BSI Webinar

ยกระดับ Data center ด้วยมาตรฐาน ISO27001:2022

สถาบันมาตรฐานอังกฤษ

วนา ตรีวัชรานนท์

ตำแหน่งปัจจุบัน
BSI client manager

ประสบการณ์
- ISO Auditor for CB
- Internal auditor in Bank firm
- IT security specialist in IT solution service
- Quality assurance supervisor in IT service and Manufacturing

TOPIC

1 ความมั่นคงปลอดภัยของ Data center เป็นส่วนหนึ่งของความมั่นคงปลอดภัยของข้อมูลได้อย่างไร

2 ISO27001:2022 ช่วยให้ Data center มีความมั่นคงปลอดภัยได้อย่างไร

3 การประยุกต์ใช้มาตรการควบคุมตาม ISO27001:2022 สำหรับ Data center

4 บทสรุปการดำเนินการรักษาความมั่นคงปลอดภัยของ Data center อย่างต่อเนื่อง

ความมั่นคงปลอดภัยของ Data center เป็นส่วนหนึ่งของความมั่นคงปลอดภัยของข้อมูลได้อย่างไร??

Information: Confidential / Integrity / Availability

Information that is not intend to be made integrity, available or disclosed to unauthorized individuals, entities or processes

Information can be in any media

Information system

Set of application, services, information technology assets, or other information-handling

Information processing facility

Any information processing system, service or infrastructure, or the physical location housing it.

Asset

Anything that has value to the organization

- Primary assets: Information and business processes and activities.
- Supporting assets (on which the primary assets relay) of all types, Ex. Hardware, software, network, personnel

Information life cycle

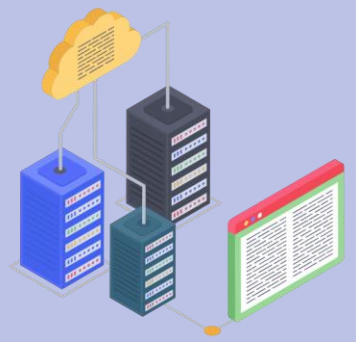
Creation/ Collection

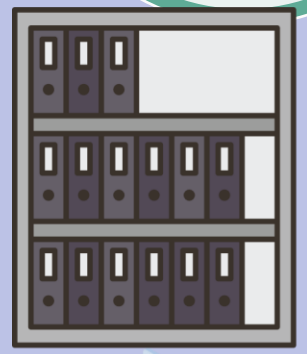
Storage

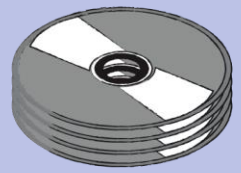
Processing

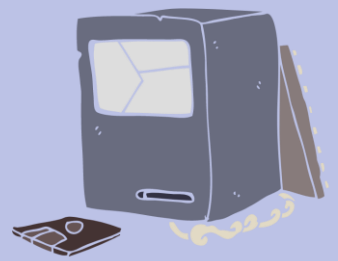
Usage/ sharing

Disposal









Information Owner

- Physical Access record/log
- System Access record/log
- Asset movement record
- Authentication information
- CCTV record
- Monitoring record/log
- Cabling layout
- Electric diagram
- Client contact list
- Client contract
- Operation/Change record
- Configuration of Facility system
- Etc.

Information Custodian

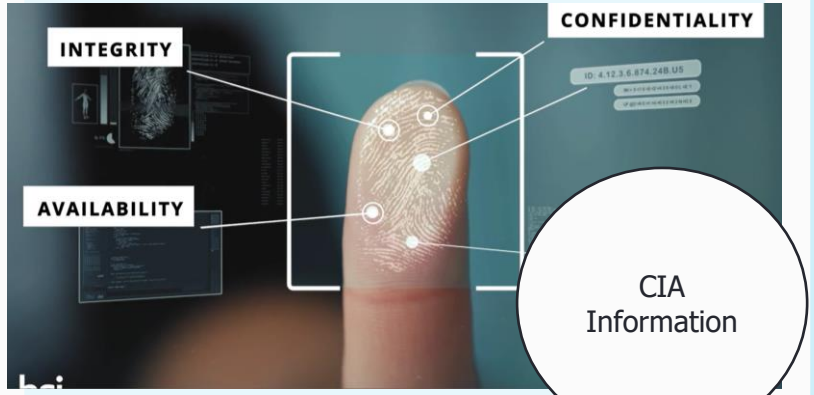
- Client's storage media
- Server/Database/Network: data, log, configuration.
- Back up tape
- Etc.

Information in Data Center

ISO27001:2022 ช่วยให้ Data center มีความมั่นคงปลอดภัยได้อย่างไร

ISO27001 help organizations manage and protect information, reducing the risk of data breaches, cyber-attacks, and other security incidents. It also helps organizations comply with legal and regulatory requirements related to information security.

3 principles of ISMS



It’s a valuable tool for organizations seeking to enhance their information security posture and demonstrate their commitment to protecting information security posture and demonstrate the commitment to protecting information

Risk from Threat / Vulnerability

What is ISO/IEC 27001:2022 Information security management system or ISMS?

- Globally recognized standard for information security management.
- The standard provides a systematic and structured approach to managing and protecting information within an organization.
- The ISMS is a set of policies, procedures and control that govern how an organization manages its information security risk
- The standard is designed to be flexible and can be applied to all types of organization of any size, from small business to multinational corporations


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

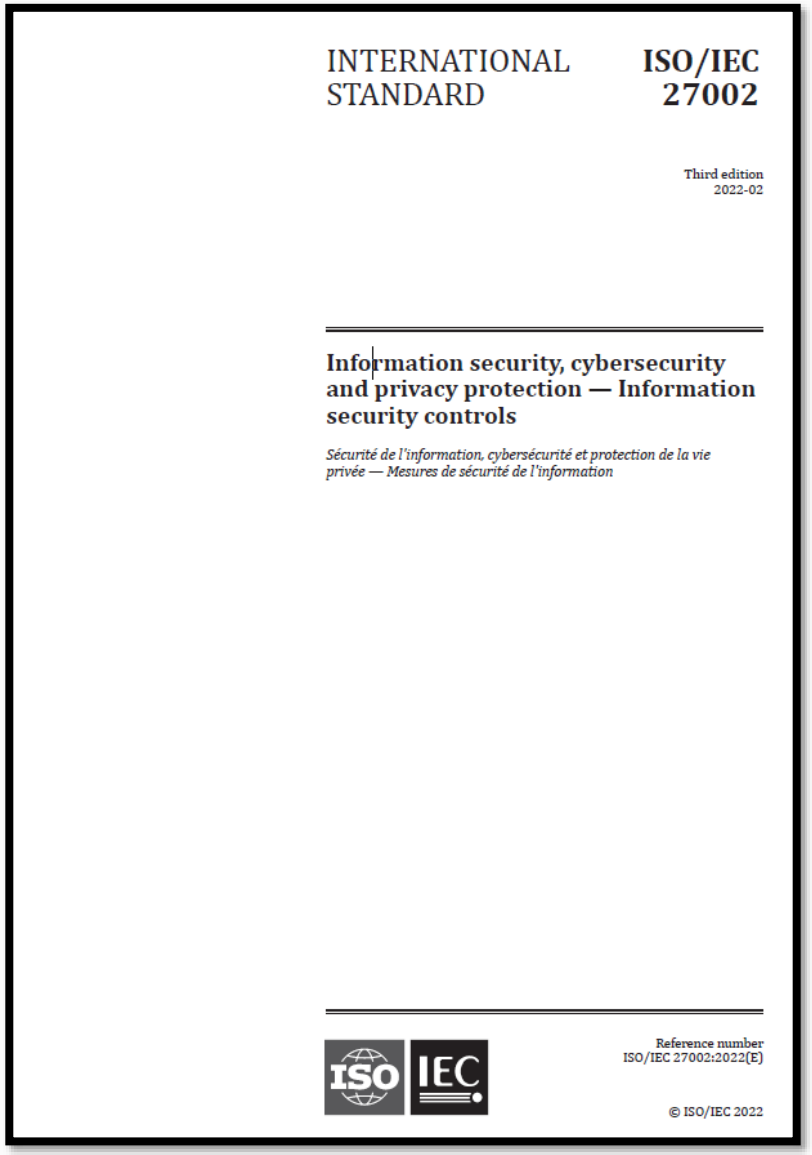
ISO IEC

Reference number
ISO/IEC 27001:2022(E)

