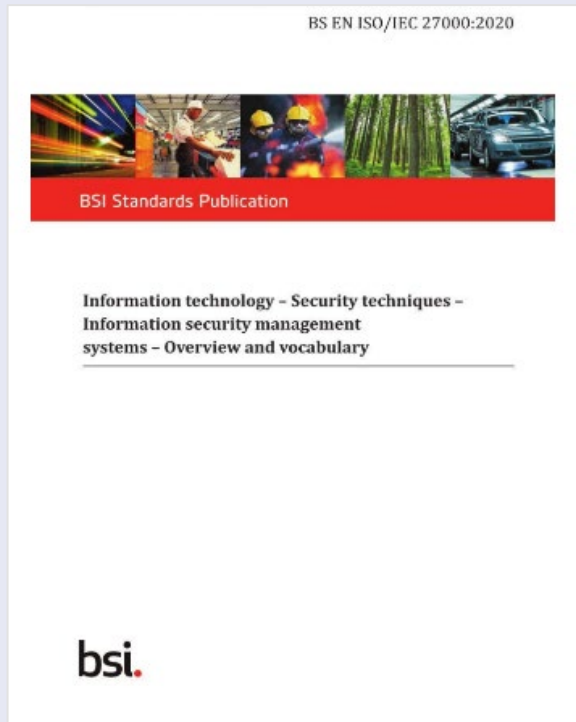
มาตรฐานการจัดการ
ของผู้ให้บริการ
Cloud Service





ISO/IEC 27001: 2022

ISO standards for information security management



The harmonized approach with ISMS additions



Example of Annex A

ISO/IEC 27001:2022(E)

Annex A (normative)

Information security controls reference

The information security controls listed in [Table A.1](#) are directly derived from and aligned with those listed in ISO/IEC 27002:2022^[4], Clauses 5 to 8, and shall be used in context with [6.1.3](#).

Table A.1 — Information security controls

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



CSA STAR

Cloud Security Alliance (CSA)
Security, Trust, Assurance and Risk (STAR)



Who is the Cloud Security Alliance?



STAR CERTIFICATION (ISO/IEC 27001)

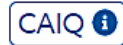
Acquia

Acquia offers enterprises unparalleled freedom to innovate and increase business agility by creating extraordinary web experiences. The fastest growing open clo...

Listed Since: 01/13/2013



Submissions:



Submissions:



[View Listing](#)

Acronis

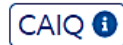
Acronis International GmbH

Acronis sets the standard for cyber protection through its innovative backup, anti-ransomware, disaster recovery, storage, and enterprise file sync and share so...

Listed Since: 05/06/2020



Submissions:



[View Listing](#)

Cloud Controls Matrix CCM V. 4

197 controls

Human resources	Application and interface security	Change control and configuration management	Datacenter security and privacy	Infrastructure and virtualization	Identity access management	Logging and monitoring
Business continuity management and operational resilience	Cryptography encryption and key management	Application and interface security	Governance, risk management and compliance	Interoperability and portability	Security incident management, e-discovery and cloud forensics	Supply chain management, transparency and accountability
		Universal endpoint management	Audit and Assurance	Threat and Vulnerability management		



ISO/IEC 27017



BS EN ISO/IEC 27002:2017
Incorporating corrigenda September 2014 and November 2015



BSI Standards Publication

**Information technology —
Security techniques —
Code of practice for
information security controls
(ISO/IEC 27002:2013)**

Licensed copy: Chitreyul Sawatprasert, BSI Global Assurance, Version 001

bsi.



