# BSI Webinar

เตรียมความพร้อมและรับมือกับภัยทางไซเบอร์ด้วย

# ISO/IEC 27001:2022

## สำหรับอุตสาหกรรมการผลิต

สถาบันมาตรฐานอังกฤษ

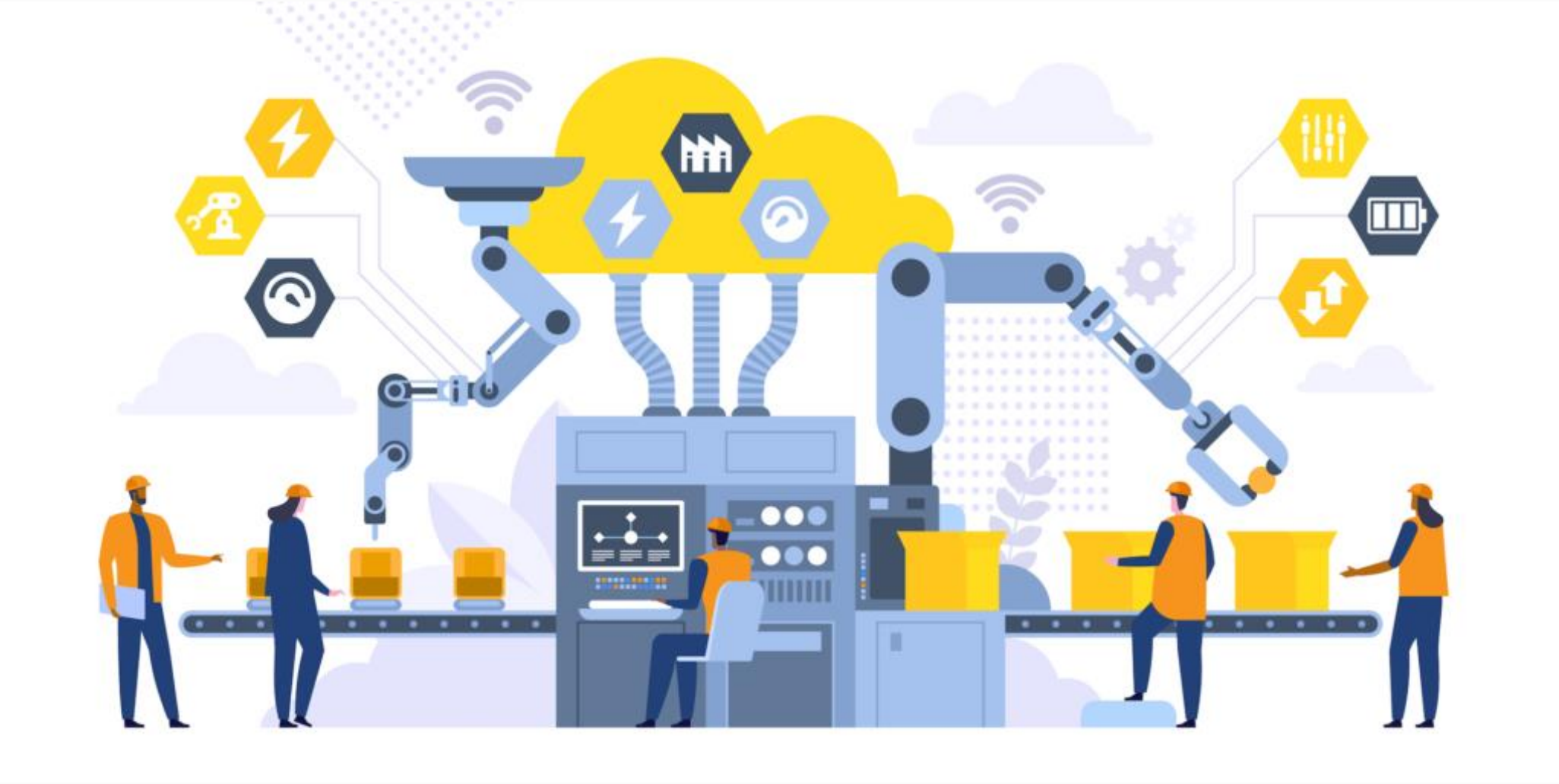
# TOPIC

1 สารสนเทศ กับ อุตสาหกรรมการผลิต และภัยคุกคามที่อาจเกิดขึ้น

2 ISO/IEC 27001:2022 ช่วยให้สารสนเทศมีความมั่นคงปลอดภัยได้อย่างไร

3 การประยุกต์ใช้ข้อกำหนดและมาตรการควบคุมตาม ISO/IEC 27001:2022

