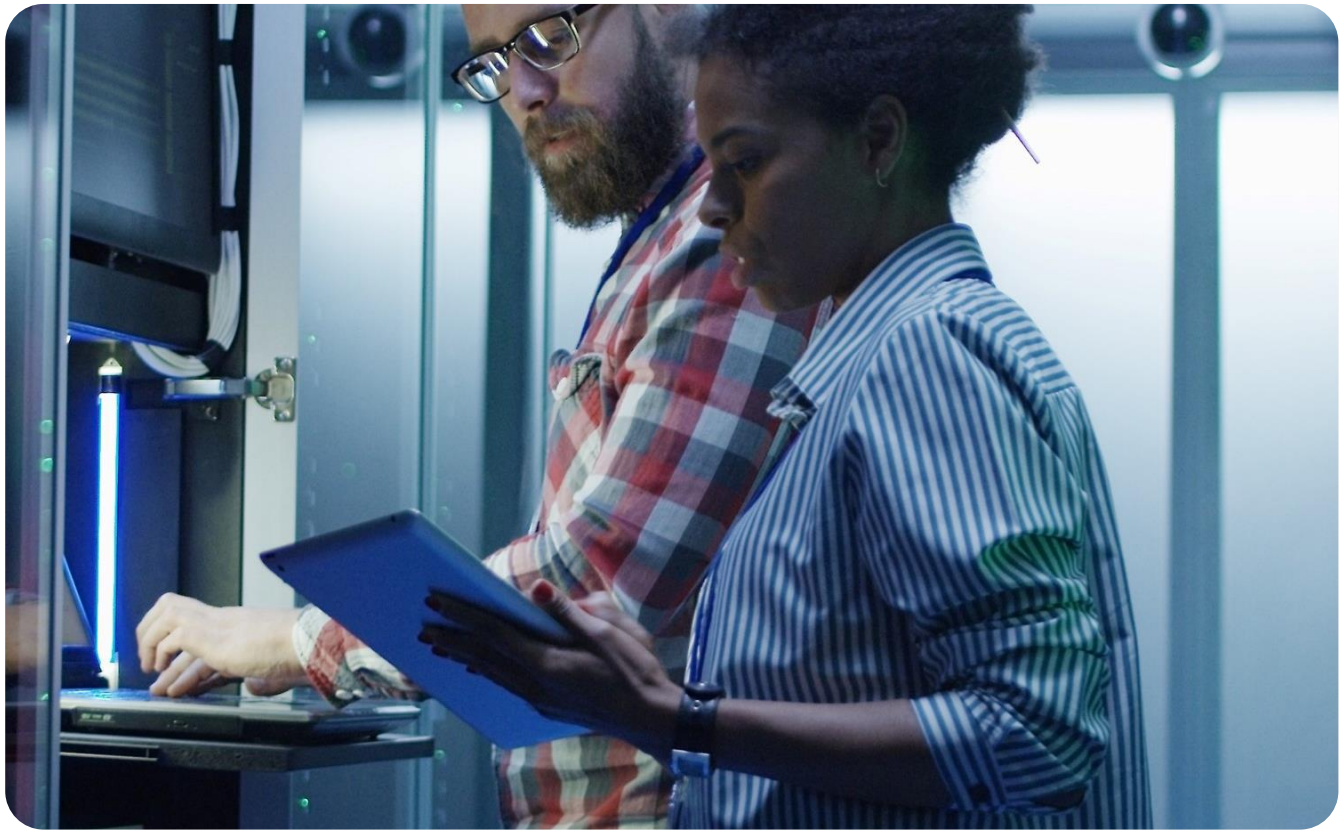
BSI Webinar

Cyber security & PDPA สำหรับ โรงงานผู้ผลิต

BSI Thailand

Discussion Topic



1. ภัยคุกคาม และผลกระทบ ด้าน Cyber security & PDPA สำหรับ โรงงานผู้ผลิต

2. การจัดการภัยคุกคาม ด้าน Cyber security & PDP และ มาตราฐานการจัดการภัยคุกคาม ด้าน Cyber security & PDPA ที่เกี่ยวข้อง

ภัยคุกคาม และผลกระทบ ด้าน Cyber security & PDPA สำหรับ โรงงานผู้ผลิต

Industrial Revolution

Industrial Revolution 1.0

- Y1784
- Hydro power

Industrial Revolution 2.0

- Y1870
- Electric power
- Mass production

Industrial Revolution 3.0

- 1969
- ICT and Electronic

Industrial Revolution 4.0

- Technology Digital and internet

ความเชื่อในโรงงาน ?

