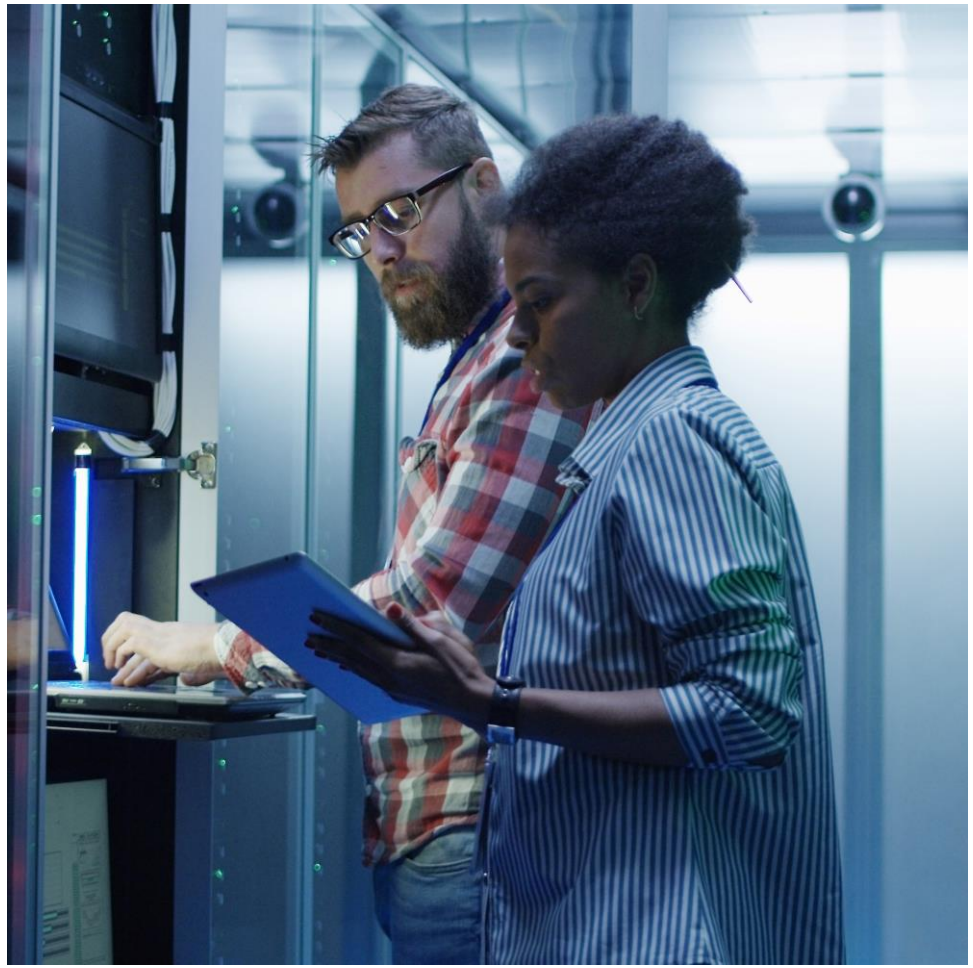
Cyber Security and Privacy for factory

BSI Group (Thailand) Ltd.

Discussion Topic.

1. ภัยและผลกระทบต่อระบบการผลิตในโรงงาน จาก Cyber, Security, และ Privacy ที่มีผลกระทบต่อชื่อเสียงโรงงาน และการผลิต

2. มาตรฐาน ISO/IEC 27001, ISO/IEC 27701 ที่อาจนำมาประยุกต์ใช้เพื่อป้องกัน



bsi.

ภัยและผลกระทบต่อระบบการผลิตในโรงงาน จาก Cyber, Security, และ Privacy ที่มีผลกระทบต่อชื่อเสียงโรงงาน และการผลิต

bsi.

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

bsi.

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

bsi.