# สารสนเทศกับอุตสาหกรรมการผลิตและภัยคุกคามที่อาจเกิดขึ้น



# Information can be in any media (electronic/paper)

## 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 Lifecycle

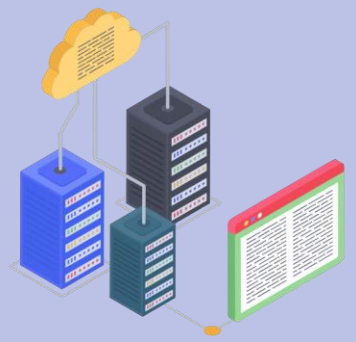
Creation/ Collection

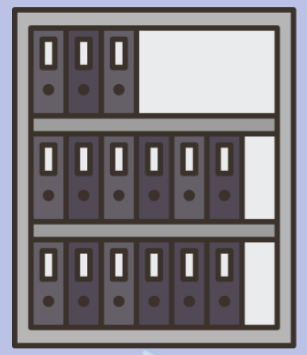
Storage

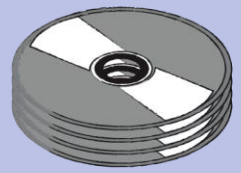
Processing

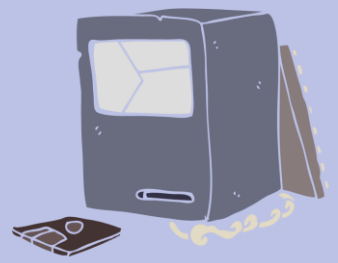
Usage/ sharing

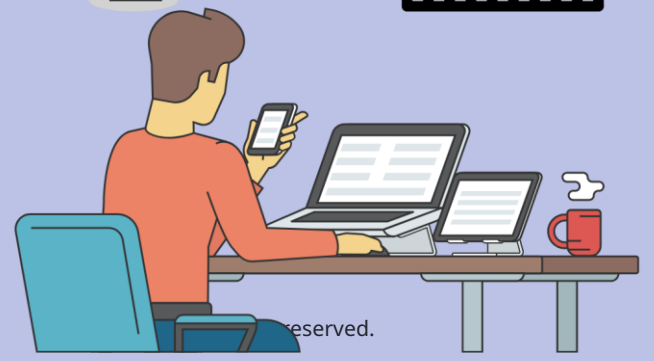
Disposal

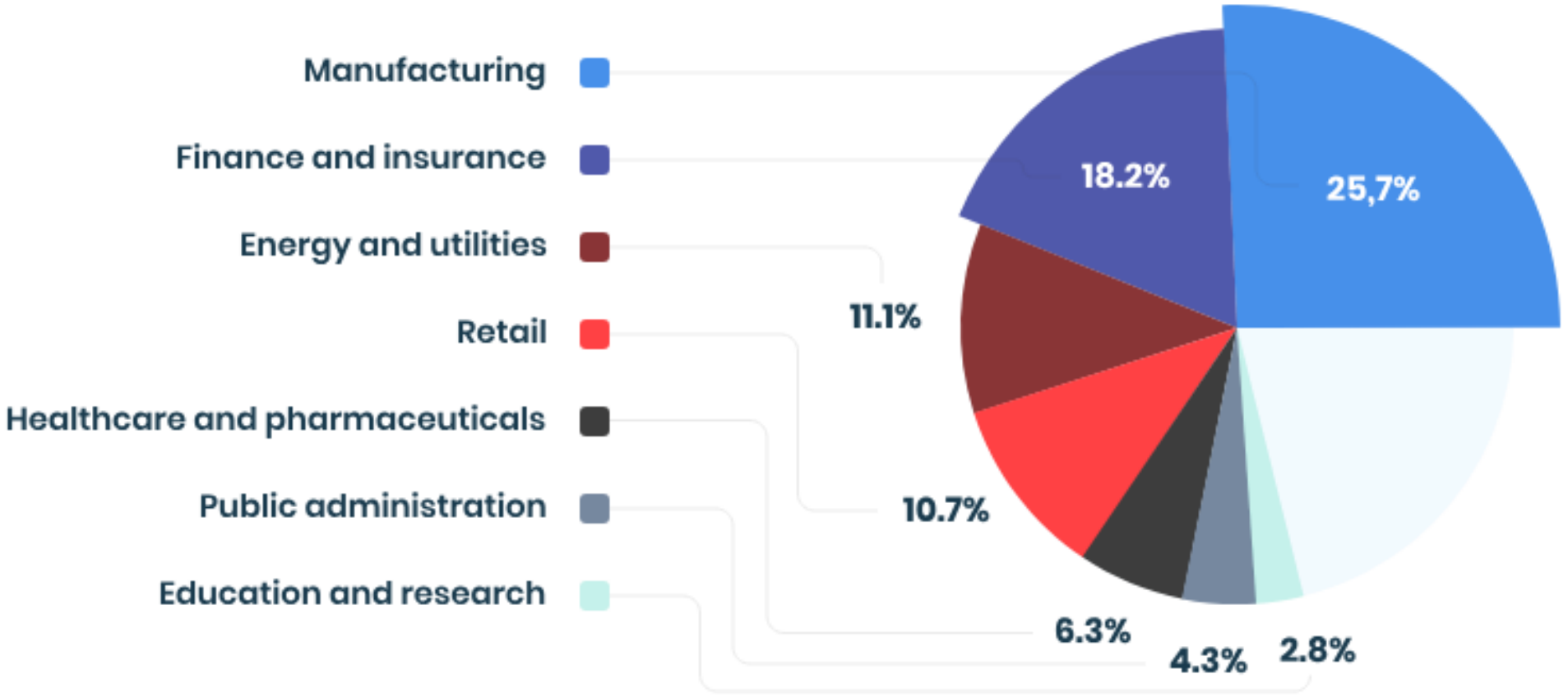