- ไม่เป็นไร ระบบเราไม่ได้ ออก Internet
- ไม่ใช้ USB แล้วทำงานไม่ได้
- ตั้ง Password – 123, 1234, name, etc.
- Share username ได้
- backup ไว้แล้ว หากโดนโจมดี ก็เอาที่ backup ขึ้นมา ได้ไม่นานหรอก
- Engineer ปรับเปลี่ยน program
- การใช้กระดาษ 2 หน้า / EMP - ลดการใช้กระดาษ

ความเชื่อในโรงงาน ?

ระบบเราเป็นระบบปิด ไม่มีอะไรหรอก

ระบบ control เรา ไม่ได้ใช้ Windows ของเราปลอดภัย

เราต่อ ระบบ ให้ Vendor connect ได้ตลอดเวลา เพื่อแก้ปัญหาได้เร็ว

Vendor เรา เขาเป็น บริษัท Inter ไม่มีปัญหาหรอก

Password ที่ควบคุมระบบ ใหญ่ อยู่ที่ vendor ก็ OK

ภัยคุกคาม และผลกระทบ ด้าน Cyber security & PDPA สำหรับ โรงงานผู้ผลิต

สหรัฐฯ ประกาศภาวะฉุกเฉินหลัง บ.ท่อส่งน้ำมันรายใหญ่โดนมัลแวร์เรียกค่าไถ่โจมตี เดือน พฤษภาคม พ.ศ. 2564 – BBC New

แฮกเกอร์ได้โจมตีทางไซเบอร์ โรงงานผลิตชิ้นส่วนพลาสติกและชิ้นส่วนอิเล็กโทรนิกส์ให้กับโรงงานผลิตรถยนต์ กุมภาพันธ์ 2022/ บริษัทผลิตรถยนต์ต้องออกมาประกาศหยุดการผลิตรถยนต์ชั่วคราวในสายการผลิต 28 แห่ง - www.nectec.or.th

โรงงานผลิตเลนส์และผลิตภัณฑ์ด้าน Optical ชื่อดังจากญี่ปุ่นถูกโจมตีไซเบอร์ - www.techtalkthai

บ.โรงไฟฟ้านิวเคลียร์” เกาหลีใต้โดนแฮก - https://mgronline.com

- ชื่อเสียงองค์กร
- Productivity
- ความเชื่อมั่นลูกค้า

- ข้อมูลส่วนบุคลที่หลุดออกไป *มีกฎหมายควบคุม*
- *กระทบความมั่นคง เมื่อให้บริการ* ไม่ได้
- Etc.

พระราชบัญญัติ คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

พระราชบัญญัติ

คุ้มครองข้อมูลส่วนบุคคล

พ.ศ. ๒๕๖๒

พระบาทสมเด็จพระปรเมนทรรามาธิบดีศรีสินทรมหาวชิราลงกรณ

พระวชิรเกล้าเจ้าอยู่หัว

ให้ไว้ ณ วันที่ ๒๔ พฤษภาคม พ.ศ. ๒๕๖๒

เป็นปีที่ ๔ ในรัชกาลปัจจุบัน

พระบาทสมเด็จพระปรเมนทรรามาธิบดีศรีสินทรมหาวชิราลงกรณ พระวชิรเกล้าเจ้าอยู่หัว มีพระบรมราชโองการโปรดเกล้าฯ ให้ประกาศว่า

พระราชบัญญัติ คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ - หมวด ๗ บทกำหนดโทษ