Cyber, Security, and Privacy Threat in factory

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

โรงงานผลิตเลนส์และผลิตภัณฑ์ด้าน Optical ชื่อดังจากญี่ปุ่นถูกโจมตีไซเบอร์ - www.techtalkthai

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

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

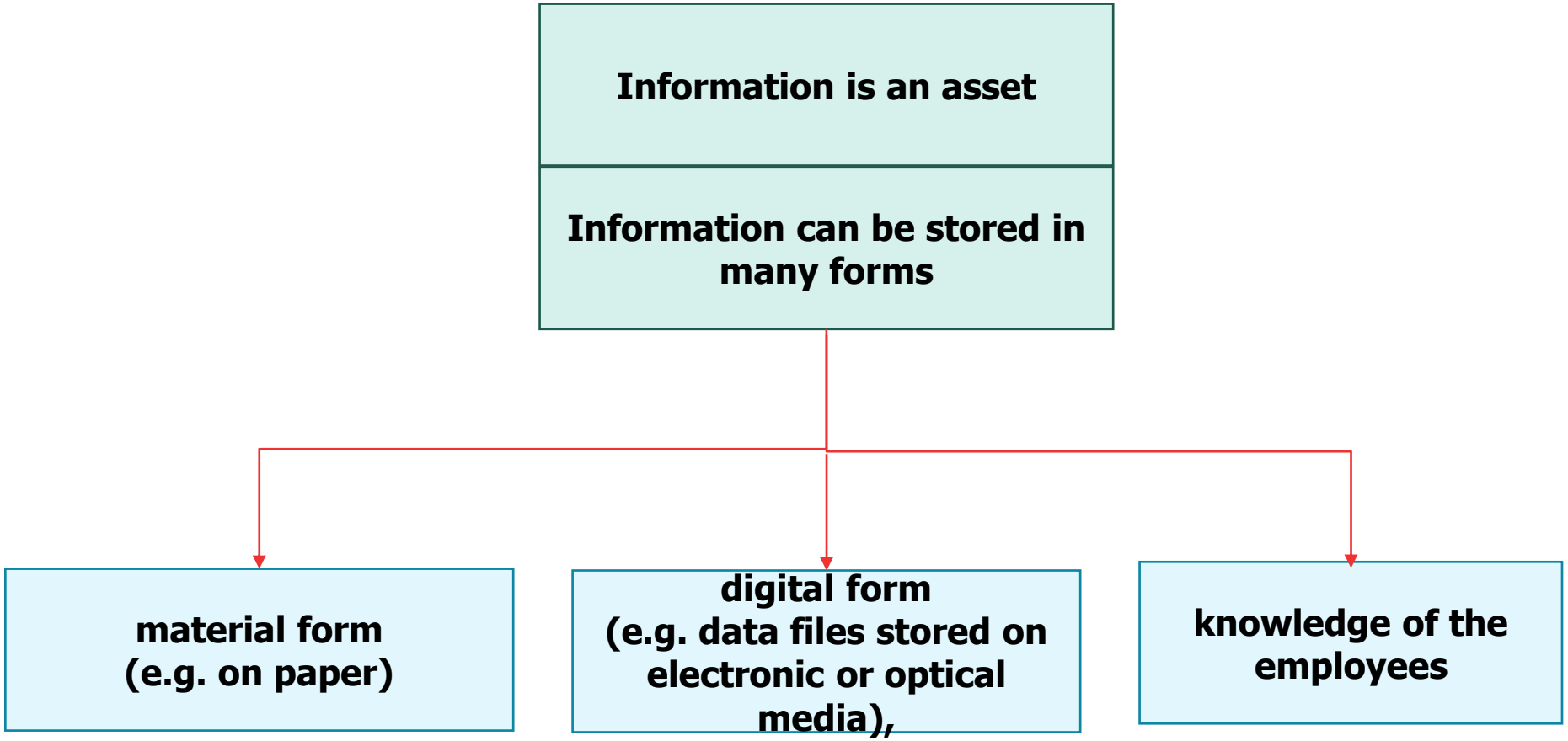
- ชื่อเสียงองค์กร
- Productivity
- ความเชื่อมั่นลูกค้า
- ข้อมูลส่วนบุคลที่หลุดออกไป มีกฎหมายควบคุม
- กระทบความมั่นคง เมื่อให้บริการ ไม่ได้
- Etc.

bsi.