# Share of attacks by industry in 2023




*According to the 2024 X-Force Threat Intelligence Index by IBM Security*

Ekran
www.ekransystem.com

Credit: https://www.ekransystem.com/en/blog/5-industries-most-risk-of-data-breaches

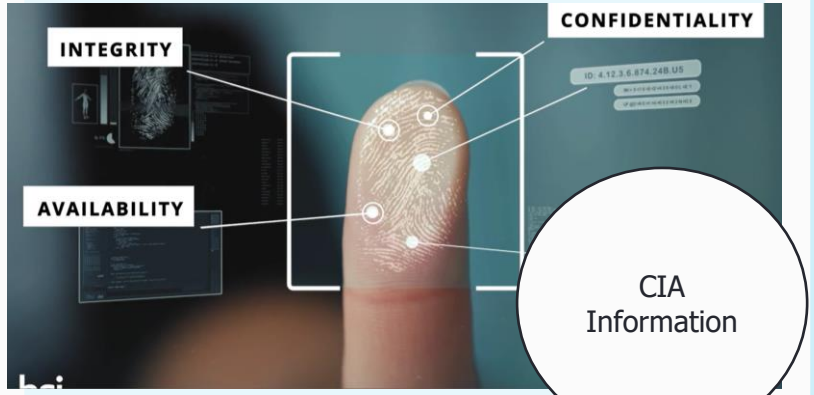
# Top 7 Cyber Security Risks in Manufacturing 2024


Credit: https://itopia.com.au/insights/top-7-cyber-security-risks-in-manufacturing/