- **โทษอาญา:**

  ต้องระวางโทษ จำคุกไม่เกินหกเดือน หรือปรับไม่เกินห้าแสนบาท หรือทั้งจำทั้งปรับ

ดูรายละเอียดในหมวด ๗ บทกำหนดโทษ ในแต่ละมาตรา

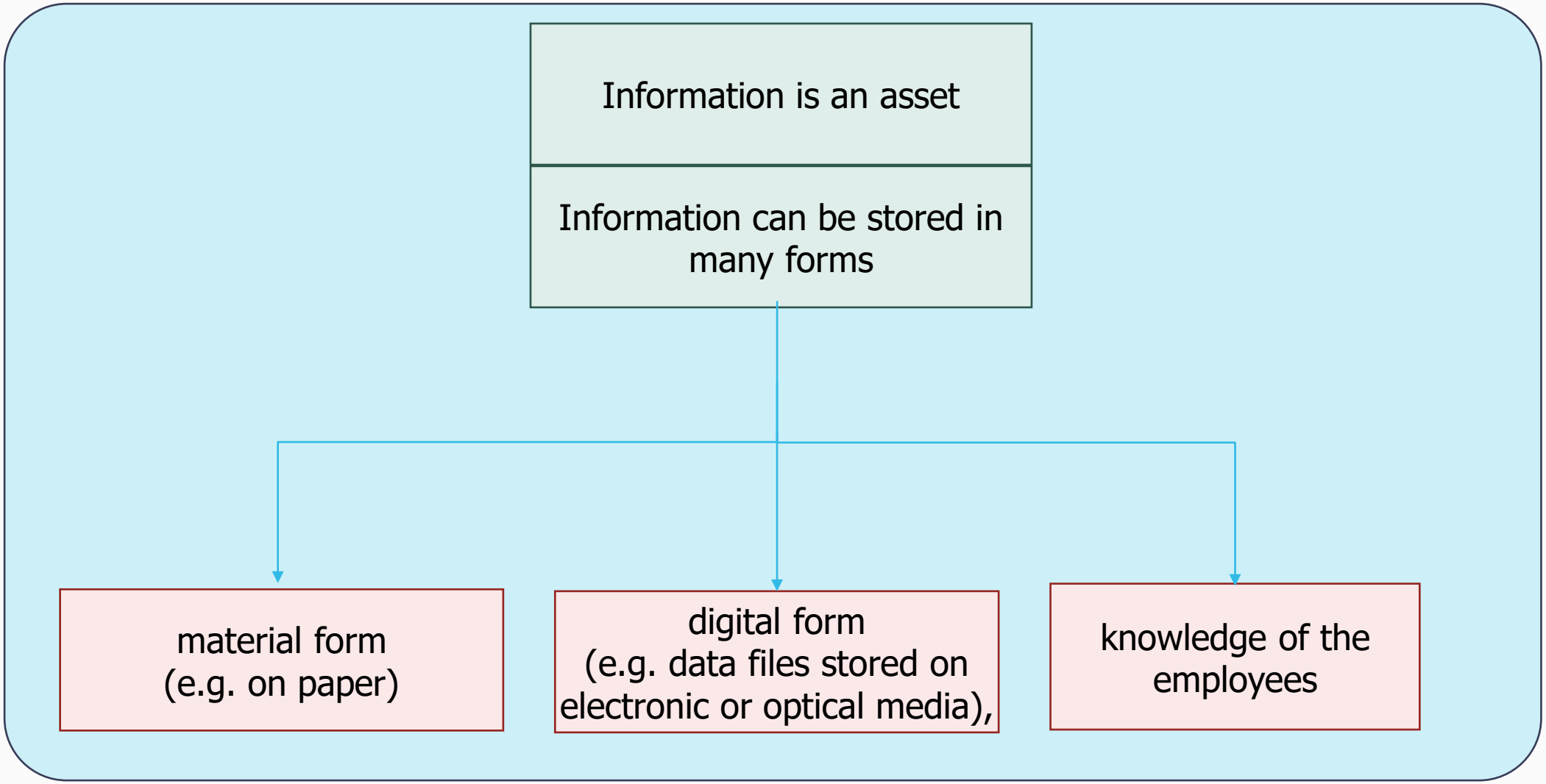
- **โทษทางปกครอง:**

โทษปรับทางปกครองไม่เกิน