© ISO/IEC 2022

ISO/IEC 27002 Information security controls

- It is to be used as a reference for determining and implementing controls for information security risk treatment in an information security management system (ISMS) based on ISO/IEC 27001. It can also be used as a guidance document for organizations determining and implementing commonly accepted information security controls. Furthermore, this document is intended for use in developing industry and organization-specific information security management guidelines, taking into consideration their specific information security risk environment(s). Organizational or environment-specific controls other than those included in this document can be determined through risk assessment as necessary.
- Organizations of all types and sizes (including public and private sector, commercial and non-profit) create, collect, process, store, transmit and dispose of information in many forms, including electronic, physical and verbal (e.g. conversations and presentations).


INTERNATIONAL STANDARD

ISO/IEC 27002

Third edition
2022-02

Information security, cybersecurity and privacy protection — Information security controls

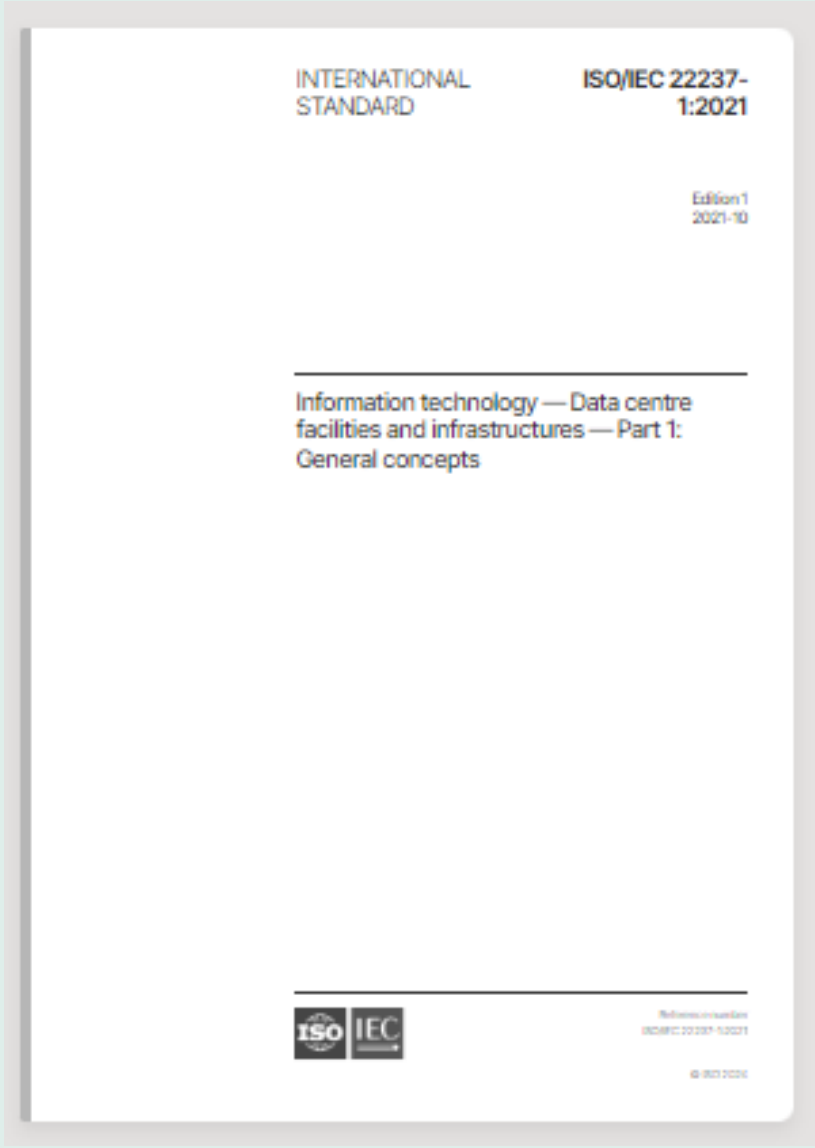
Sécurité de l'information, cybersécurité et protection de la vie privée — Mesures de sécurité de l'information

ISO IEC

Reference number
ISO/IEC 27002:2022(E)

ISO/IEC 22237: Data centre facilities and infrastructures

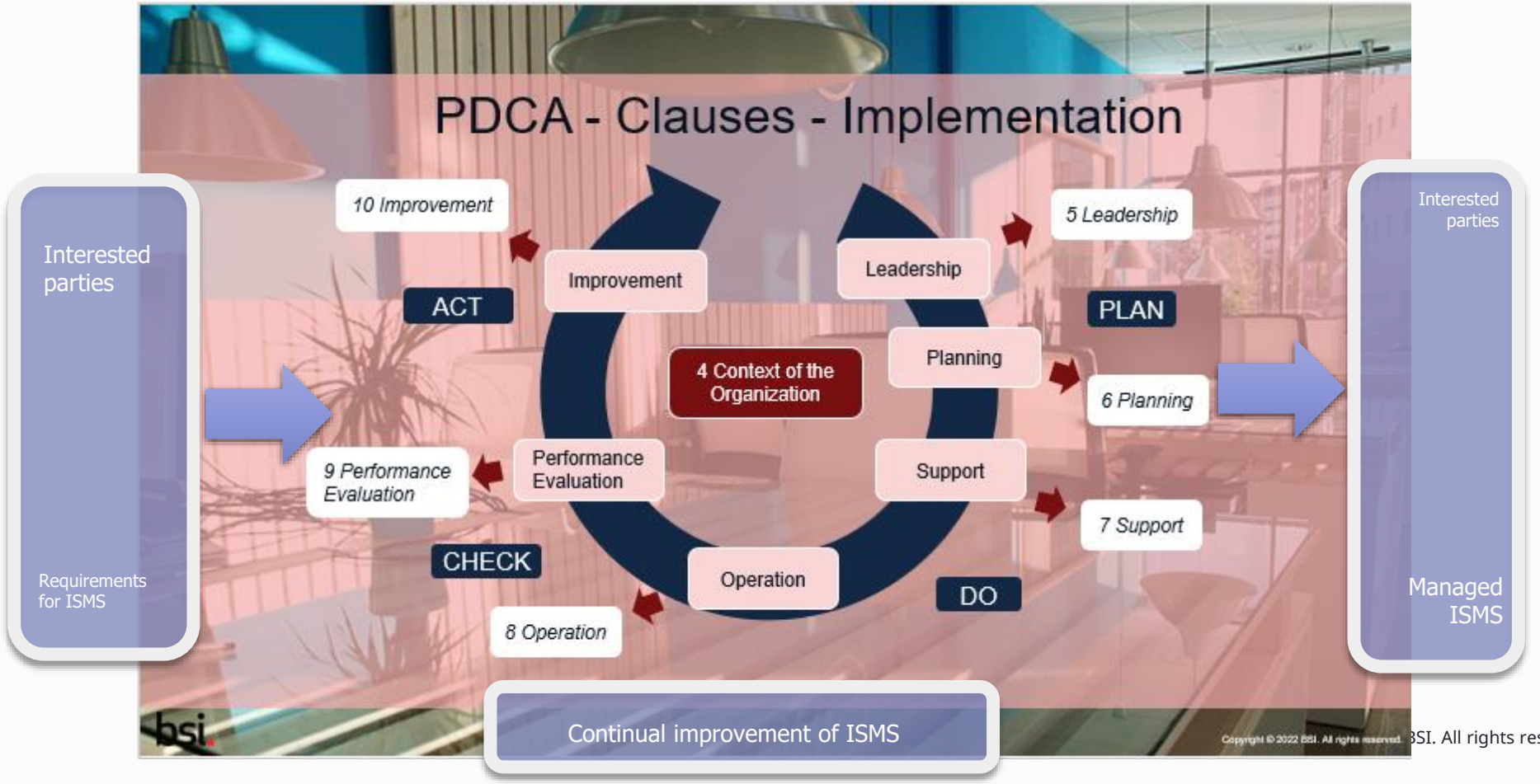
- https://www.iso.org/search.html?PROD_isoorg_en%5Bquery%5D=22237