CONTENTS

	<i>Page</i>
1 Scope.....	1
2 Normative references.....	1
2.1 Identical Recommendations International Standards.....	1
2.2 Additional References.....	1
3 Definitions and abbreviations.....	1
3.1 Terms defined elsewhere.....	1
3.2 Abbreviations.....	2
4 Cloud sector-specific concepts.....	2
4.1 Overview.....	2
4.2 Supplier relationships in cloud services.....	2
4.3 Relationships between cloud service customers and cloud service providers.....	3
4.4 Managing information security risks in cloud services.....	3
4.5 Structure of this standard.....	3
5 Information security policies.....	4
5.1 Management direction for information security.....	4
6 Organization of information security.....	5
6.1 Internal organization.....	5
6.2 Mobile devices and teleworking.....	6
7 Human resource security.....	6
7.1 Prior to employment.....	6
7.2 During employment.....	6
7.3 Termination and change of employment.....	7
8 Asset management.....	7
8.1 Responsibility for assets.....	7
8.2 Information classification.....	8
8.3 Media handling.....	8
9 Access control.....	8
9.1 Business requirements of access control.....	8
9.2 User access management.....	9
9.3 User responsibilities.....	10
9.4 System and application access control.....	10
10 Cryptography.....	11
10.1 Cryptographic controls.....	11
11 Physical and environmental security.....	12
11.1 Secure areas.....	12
11.2 Equipment.....	12
12 Operations security.....	13
12.1 Operational procedures and responsibilities.....	13
12.2 Protection from malware.....	14
12.3 Backup.....	14
12.4 Logging and monitoring.....	15
12.5 Control of operational software.....	16
12.6 Technical vulnerability management.....	16
12.7 Information systems audit considerations.....	17
13 Communications security.....	17
13.1 Network security management.....	17
13.2 Information transfer.....	17
14 System acquisition, development and maintenance.....	18
14.1 Security requirements of information systems.....	18
14.2 Security in development and support processes.....	18

	<i>Page</i>
14.3 Test data.....	19
15 Supplier relationships.....	19
15.1 Information security in supplier relationships.....	19
15.2 Supplier service delivery management.....	20
16 Information security incident management.....	20
16.1 Management of information security incidents and improvements.....	20
17 Information security aspects of business continuity management.....	22
17.1 Information security continuity.....	22
17.2 Redundancies.....	22
18 Compliance.....	22
18.1 Compliance with legal and contractual requirements.....	22
18.2 Information security reviews.....	23
Annex A – Cloud service extended control set.....	25
Annex B – References on information security risk related to cloud computing.....	29
Bibliography.....	30

6 Organization of information security

6.1 Internal organization

The objective specified in clause 6.1 of ISO/IEC 27002 applies.

6.1.1 Information security roles and responsibilities

Control 6.1.1 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
<p>The cloud service customer should agree with the cloud service provider on an appropriate allocation of information security roles and responsibilities, and confirm that it can fulfil its allocated roles and responsibilities. The information security roles and responsibilities of both parties should be stated in an agreement.</p> <p>The cloud service customer should identify and manage its relationship with the customer support and care function of the cloud service provider.</p>	<p>The cloud service provider should agree and document an appropriate allocation of information security roles and responsibilities with its cloud service customers, its cloud service providers, and its suppliers.</p>

Other information for cloud services

Even when responsibilities are determined within and between the parties, the cloud service customer is accountable for the decision to use the service. That decision should be made according to the roles and responsibilities determined within the cloud service customer's organization. The cloud service provider is accountable for the information security stated as part of the cloud service agreement. The information security implementation and provisioning should be made according to the roles and responsibilities determined within the cloud service provider's organization.

Ambiguity in roles and in the definition and allocation of responsibilities related to issues such as data ownership, access control, and infrastructure maintenance, can give rise to business or legal disputes, especially when dealing with third parties.

Data and files on the cloud service provider's systems that are created or modified during the use of the cloud service can be critical to the secure operation, recovery and continuity of the service. The ownership of all assets, and the parties who have responsibilities for operations associated with these assets, such as backup and recovery operations, should be defined and documented. Otherwise, there is a risk that the cloud service provider assumes that the cloud service customer performs these vital tasks (or vice versa), and a loss of data can occur.

6.1.2 Segregation of duties

Control 6.1.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.



ISO/IEC 27018



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**

bsi.