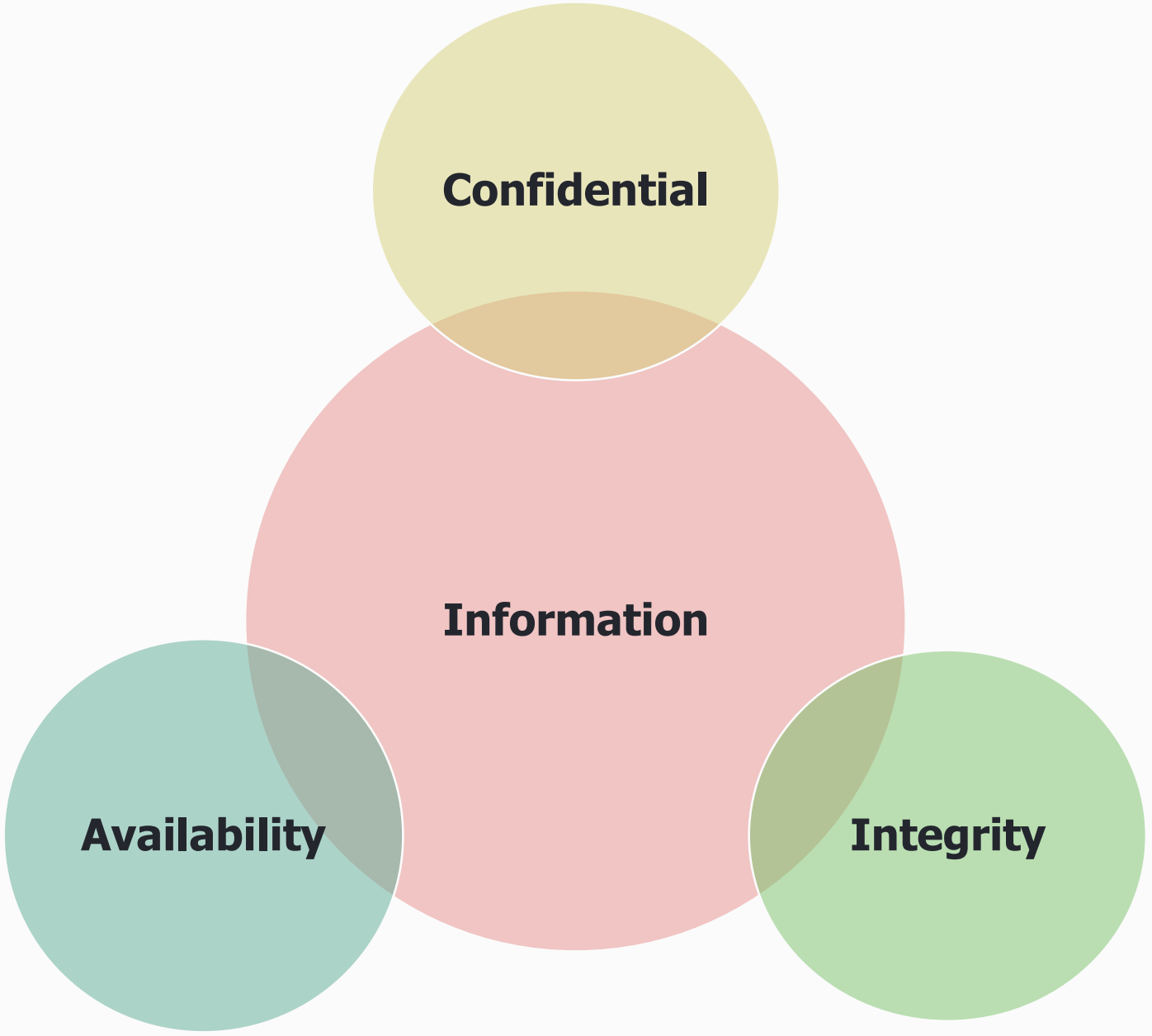
- ห้าแสนบาท
- หนึ่งล้านบาท
- สามล้านบาท
- ห้าล้านบาท

การจัดการภัยคุกคาม ด้าน Cyber security & PDP และ มาตราฐานการจัดการภัยคุกคาม ด้าน Cyber security & PDPA ที่เกี่ยวข้อง