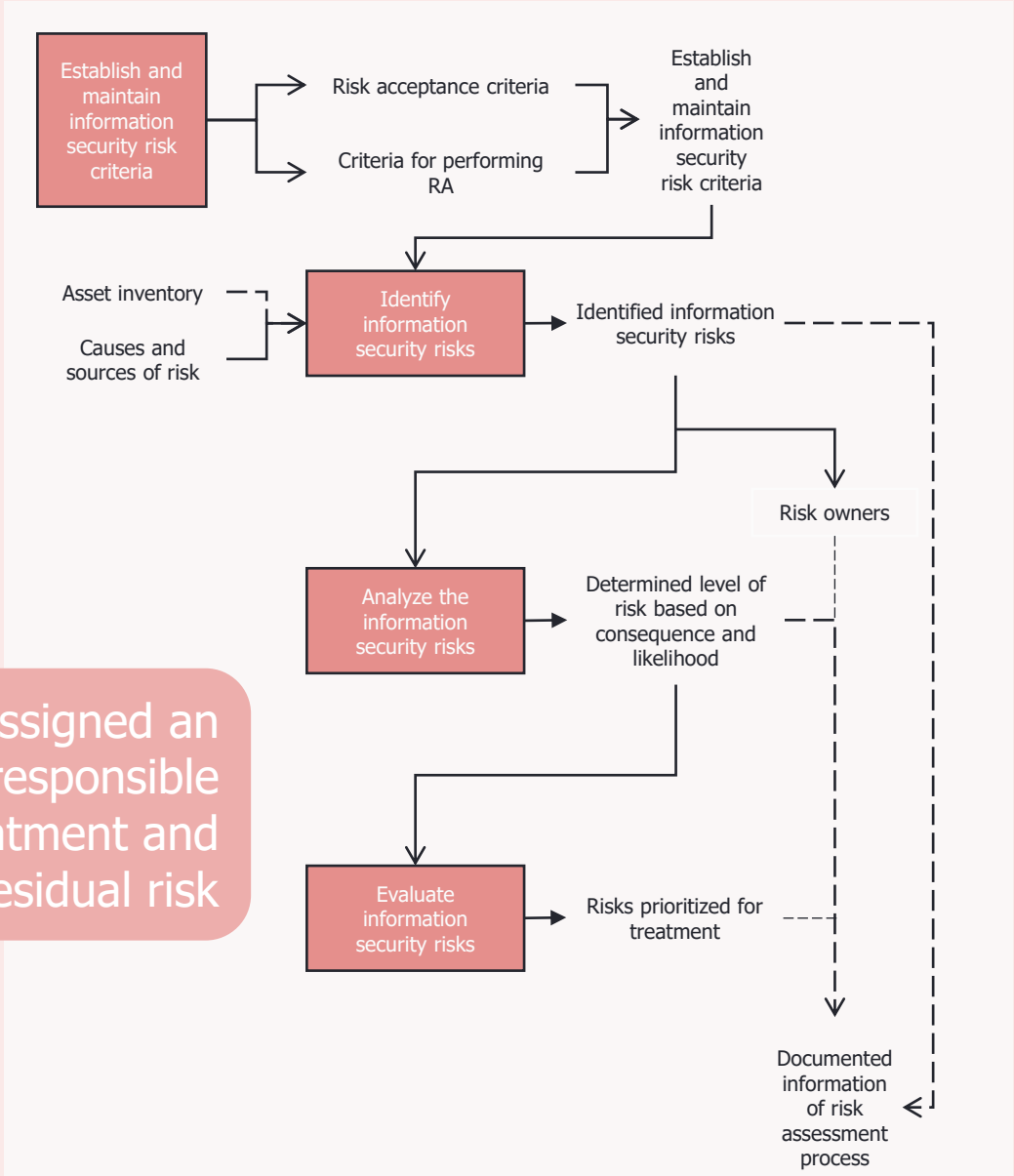
การประยุกต์ใช้มาตรการควบคุมตาม ISO27001:2022 สำหรับ Data center

PDCA and ISMS

- ISO/IEC 27001 is based on the plan-do-check-action (P-D-C-A cycle) and requires organizations to implement a comprehensive set of policies, procedures and controls to manage information security risks and ensures the confidentiality, integrity and availability of information.



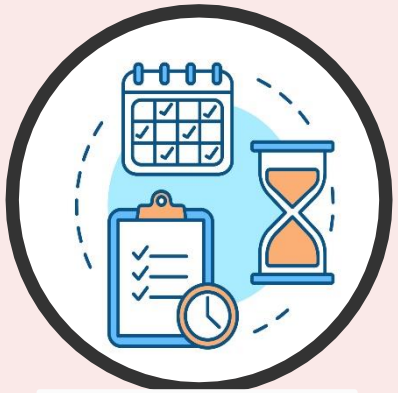
Clause 6.1.2 Information security risk assessment



Likelihood					
	Almost certain (4)	M	H	H	H
	Likely (3)	M	M	H	H
	Possible (2)	L	M	M	H
	Rare (1)	L	L	M	H
		Minor (1)	Moderate (2)	Major (3)	Extreme (4)
		Consequence			