# ISO/IEC 27001:2022 ช่วยให้สารสนเทศมีความมั่นคงปลอดภัยได้อย่างไร

ISO/IEC 27001 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*

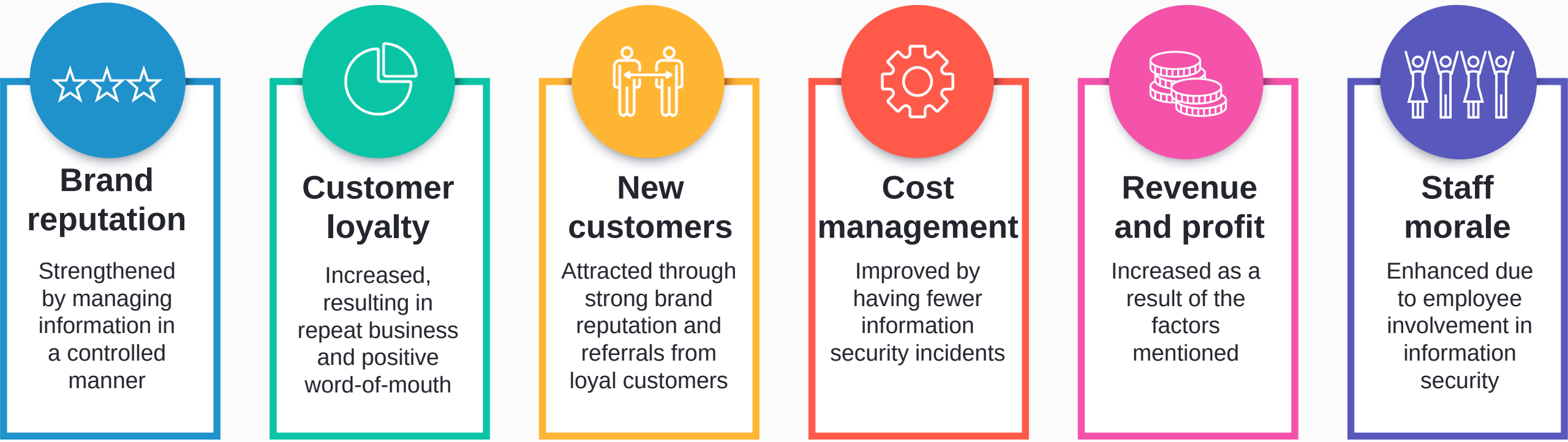
ISO IEC

Reference number
ISO/IEC 27001:2022(E)

# What do we mean by ‘information security’?

**Information Security** is preservation of **C**onfidentiality, **I**ntegrity and **A**vailability of information

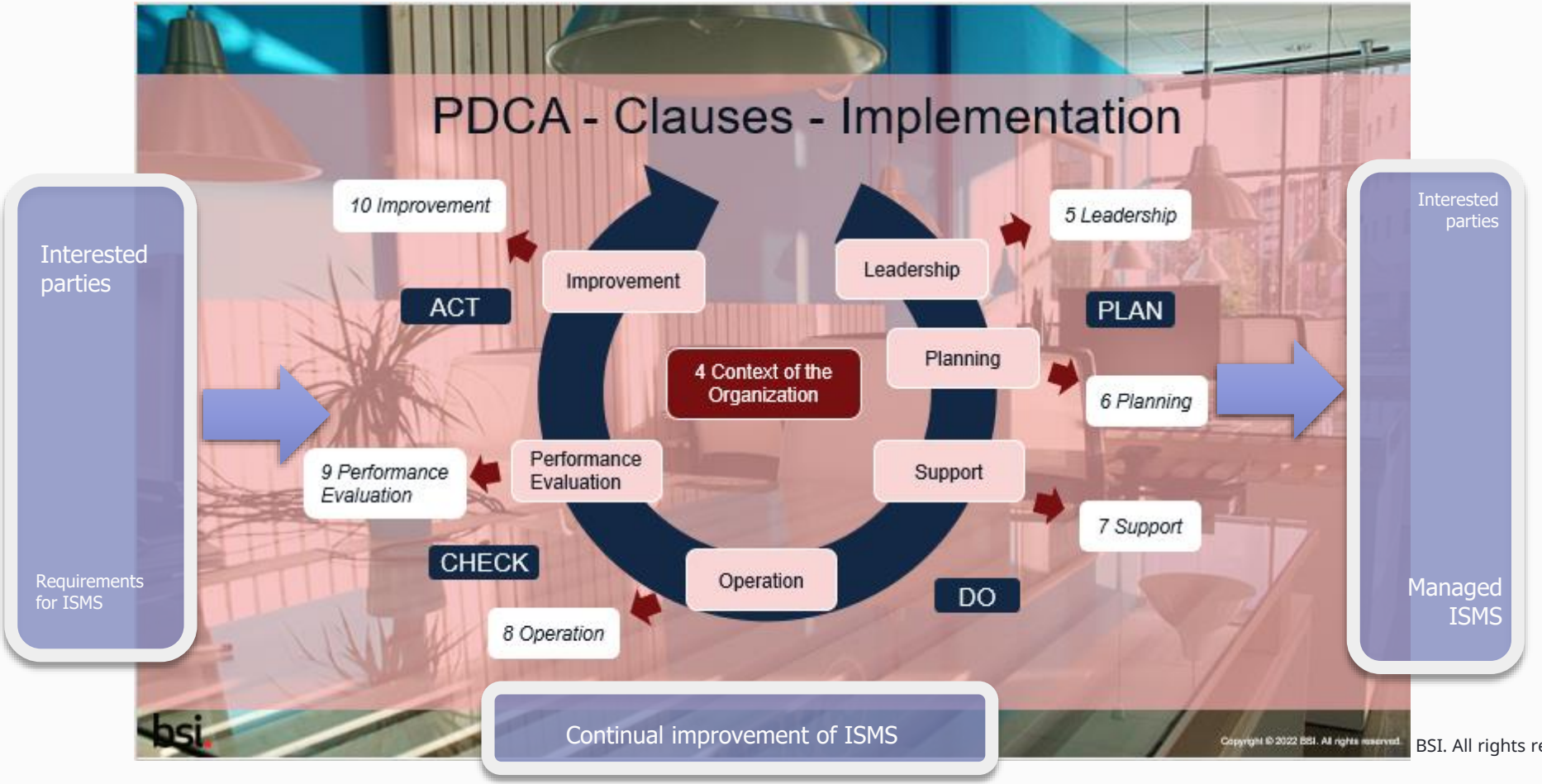
# The benefits of good information security