Information



Information Security



ISO/IEC 27001 Implementation structure

INTERNATIONAL STANDARD

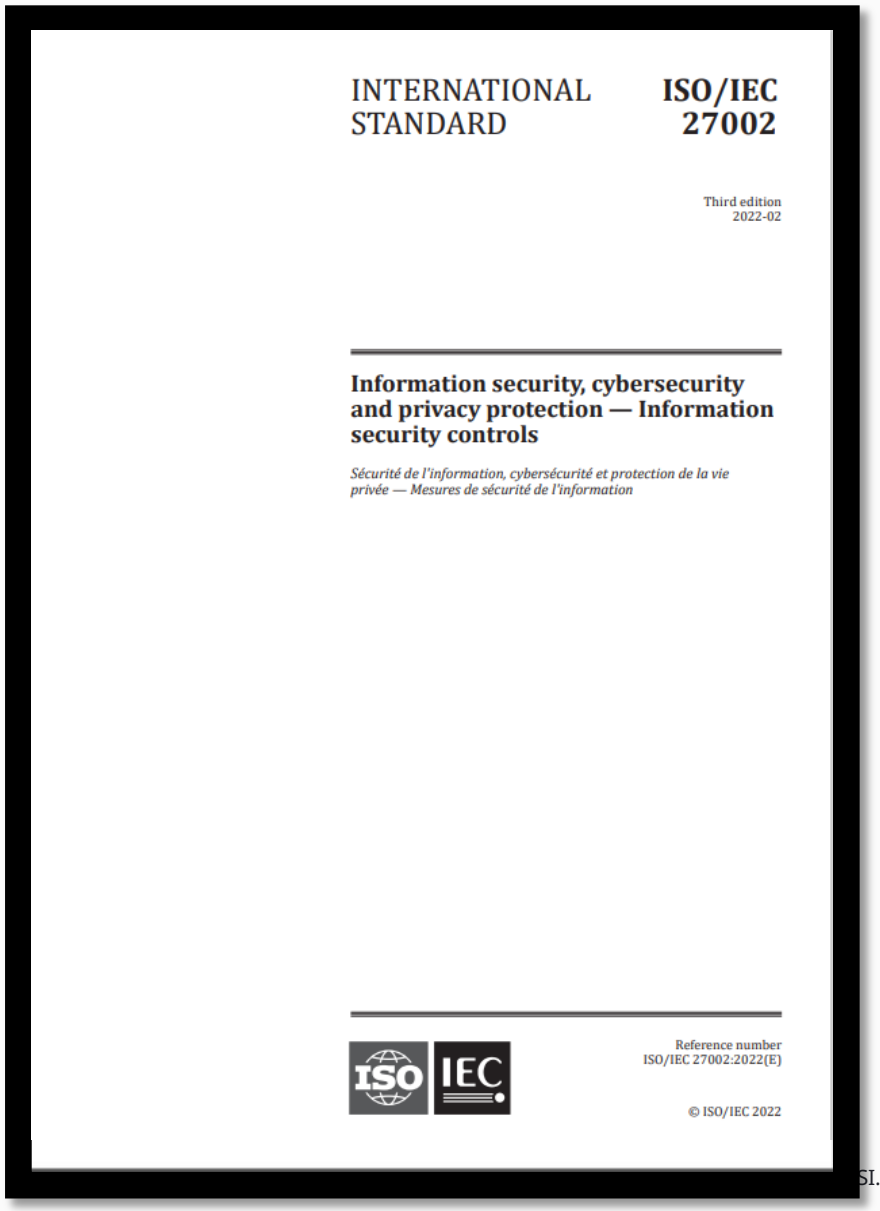
ISO/IEC 27001

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)



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 27001
Implementation structure

ISO/IEC 27001
Information security, cybersecurity and privacy protection — Information security management systems — Requirements

For the assessment and treatment of information security risks tailored to the needs of the organization

Information Security Control Annex A (5 - 8)

ISO/IEC 27002

Information security, cybersecurity and privacy protection — Information security controls