Clause 8.2

Information security risk assessment

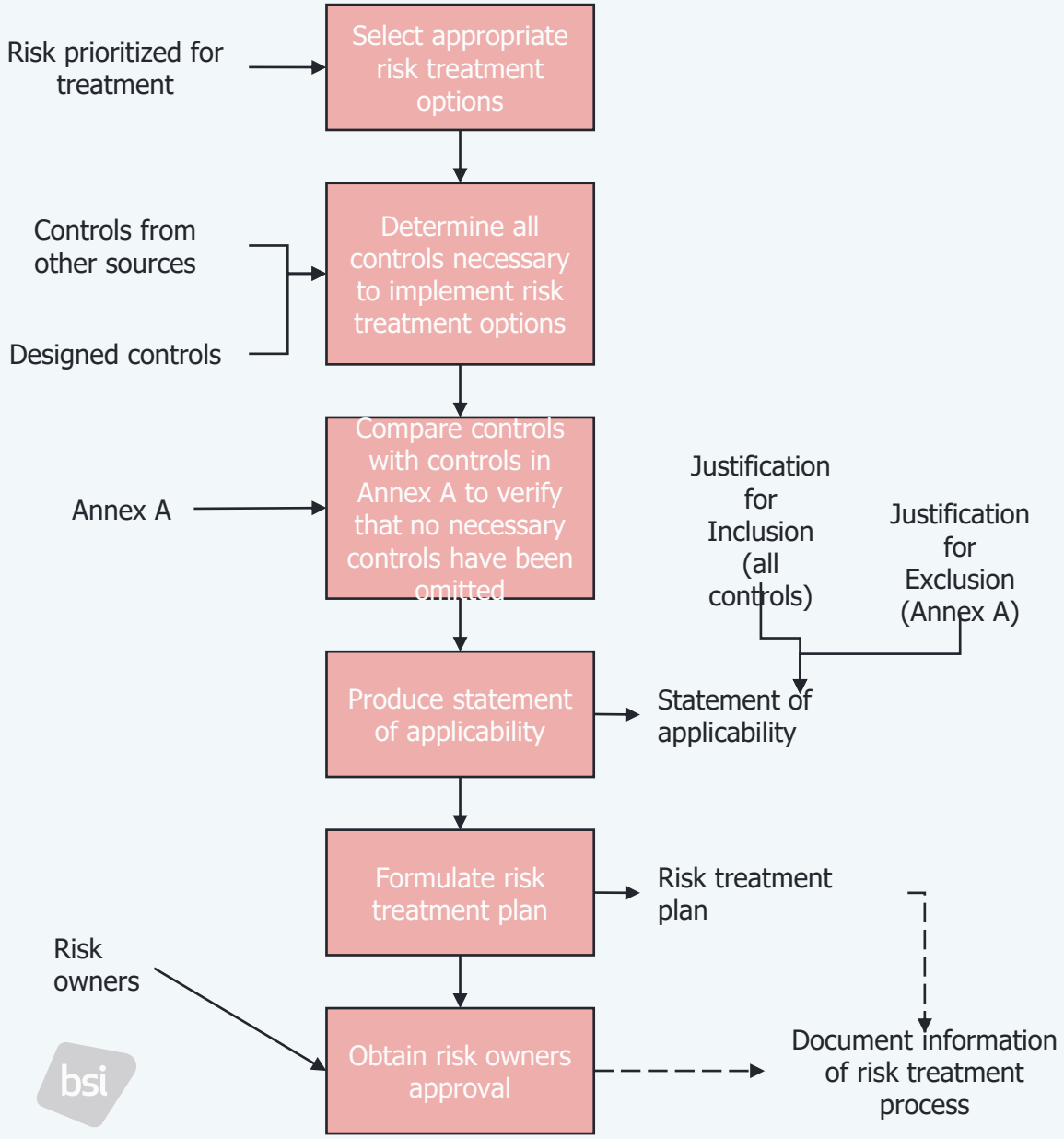


Scheduled

Changes/incidents

Each risk should be assigned an owner, who will be responsible for agreeing risk treatment and residual risk

Clause 6.1.3: Risk Treatment



Statement of Applicability

Risk Treatment Options

- Reduce/Treat
- Avoid/Terminate
- Accept/Tolerate
- Transfer/Share

Risk treatment plan

- Actions
- Target dates
- Review dates
- Responsibilities

Clause 8.3 - Information security risk treatment

ISO/IEC 27002:2022

- 4 security clause
- 93 controls

Annex A.5 - Organizational controls
37 controls

Annex A.6 - People controls
8 controls

Annex A.7 - Physical controls
14 controls

Annex A.8 - Technological controls
34 controls

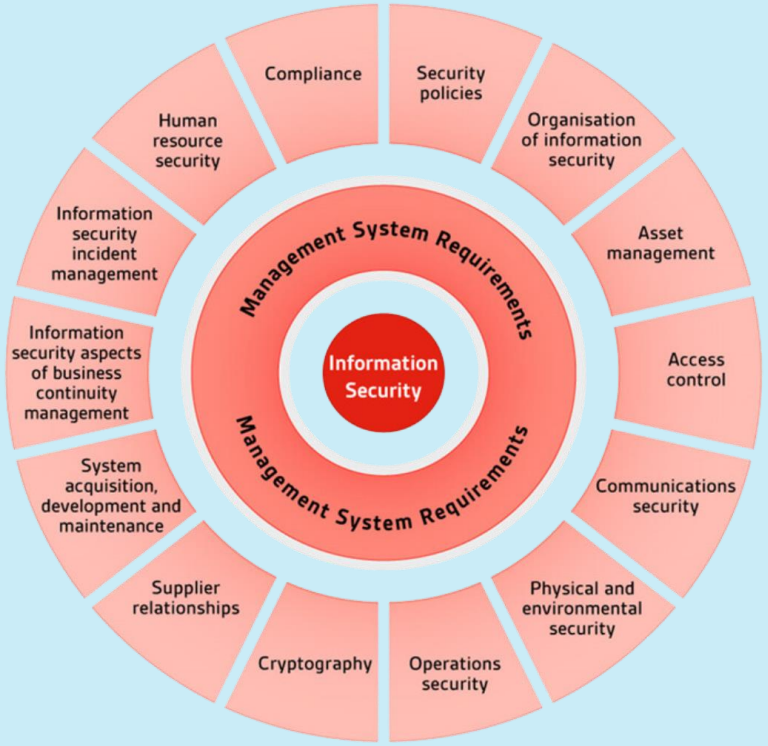
Statement of Applicability (ISO/IEC 27001:2022)

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

ISO/IEC 27001:2022 (Annex A)	ISO/IEC 27001:2013 (Annex A)	Control name	Applicable (Y/N)	Justification for inclusion or excluding	Process applicable	Related documented information
5.1	A.5.1.1, A.5.1.2	Policies for information security	Y	LR, CO, RRA	Management process	BSI-PL-001 (Information security, cybersecurity, and privacy protection)
5.2	A.6.1.1	Information security roles and responsibilities	Y	LR, CO, RRA	HR process	BSI-HR-001 (Recruitment procedure)
5.3	A.6.1.2	Segregation of duties	Y	LR, CO, RRA	HR process	BSI-HR-001 (Recruitment procedure)
5.4	A.7.2.1	Management responsibilities				
5.5	A.6.1.3	Contact with authorities				
5.6	A.6.1.4	Contact with special interest groups				
5.7	New	Threat intelligence				
5.8	A.6.1.5, A.14.1.1	Information security in project management				
5.9	A.8.1.1, A.8.1.2	Inventory of information and other associated assets				
5.10	A.8.1.3, A.8.2.3	Acceptable use of information and other associated assets				
5.11	A.8.1.4	Return of assets				
5.12	A.8.2.1	Classification of information				
5.13	A.8.2.2	Labelling of information				
5.14	A.13.2.1, A.13.2.2, A.13.2.3	Information transfer				
5.15	A.9.1.1, A.9.1.2	Access control				

ISO/IEC 27002:2013

- 14 security clause
- 35 security categories
- 114 controls



Clause 8: Operation

Clause 8.1

- Implementation of the actions determined in Clause 6
- Planning, implementation and control of the processes needed to meet information security requirements and achieve information security objectives

Managed

Reviewed

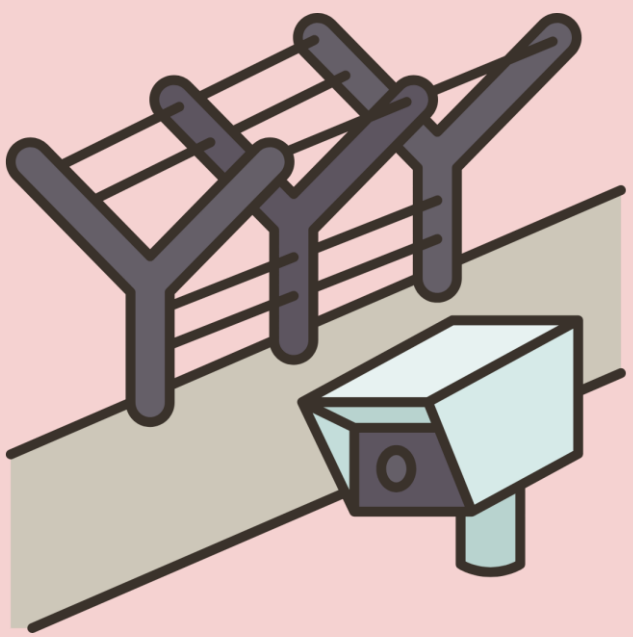
Monitored

Annex A: 7 Physical control

7.1 Physical Security perimeters

Control: Security perimeters should be defined and used to protect areas that contain information and other associated assets.