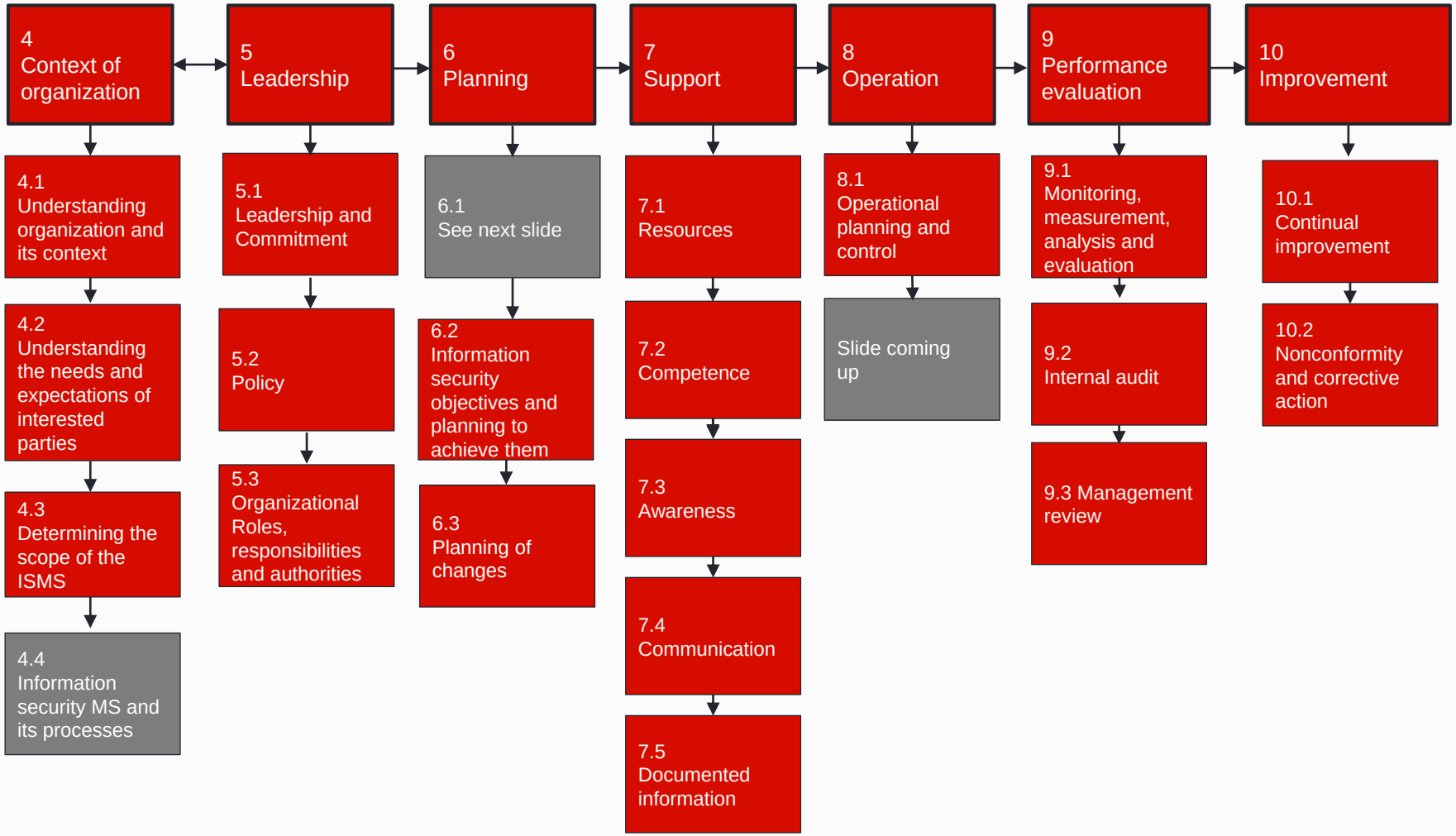
# การประยุกต์ใช้ข้อกำหนดและมาตรการควบคุมตาม ISO/IEC 27001:2022