Information security controls

Requirement 5 – 8

5 - Organizational controls
6 - People controls
7 - Physical controls
8 - Technological controls

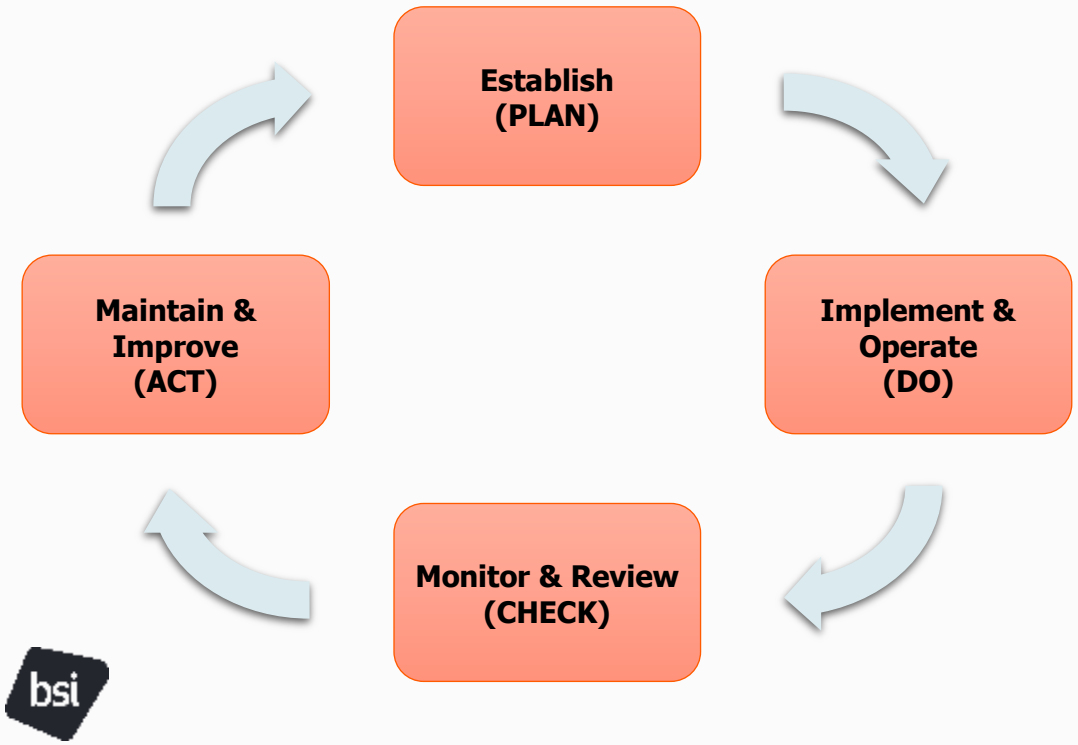
ISMS Requirement and PDCA Cycle

0 Introduction

1 Scope

2 Normative references

3 Terms and definitions



PLAN

- 4 Context of the organization
- 5 Leadership
- 6 Planning
- 7 Support

DO

- 8 Operation

CHECK

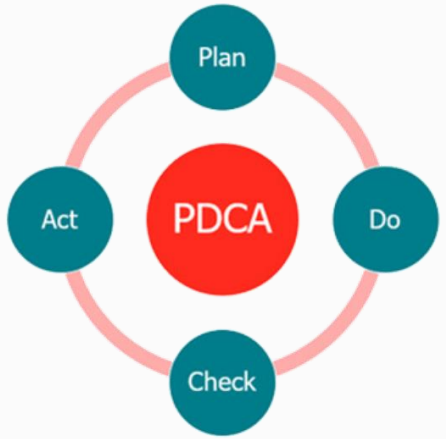
- 9 Performance evaluation

ACT

- 10 Improvement

ISMS Requirement

- 4 Context of organization
  - 4.1 Understanding context
  - 4.2 Understanding the needs and expectations of interested parties
  - 4.3 Determining the scope of the ISMS
  - 4.4 ISMS
- 5 Leadership
  - 5.1 Leadership and commitment
  - 5.2 Policy
  - 5.3 Organizational roles, responsibilities and authorities
- 6 Planning
  - 6.1 Actions to address risks and opportunities
  - 6.2 IS objectives and planning
- 7 Support
  - 7.1 Resources
  - 7.2 Competence
  - 7.3 Awareness
  - 7.4 Communication
  - 7.5 Documented information
- 8 Operation
  - 8.1 Operational planning and control
  - 8.2 IS risk assessment
  - 8.3 IS risk treatment
  - Annex A
- 9 Performance Evaluation
  - 9.1 Monitoring, measurement, analysis and evaluation
  - 9.2 Internal audit
  - 9.3 Management review
- 10 Improvement
  - 10.1 Nonconformity and corrective action
  - 10.2 Continual improvement



Annex A (ISO/IEC 27001) OR ISO 27002 Clauses

Clause 5 - Organizational controls
37 controls

Clause 6 - People controls
8 controls

Clause 7 - Physical controls
14 controls

Clause 8 - Technological controls
34 controls

Annex A (ISO/IEC 27001) OR ISO 27002 Clauses

5. Organizational controls

5.1	Policies for information security
5.2	Information security roles and responsibilities
5.3	Segregation of duties
5.4	Management responsibilities
5.5	Contact with authorities
5.6	Contact with special interest groups
5.7	Threat intelligence
5.8	Information security in project management
5.9	Inventory of information and other associated assets
5.10	Acceptable use of information and other associated assets

5.11	Return of assets
5.12	Classification of information
5.13	Labelling of information
5.14	Information transfer
5.15	Access control
5.16	Identity management
5.17	Authentication information
5.18	Access rights
5.19	Information security in supplier relationships
5.20	Addressing information security within supplier agreements

5.21	Managing information security in the ICT supply chain
5.22	Monitoring, review and change management of supplier services