Purpose: To prevent unauthorized physical access, damage and interference to the organization's information and other associated assets.



Annex A: 7 Physical control

7.2 Physical entry

Control: Secure areas should be protected by appropriate entry controls and access points.
Purpose: To ensure only authorized physical access to the organization’s information and other associated assets occurs.

- Physical logbook or electronic audit trail of all access
- Authentication of access door system
- Area monitoring by personnel
- Wearing visible identification of visitor, staff, vendor
- Exit door, loading area

Annex A: 7 Physical control

7.3 Securing offices, room and facilities

Control: Physical security for offices, rooms and facilities should be designed and implemented.

Purpose: To prevent unauthorized physical access, damage and interference to the organization's information and other associated assets in offices, rooms and facilities.

- Avoid access by the public
- No making directories, internal tel. book and online accessible maps

Annex A: 7 Physical control

7.4 Physical security monitoring

Control: Premises should be continuously monitored for unauthorized physical access.

Purpose: To detect and deter unauthorized physical access.

- CCTV
- Motion detection
- Sensor
- Alarm of accessible windows

Annex A: 7 Physical control

7.5 Protecting against physical and environmental threats

Control: Protection against physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to infrastructure should be designed and implemented.

Purpose: To prevent or reduce the consequences of events originating from physical and environmental threats.

- Fire
- Flooding
- Electrical Surges
- Explosive and weapon

Annex A: 7 Physical control

7.6 Working in secure areas

Control: Security measures for working in secure areas should be designed and implemented.

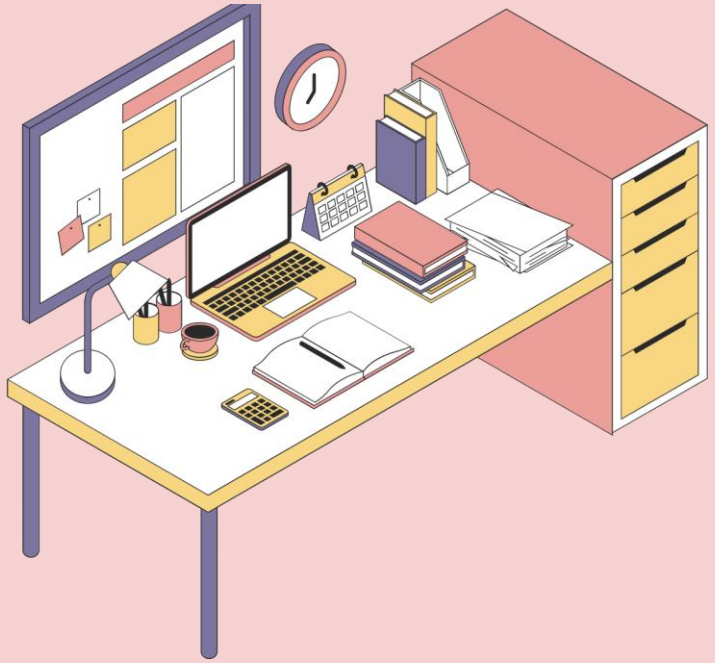
Purpose: To protect information and other associated assets in secure areas from damage and unauthorized interference by personnel working in these areas.

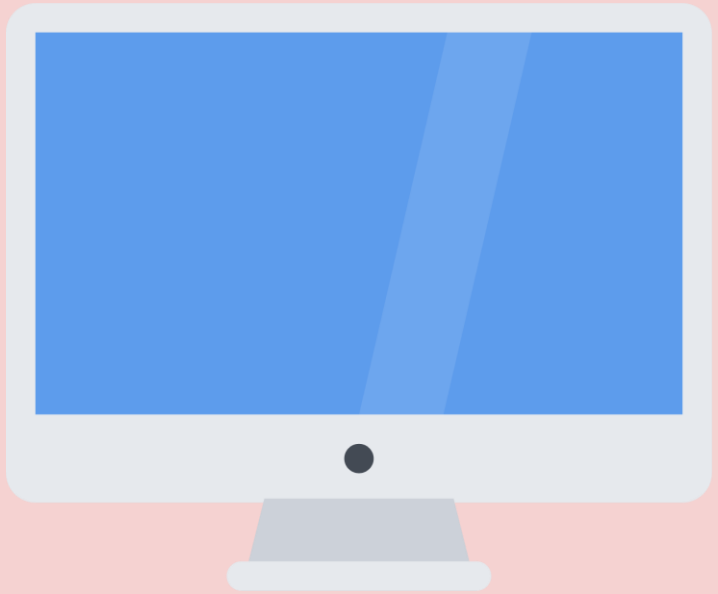
Annex A: 7 Physical control

7.7 Clear desk and clear screen

Control: Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities should be defined and appropriately enforced.

Purpose: To reduce the risks of unauthorized access, loss of and damage to information on desks, screens and in other accessible locations during and outside normal working hours.





Annex A: 7 Physical control

7.8 Equipment siting and protection

Control: Equipment should be sited securely and protected.

Purpose: To reduce the risks from physical and environmental threats, and from unauthorized access and damage.

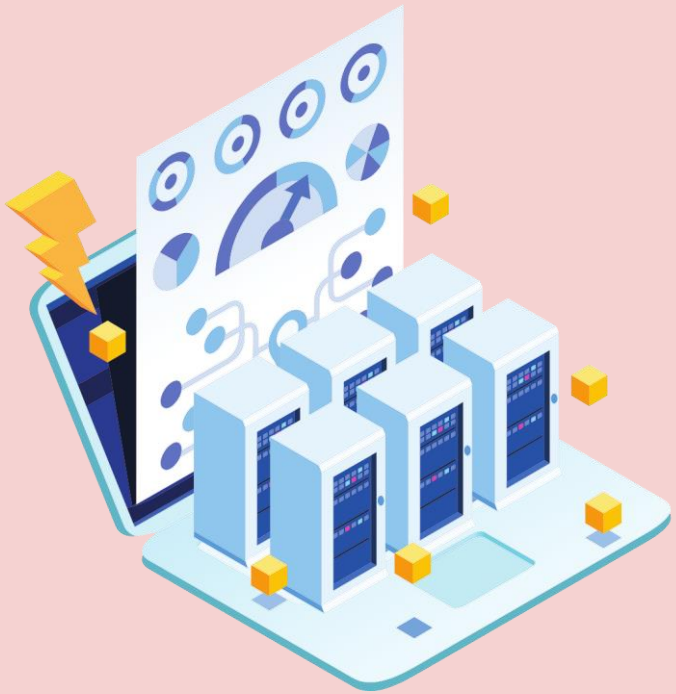
- Applying lightning protection
- Physical separating from other organization

Annex A: 7 Physical control

7.9 Security of asset off-premises

Control: Off-site assets should be protected.

Purpose: To prevent loss, damage, theft or compromise of off-site devices and interruption to the organization’s operations.



- Not leaving it unattended in unsecured places
- Protecting it all time from water, heat, humidity and dust etc.
- Record of authorization for removed asset.

Annex A: 7 Physical control

7.10 Storage media

Control: Storage media should be managed through their life cycle of acquisition, use, transportation and disposal in accordance with the organization’s classification scheme and handling requirements.

Purpose: To ensure only authorized disclosure, modification, removal or destruction of information on storage media.