## PDCA and ISMS

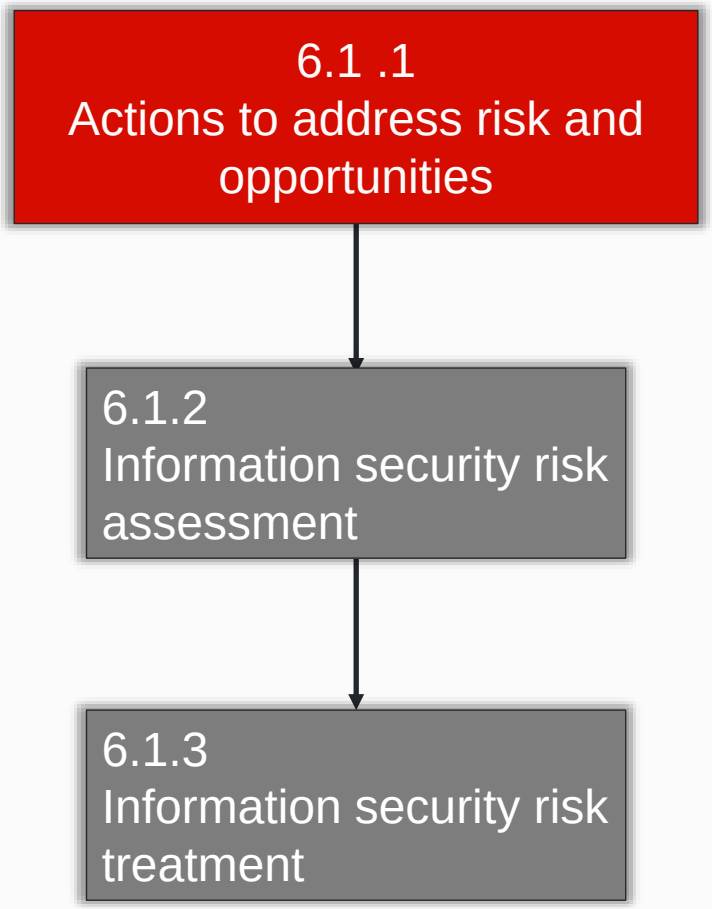
ISO/IEC 27001 is based on the plan-do-check-action (P-D-C-A cycle) and requires organizations to implement a comprehensive set of policies, procedures and controls to manage information security risks and ensures the confidentiality, integrity and availability of information.