Contents	Page
Foreword	vi
Introduction	vii
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Overview	3
4.1 Structure of this document	3
4.2 Control categories	4
5 Information security policies	4
5.1 Management direction for information security	4
5.1.1 Policies for information security	4
5.1.2 Review of the policies for information security	5
6 Organization of information security	5
6.1 Internal organization	5
6.1.1 Information security roles and responsibilities	5
6.1.2 Segregation of duties	5
6.1.3 Contact with authorities	5
6.1.4 Contact with special interest groups	5
6.1.5 Information security in project management	5
6.2 Mobile devices and teleworking	5
7 Human resource security	5
7.1 Prior to employment	5
7.2 During employment	5
7.2.1 Management responsibilities	6
7.2.2 Information security awareness, education and training	6
7.2.3 Disciplinary process	6
7.3 Termination and change of employment	6
8 Asset management	6
9 Access control	6
9.1 Business requirements of access control	6
9.2 User access management	6
9.2.1 User registration and de-registration	7
9.2.2 User access provisioning	7
9.2.3 Management of privileged access rights	7
9.2.4 Management of secret authentication information of users	7
9.2.5 Review of user access rights	7
9.2.6 Removal or adjustment of access rights	7
9.3 User responsibilities	7
9.3.1 Use of secret authentication information	7
9.4 System and application access control	7
9.4.1 Information access restriction	7
9.4.2 Secure log-on procedures	8
9.4.3 Password management system	8
9.4.4 Use of privileged utility programs	8
9.4.5 Access control to program source code	8
10 Cryptography	8
10.1 Cryptographic controls	8
10.1.1 Policy on the use of cryptographic controls	8
10.1.2 Key management	8
11 Physical and environmental security	8

11.1 Secure areas	8
11.2 Equipment	9
11.2.1 Equipment siting and protection	9
11.2.2 Supporting utilities	9
11.2.3 Cabling security	9
11.2.4 Equipment maintenance	9
11.2.5 Removal of assets	9
11.2.6 Security of equipment and assets off-premises	9
11.2.7 Secure disposal or re-use of equipment	9
11.2.8 Unattended user equipment	9
11.2.9 Clear desk and clear screen policy	9
12 Operations security	9
12.1 Operational procedures and responsibilities	9
12.1.1 Documented operating procedures	10
12.1.2 Change management	10
12.1.3 Capacity management	10
12.1.4 Separation of development, testing and operational environments	10
12.2 Protection from malware	10
12.3 Backup	10
12.3.1 Information backup	10
12.4 Logging and monitoring	11
12.4.1 Event logging	11
12.4.2 Protection of log information	11
12.4.3 Administrator and operator logs	11
12.4.4 Clock synchronization	12
12.5 Control of operational software	12
12.6 Technical vulnerability management	12
12.7 Information systems audit considerations	12
13 Communications security	12
13.1 Network security management	12
13.2 Information transfer	12
13.2.1 Information transfer policies and procedures	12
13.2.2 Agreements on information transfer	12
13.2.3 Electronic messaging	12
13.2.4 Confidentiality or non-disclosure agreements	12
14 System acquisition, development and maintenance	13
15 Supplier relationships	13
16 Information security incident management	13
16.1 Management of information security incidents and improvements	13
16.1.1 Responsibilities and procedures	13
16.1.2 Reporting information security events	13
16.1.3 Reporting information security weaknesses	13
16.1.4 Assessment of and decision on information security events	13
16.1.5 Response to information security incidents	14
16.1.6 Learning from information security incidents	14
16.1.7 Collection of evidence	14
17 Information security aspects of business continuity management	14
18 Compliance	14
18.1 Compliance with legal and contractual requirements	14
18.2 Information security reviews	14
18.2.1 Independent review of information security	14
18.2.2 Compliance with security policies and standards	14
18.2.3 Technical compliance review	14
Annex A (normative) Public cloud PII processor extended control set for PII protection	15