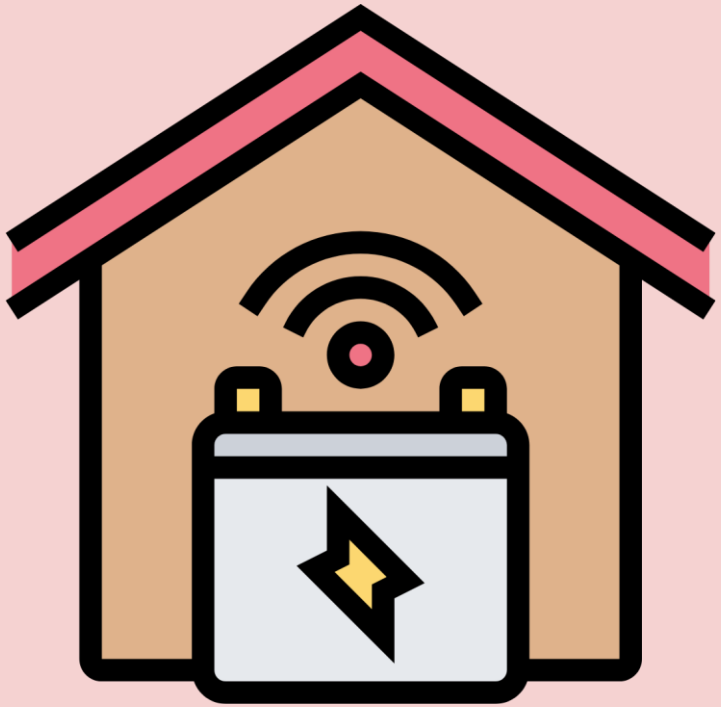
- Information can be vulnerable to unauthorized access, misuse or corruption during physical transport, for instance when sending storage media via the postal service or via courier.
- Secure reuse or disposal

Annex A: 7 Physical control

7.11 Supporting utilities

Control: Information processing facilities should be protected from power failures and other disruptions caused by failures in supporting utilities.

Purpose: To prevent loss, damage or compromise of information and other associated assets, or interruption to the organization’s operations due to failure and disruption of supporting utilities.



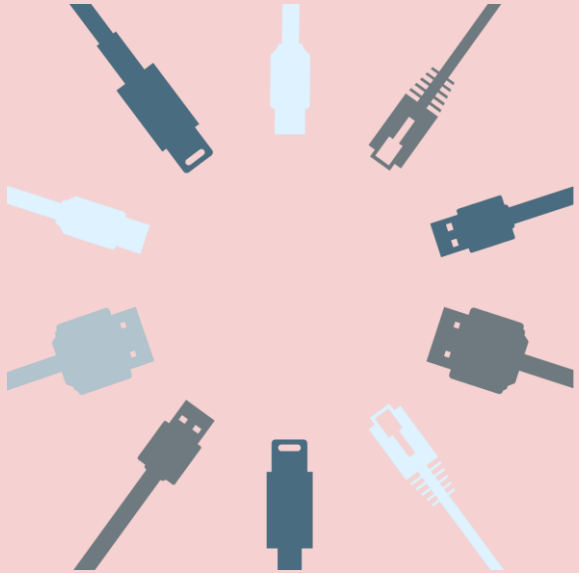
- Configuration, operation and maintain

Annex A: 7 Physical control

7.12 Cabling security

Control: Cables carrying power, data or supporting information services should be protected from interception, interference or damage.

Purpose: To prevent loss, damage, theft or compromise of information and other associated assets and interruption to the organization’s operations related to power and communications cabling.



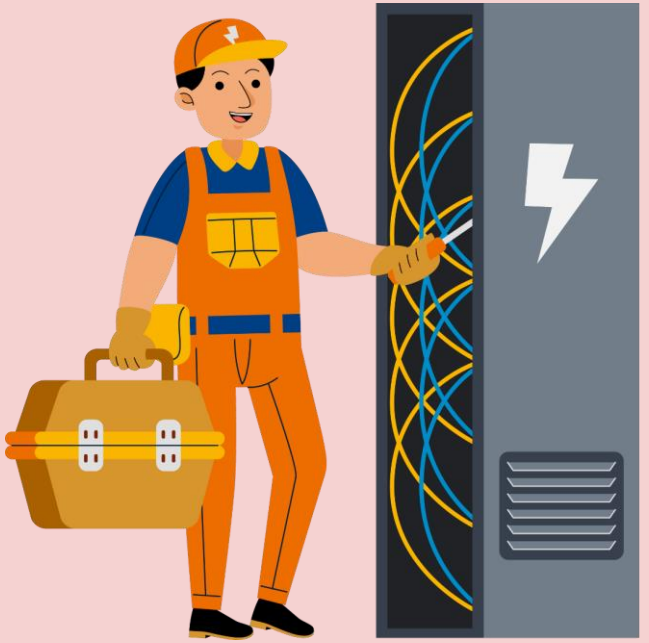
- Segregating power cable from communication cable
- Underground cable protecting from accidental cut.
- Access control for patch panels and cable room

Annex A: 7 Physical control

7.13 Equipment maintenance

Control: Equipment should be maintained correctly to ensure availability, integrity and confidentiality of information.

Purpose: To prevent loss, damage, theft or compromise of information and other associated assets and interruption to the organization’s operations caused by lack of maintenance.



Annex A: 7 Physical control

7.14 Secure disposal or re-use of equipment

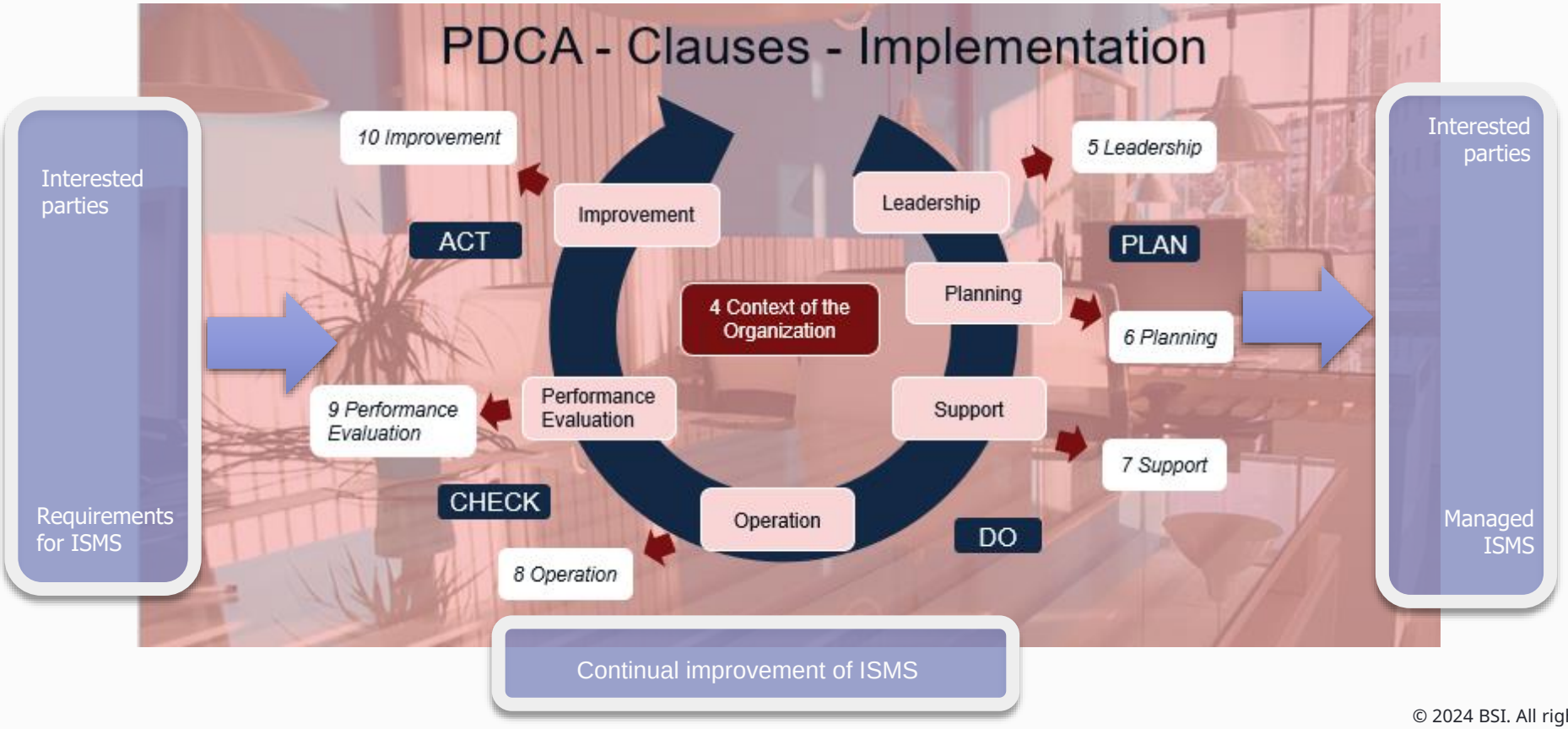
Control: Items of equipment containing storage media should be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.