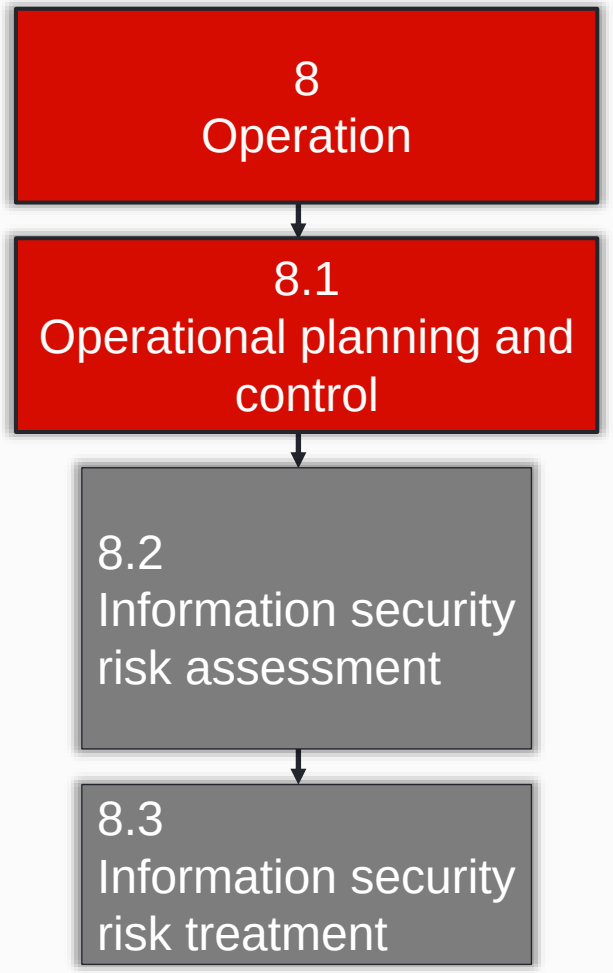


# ISO/IEC 27001:2022 Clause requirements



# ISO/IEC 27001:2022 Clause requirements (continue)



# ISO/IEC 27001:2022 Annex A.

A.5 - Organizational controls (37 controls)

A.6 - People controls (8 controls)

A.7 - Physical controls (14 controls)

A.8 - Technological controls (34 controls)

# ISO/IEC 27001:2022 Annex A.

## A.5 - Organizational controls
## 37 controls

A5.1 Policies for information security
A5.2 Information security roles and responsibilities
A5.3 Segregation of duties
A5.4 Management responsibilities
A5.5 Contact with authorities
A5.6 Contact with special interest groups
A5.7 Threat intelligence
A5.8 Information security in project management
A5.9 Inventory of information and other associated assets
A5.10 Acceptable use of information and other associated assets
A5.11 Return of assets
A5.12 Classification of information
A5.13 Labelling of information
A5.14 Information transfer
A5.15 Access control
A5.16 Identity management
A5.17 Authentication information
A5.18 Access rights
A5.19 Information security in supplier relationships
A5.20 Addressing information security within supplier agreements
A5.21 Managing information in the ICT supply chain
A5.22 Monitoring, review and change management of supplier services
A5.23 Information security for use of cloud services
A5.24 Information security incident management planning and preparation
A5.25 Assessment and decision on information security events
A5.26 Response to information security incidents
A5.27 Learning from information security incidents
A5.28 Collection of evidence
A5.29 Information security during disruption
A5.30 ICT readiness for business continuity
A5.31 Legal, statutory, regulatory and contractual requirements
A5.32 Intellectual property rights
A5.33 Protection of records
A5.34 Privacy and protection of PII
A5.35 Independent review of information security
A5.36 Conformance with policies, rules and standards for information security
A5.37 Documented operating procedures

# ISO/IEC 27001:2022 Annex A.

**A.6 - People controls**
**8 controls**

| | |
|---|---|
| A6.1 | Screening |
| A6.2 | Terms and definitions of employment |
| A6.3 | Information security awareness, education and training |
| A6.4 | Disciplinary process |
| A6.5 | Responsibilities after termination or change of employment |
| A6.6 | Confidentiality or non-disclosure agreements |
| A6.7 | Remote working |
| A6.8 | Information security event reporting |