Bibliography	23
---------------------	-----------



ISO/IEC 27701



“

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

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



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

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

[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

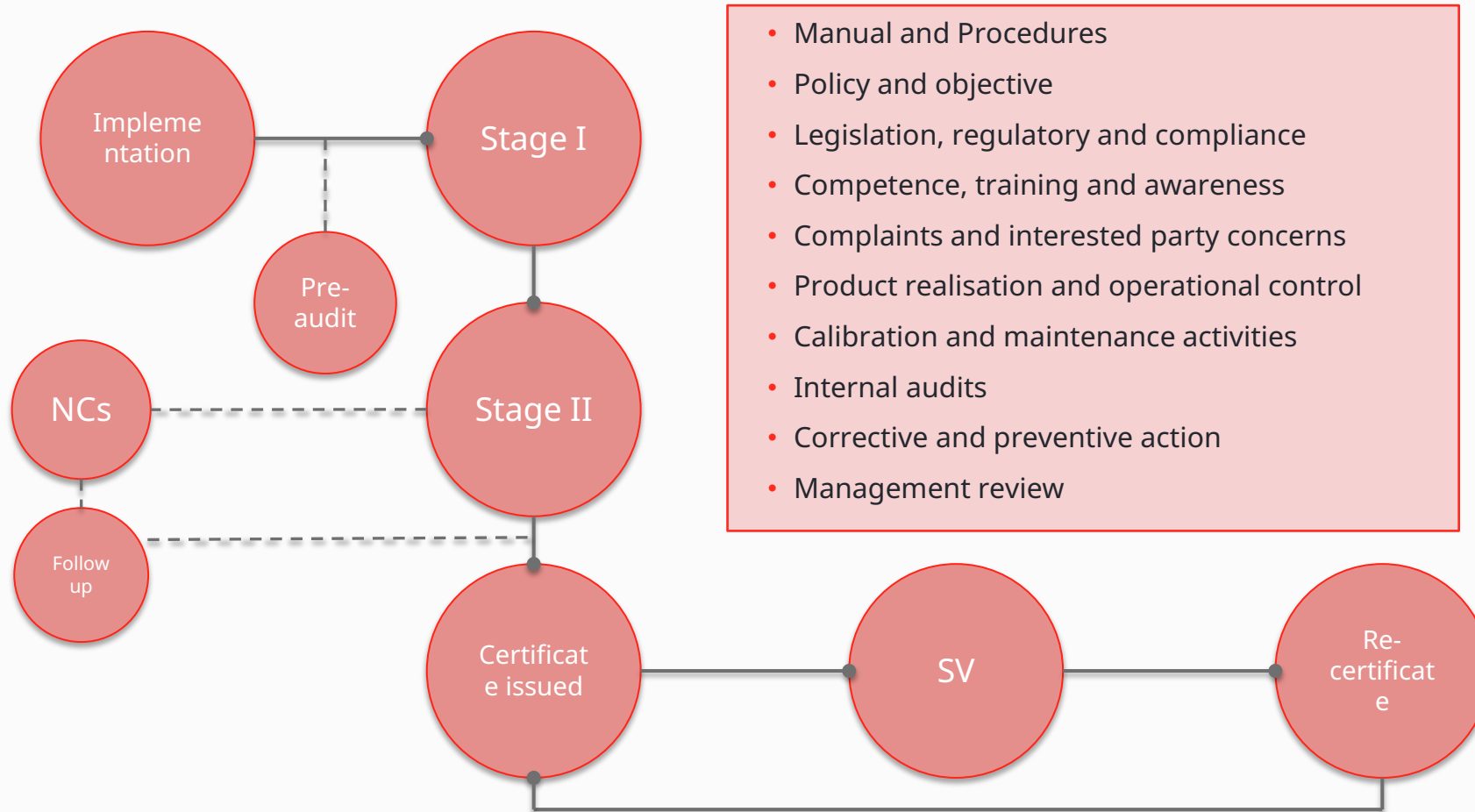
Annex	Detail
Annex A (informative)	PIMS-specific reference control objectives and controls (PII Controllers)
Annex B (normative)	PIMS-specific reference control objectives and controls (PII Processors)
Annex C (informative)	Mapping to ISO/IEC 29100 Table C.1 — Mapping of controls for PII controllers 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



การขอการรับรอง



Approval Process



" Q&A

ทบทวนและถามคำถาม



สแกน QR code เป็นเพื่อนกับเราใน Line official ของ BSI
เพื่อไม่ให้พลาดข่าวสารข้อมูลที่เป็นประโยชน์ในสายอาชีพของท่าน

- Free webinars
- Tool และบทความดีๆ