Purpose: To prevent leakage of information from equipment to be disposed or re-used.

- Return the facility to original condition
- Ability to reuse the control at next facility
- Not leaving sensitive data

PDCA and ISMS

- ISO/IEC 27001 is based on the plan-do-check-action (P-D-C-A cycle) and requires organizations to implement a comprehensive set of policies, procedures and controls to manage information security risks and ensures the confidentiality, integrity and availability of information.



Clause 9: Performance Evaluation

9.1 Monitoring, measurement, analysis and evaluation

Determine what needs to be monitored and measured

Determine the methods for monitoring, measuring, analysis and evaluation

Clause 9: Performance evaluation (9.2)

9.2. Internal audit

Required at planned intervals

Provides conformance information

Assess the effective implementation and maintenance of the ISMS

Management Review (9.3)

General 9.3.1
Management review inputs (9.3.2)
Management review results (9.3.3)

What has been achieved?

- Audits - Internal - External
- Actions Outstanding
- Objectives and Targets
- New Technologies
- Operational Control
- Legal Compliance
- Policy
- Training Needs
- ISMS Performance
- Feedback
- Risk management
- Corrective actions
- Opportunities for continual improvement

What needs to change?

Improvement action plan

Clause 10: Improvement

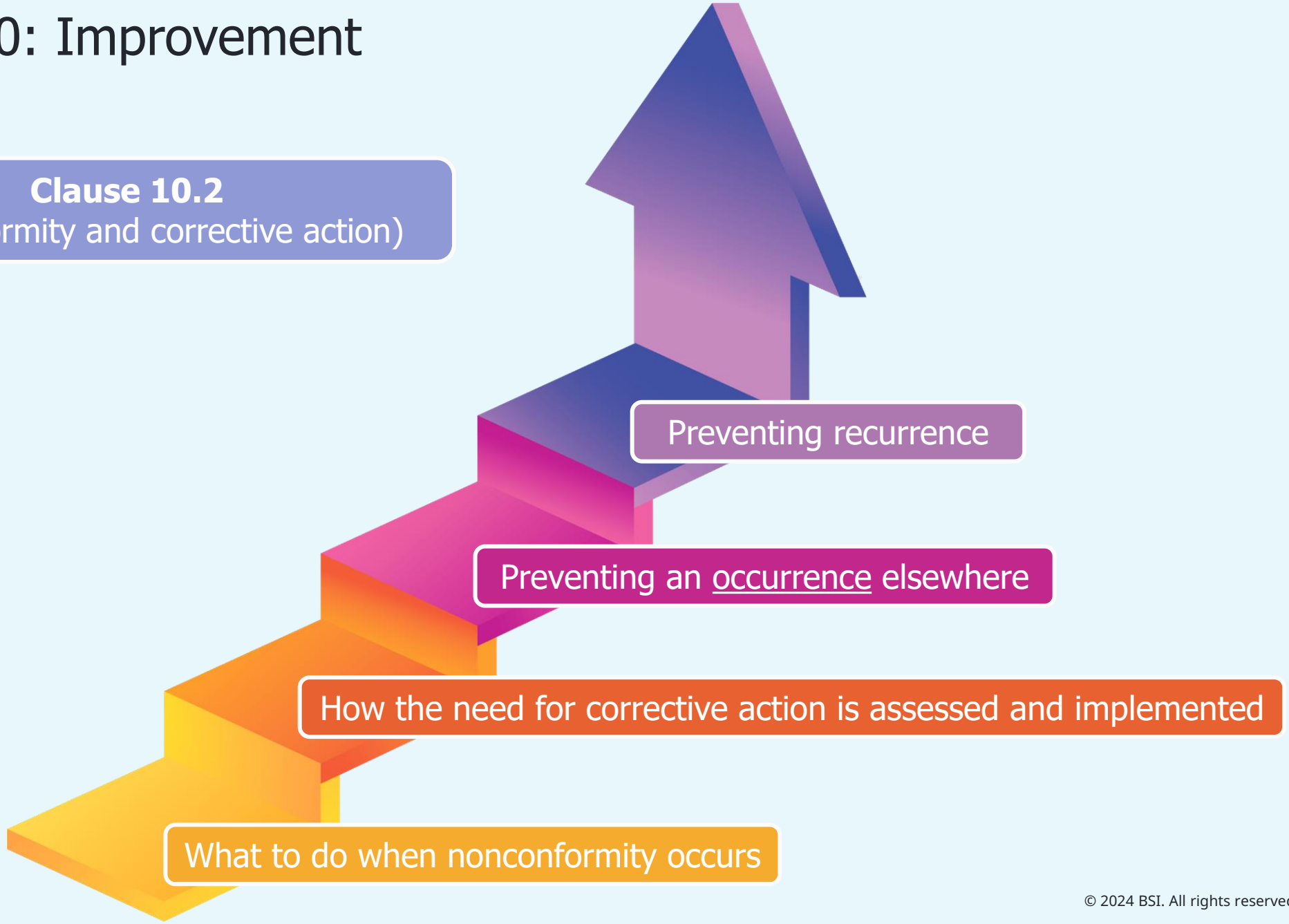
Clause 10.1 (Continual improvement)