5.23	Information security for use of cloud services
5.24	Information security incident management planning and preparation
5.25	Assessment and decision on information security events
5.26	Response to information security incidents
5.27	Learning from information security incidents
5.28	Collection of evidence
5.29	Information security during disruption
5.30	ICT readiness for business continuity

Annex A (ISO/IEC 27001) OR ISO 27002 Clauses

5. Organizational controls

5.31	Legal, statutory, regulatory and contractual requirements
5.32	Intellectual property rights
5.33	Protection of records
5.34	Privacy and protection of PII
5.35	Independent review of information security
5.36	Compliance with policies, rules and standards for information security
5.37	Documented operating procedures

Annex A (ISO/IEC 27001) OR ISO 27002 Clauses

6. People controls

6.1	Screening
6.2	Terms and conditions of employment
6.3	Information security awareness, education and training
6.4	Disciplinary process
6.5	Responsibilities after termination or change of employment
6.6	Confidentiality or non-disclosure agreements
6.7	Remote working
6.8	Information security event reporting

Annex A (ISO/IEC 27001) OR ISO 27002 Clauses

7. Physical controls

7.1	Physical security perimeters
7.2	Physical entry
7.3	Securing offices, rooms and facilities
7.4	Physical security monitoring
7.5	Protecting against physical and environmental threats
7.6	Working in secure areas
7.7	Clear desk and clear screen

7.8	Equipment siting and protection
7.9	Security of assets off-premises
7.10	Storage media
7.11	Supporting utilities
7.12	Cabling security
7.13	Equipment maintenance
7.14	Secure disposal or re-use of equipment

Annex A (ISO/IEC 27001) OR ISO 27002 Clauses

8. Technological controls

8.1	User endpoint devices
8.2	Privileged access rights
8.3	Information access restriction
8.4	Access to source code
8.5	Secure authentication
8.6	Capacity management
8.7	Protection against malware
8.8	Management of technical vulnerabilities

8.9	Configuration management
8.10	Information deletion
8.11	Data masking
8.12	Data leakage prevention
8.13	Information backup
8.14	Redundancy of information processing facilities
8.15	Logging
8.16	Monitoring activities

Annex A (ISO/IEC 27001) OR ISO 27002 Clauses

8. Technological controls

8.17	Clock synchronization
8.18	Use of privileged utility programs
8.19	Installation of software on operational systems
8.20	Networks security
8.21	Security of network services
8.22	Segregation of networks
8.23	Web filtering
8.24	Use of cryptography