# ISO/IEC 27001:2022 Annex A.

**A.7 - Physical controls**
**14 controls**

| | |
|---|---|
| A7.1 | Physical security perimeters |
| A7.2 | Physical entry |
| A7.3 | Securing offices, rooms and facilities |
| A7.4 | Physical security monitoring |
| A7.5 | Protecting against physical and environmental threats |
| A7.6 | Working in secure areas |
| A7.7 | Clear desk and clear screen |
| A7.8 | Equipment siting and protection |
| A7.9 | Security of assets off-premises |
| A7.10 | Storage media |
| A7.11 | Supporting utilities |
| A7.12 | Cabling security |
| A7.13 | Equipment maintenance |
| A7.14 | Secure disposal or re-use of equipment |

# ISO/IEC 27001:2022 Annex A.

## A.8 - Technological controls
## 34 controls

| | |
|---|---|
| A8.1 | User endpoint devices |
| A8.2 | Privileged access rights |
| A8.3 | Information access restriction |
| A8.4 | Access to source code |
| A8.5 | Secure authentication |
| A8.6 | Capacity management |
| A8.7 | Protection against malware |
| A8.8 | Management of technical vulnerabilities |
| A8.9 | Configuration management |
| A8. 10 | Information deletion |
| A8.11 | Data masking |
| A8.12 | Data leakage prevention |
| A8.13 | Information backup |
| A8.14 | Redundancy of information processing facilities |
| A8.15 | Logging |
| A8.16 | Monitoring activities |
| A8.17 | Clock synchronization |
| A8.18 | Use of privileged utility programs |
| A8.19 | Installation of software on operational systems |
| A8. 20 | Networks security |
| A8.21 | Security of network services |
| A8.22 | Segregation of networks |
| A8.23 | Web filtering |
| A8.24 | Use of cryptography |
| A8.25 | Secure development lifecycle |
| A8.26 | Application security requirements |
| A8.27 | Secure system architecture and engineering principles |
| A8.28 | Secure coding |
| A8.29 | Security testing in development and acceptance |
| A8. 30 | Outsourced development |
| A8.31 | Separation of development, test and production environments |
| A8.32 | Change management |
| A8.33 | Test information |
| A8.34 | Protection of information systems during audit testing |

# Minimum Documented Requirements in ISO/IEC 27001:2022

| ISO/IEC 27001 clause: | Documented Requirements |
|---|---|
| 4.1 | - |
| 4.2 | - |
| 4.3 | Scope |
| 4.4 | - |
| 5.1 | - |
| 5.2 | Policy |
| 5.3 | - |
| 6.1.1 | - |
| 6.1.2 | Information security risk assessment process |
| 6.1.3 | Statement of Applicability<br>Information security risk treatment plan<br>Information security risk treatment process |
| 6.2 | Information security objectives |
| 6.3 | - |
| 7.1 | - |
| 7.2 | Evidence of competence |
| 7.3 | - |
| 7.4 | - |
| 7.5.1 | Documented information required by this International Standard as well as documented information, determined by the organization, as being required for the effectiveness of the information security management system |
| 7.5.2 | - |
| 7.5.3 | Documented information of external origin determined by the organization to be necessary. |
| 8.1 | Information to the extent necessary to have confidence that the processes have been carried out as planned |
| 8.2 | Results of information security risk assessments |
| 8.3 | Results of information security risk treatment |
| 9.1 | Evidence of monitoring and measurement results |
| 9.2 | Audit programme(s)<br>Evidence of the implementation of the audit programme(s) and the audit results |
| 9.3 | Information as evidence of the results of the management reviews |
| 10.1 | - |
| 10.2 | Information of the nature of the nonconformities and any subsequent actions taken, and the results of any corrective action. |

| ISO/IEC 27001 clause: | **Process and Procedure Requirements (not necessarily documented)** |
|---|---|
| 6.3 | Change management process |
| 7.4 | Communication process |
| 7.5 | Documented information control |
| 8.1 | Processes needed to meet information security requirements<br>Outsourced processes. |
| 9.1 | Methods for monitoring, measurement, analysis, and evaluation |

# Q&A Time

**สแกน QR code เป็นเพื่อนกับเราใน Line official ของ BSI**

เพื่อไม่ให้พลาดข่าวสารข้อมูลที่เป็นประโยชน์ในสายอาชีพของท่าน
- Free webinars
- Tool และบทความดีๆ