Enhance performance of the ISMS

Through its suitability, adequacy and effectiveness

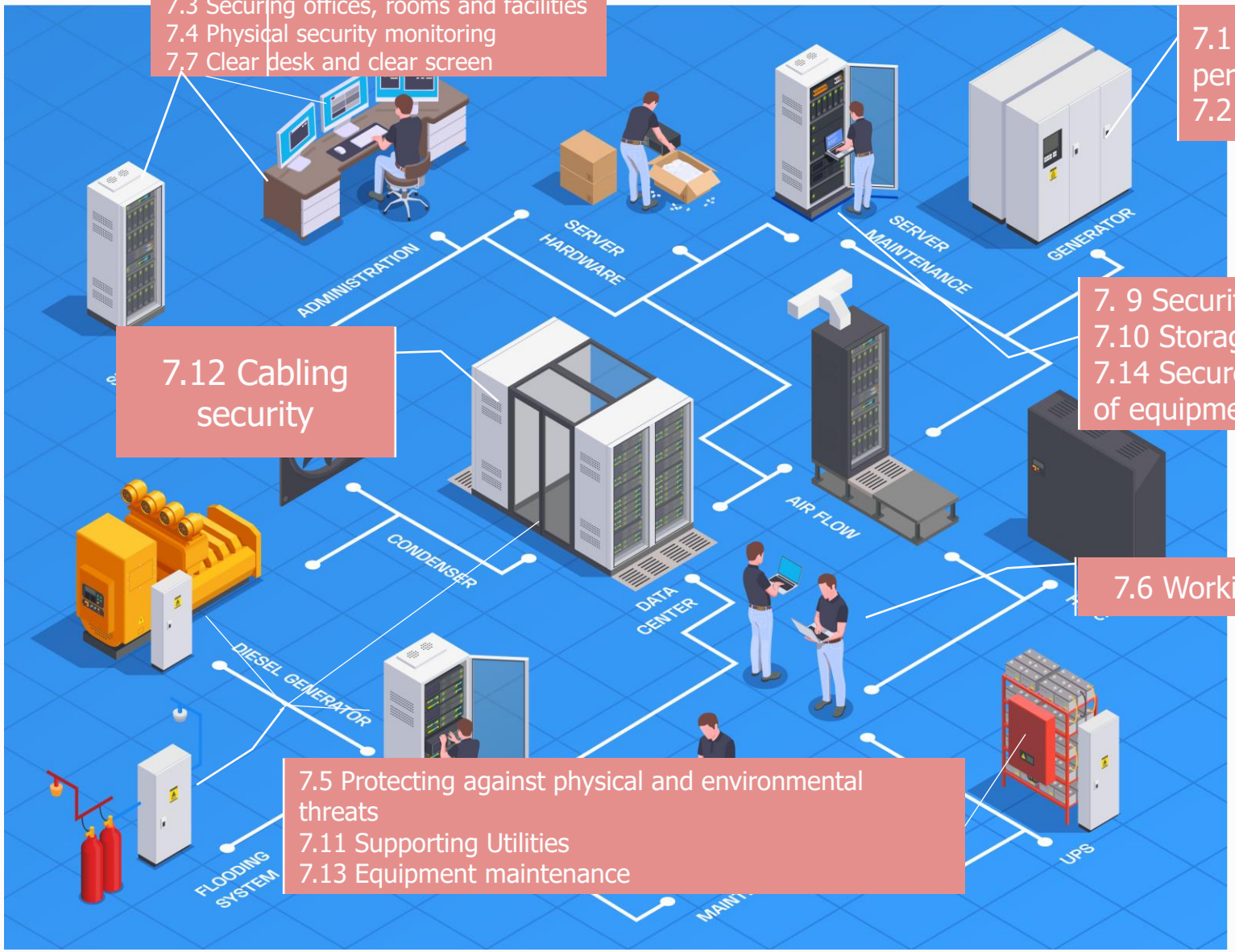
Clause 10: Improvement

Clause 10.2
(Nonconformity and corrective action)



” Summary: บทสรุปการดำเนินการรักษาความมั่นคงปลอดภัยของ Data center อย่างต่อเนื่อง”

Risk-Base-Thinking : CIA



7.3 Securing offices, rooms and facilities
7.4 Physical security monitoring
7.7 Clear desk and clear screen

7.1 Physical security perimeters
7.2 Physical Entry

7.12 Cabling security

7. 9 Security of asset off-primises
7.10 Storage media
7.14 Secure disposal and re-use of equipment

7.6 Working in secure area

7.5 Protecting against physical and environmental threats
7.11 Supporting Utilities
7.13 Equipment maintenance

Process approach

Resources Management Process

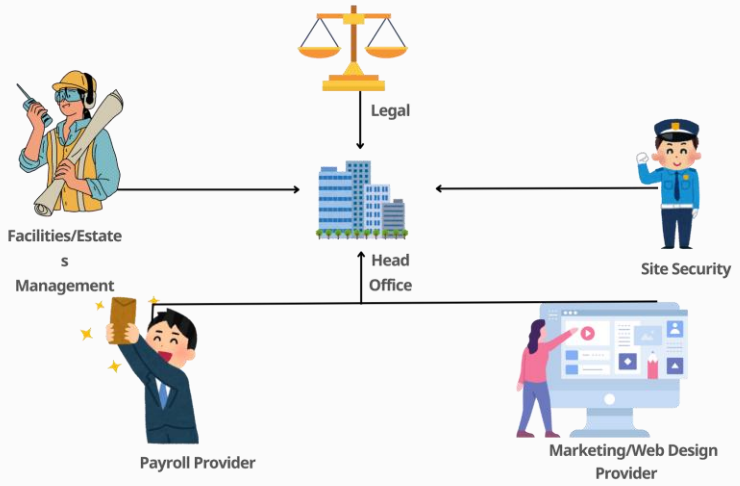
Communication Process

Document control Process

Intended Outcome

Context

Planning

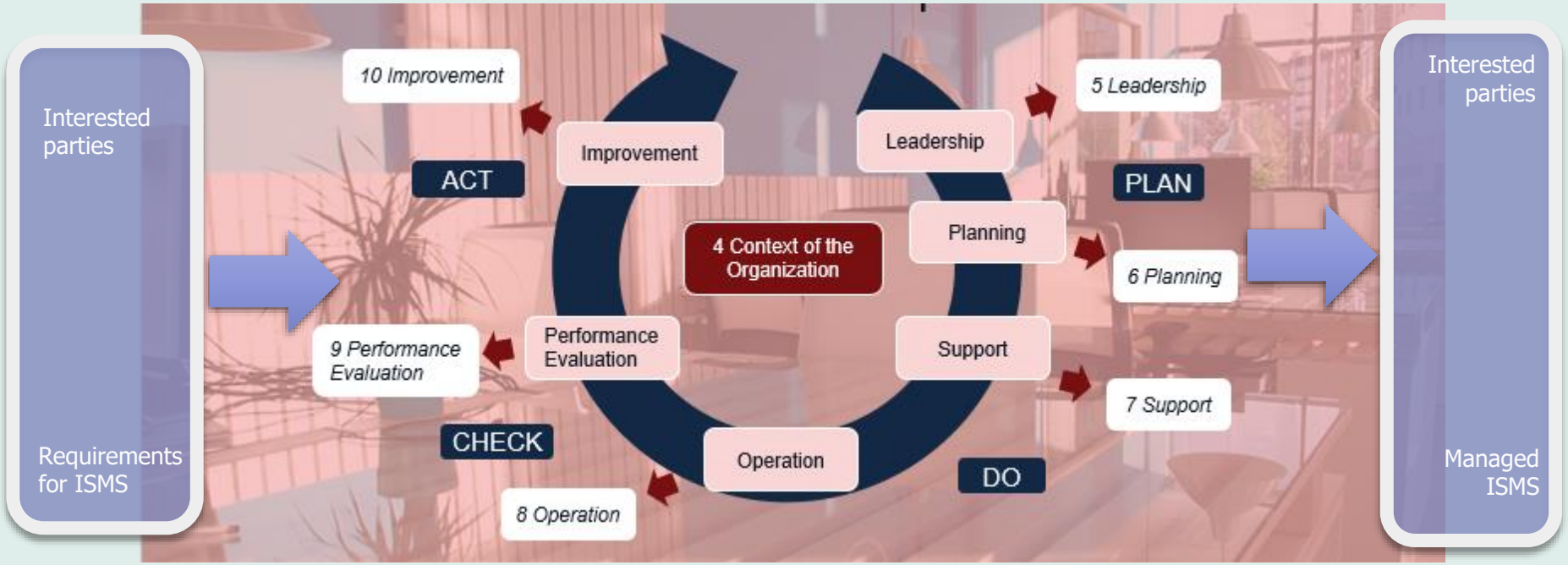


Improvement

Evaluation

Management Process

PDCA – Clauses - Implementation



Q&A Time

สแกน QR code เป็นเพื่อนกับเราใน Line official ของ BSI

เพื่อไม่ให้พลาดข่าวสารข้อมูลที่เป็นประโยชน์ในสายอาชีพของท่าน
- Free webinars
- Tool และบทความดีๆ