8.25	Secure development life cycle
8.26	Application security requirements
8.27	Secure system architecture and engineering principles
8.28	Secure coding
8.29	Security testing in development and acceptance
8.30	Outsourced development
8.31	Separation of development, test and production environments
8.32	Change management
8.33	Test information
8.34	Protection of information systems during audit testing

ISO/IEC 27001 (Information Security Management System (ISMS)

Why implement ISMS:	Stakeholder confidence
	Legal compliance
	Risk management
	New business and market access

ภาพรวมมาตรฐาน ISO/IEC 27701

Privacy Information Management System (PIMS)

ISO/IEC 27701

ISO/IEC 27001
(Information Security Management System)

protection of PII principals.

(PII- Personally Identifiable Information)

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

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

A.7.2 Conditions for collection and processing

A.7.2.1 Identify and document purpose
A.7.2.2 Identify lawful basis
A.7.2.3 Determine when and how consent is to be obtained
A.7.2.4 Obtain and record consent
A.7.2.5 Privacy impact assessment
A.7.2.6 Contracts with PII processors
A.7.2.7 Joint PII controller
A.7.2.8 Records related to processing PII

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

A.7.3 Obligations to PII principals

A.7.3.1 Determining and fulfilling obligations to PII principals.
A.7.3.2 Determining information for PII principals
A.7.3.3 Providing information to PII principals
A.7.3.4 Providing mechanism to modify or withdraw consent
A.7.3.5 Providing mechanism to object to PII processing
A.7.3.6 Access, correction and/or erasure
A.7.3.7 PII controllers' obligations to inform third parties
A.7.3.8 Providing copy of PII processed
A.7.3.9 Handling requests
A.7.3.10 Automated decision making

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

A.7.4 Privacy by design and privacy by default

A.7.4.1 Limit collection
A.7.4.2 Limit processing
A.7.4.3 Accuracy and quality
A.7.4.4 PII minimization objectives
A.7.4.5 PII de-identification and deletion at the end of processing
A.7.4.6 Temporary files
A.7.4.7 Retention
A.7.4.8 Disposal
A.7.4.9 PII transmission controls

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

A.7.5 PII sharing, transfer and disclosure

A.7.5.1 Identify basis for PII transfer between jurisdictions
A.7.5.2 Countries and international organizations to which PII can be transferred
A.7.5.3 Records of transfer of PII
A.7.5.4 Records of PII disclosure to third parties

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

B.8.2 Conditions for collection and processing

B.8.2.1 Customer agreement
B.8.2.2 Organization's purposes
B.8.2.3 Marketing and advertising use
B.8.2.4 Infringing instruction
B.8.2.5 Customer obligations
B.8.2.6 Records related to processing PII

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

B.8.3 Obligations to PII principals

B.8.3.1 Obligations to PII principals

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

B.8.4 Privacy by design and privacy by default

B.8.4.1 Temporary files
B.8.4.2 Return, transfer or disposal of PII
B.8.4.3 PII transmission controls

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

B.8.5 PII sharing, transfer and disclosure

B.8.5.1 Basis for PII transfer between jurisdictions
B.8.5.2 Countries and international organizations to which PII can be transferred
B.8.5.3 Records of PII disclosure to third parties
B.8.5.4 Notification of PII disclosure requests
B.8.5.5 Legally binding PII disclosures
B.8.5.6 Disclosure of subcontractors used to process PII
B.8.5.7 Engagement of a subcontractor to process PII
B.8.5.8 Change of subcontractor to process PII

ISO/IEC 27701 (Privacy Information Management System – PIMS)

Requirement ISO/IEC 27001 + GDPR requirement

Additional requirement for GDPR is separated as Controller or Processor

Base on ISO/IEC 27001 certification

Why implement PIMS:

- Provides assurance and confidence
- Maps to GDPR and various frameworks
- Tailored to PII controllers and processors
- Generates documentary evidence

Contact us

www.bsigroup.com/th-TH/

BSI Thailand

@bsithailand

Tel: 02 294 4889-92 Email: infothai@bsigroup.com