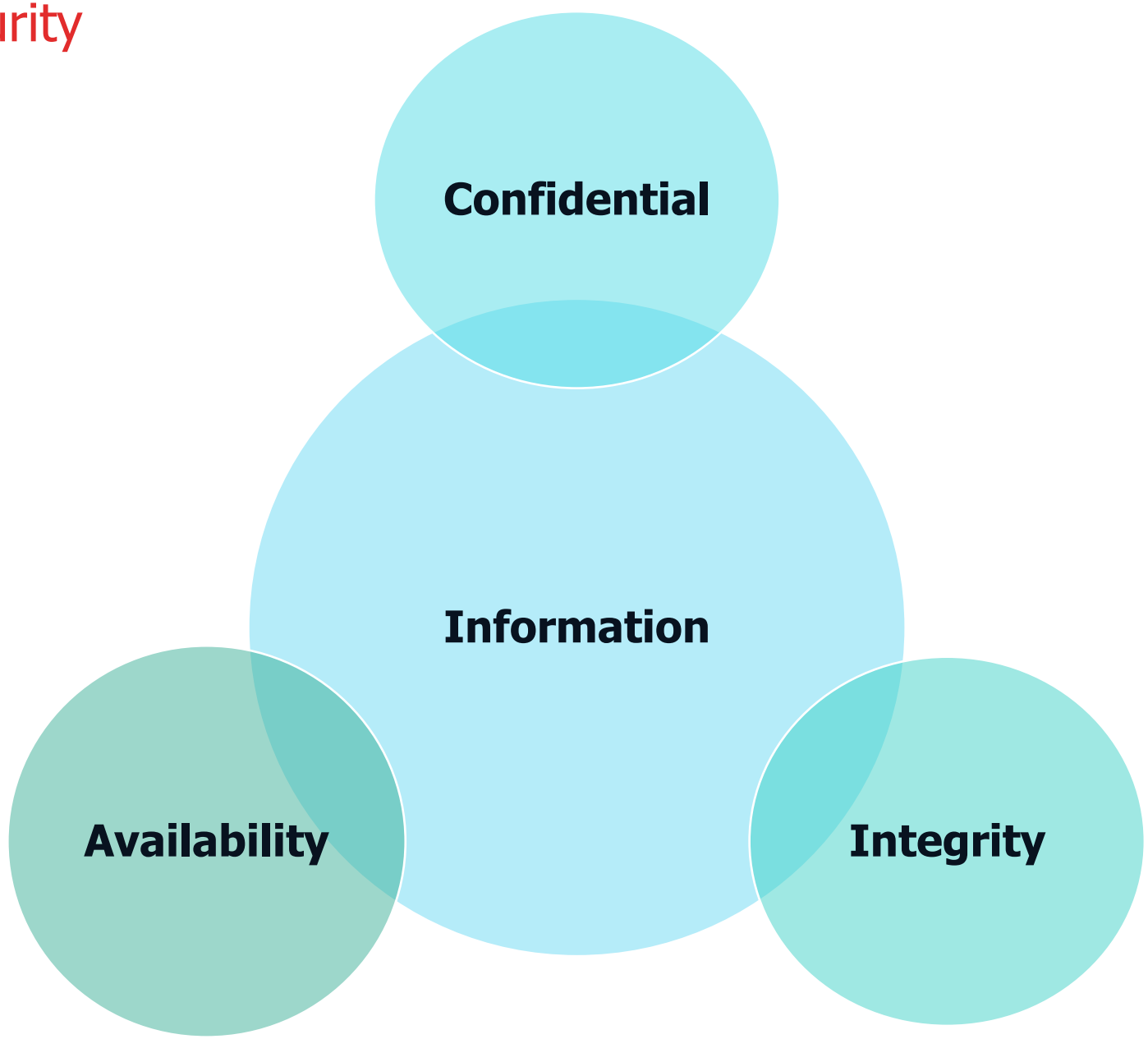
มาตรฐาน

ISO/IEC 27001, ISO/IEC 27701 ที่อาจนำมาประยุกต์ใช้เพื่อป้องกัน

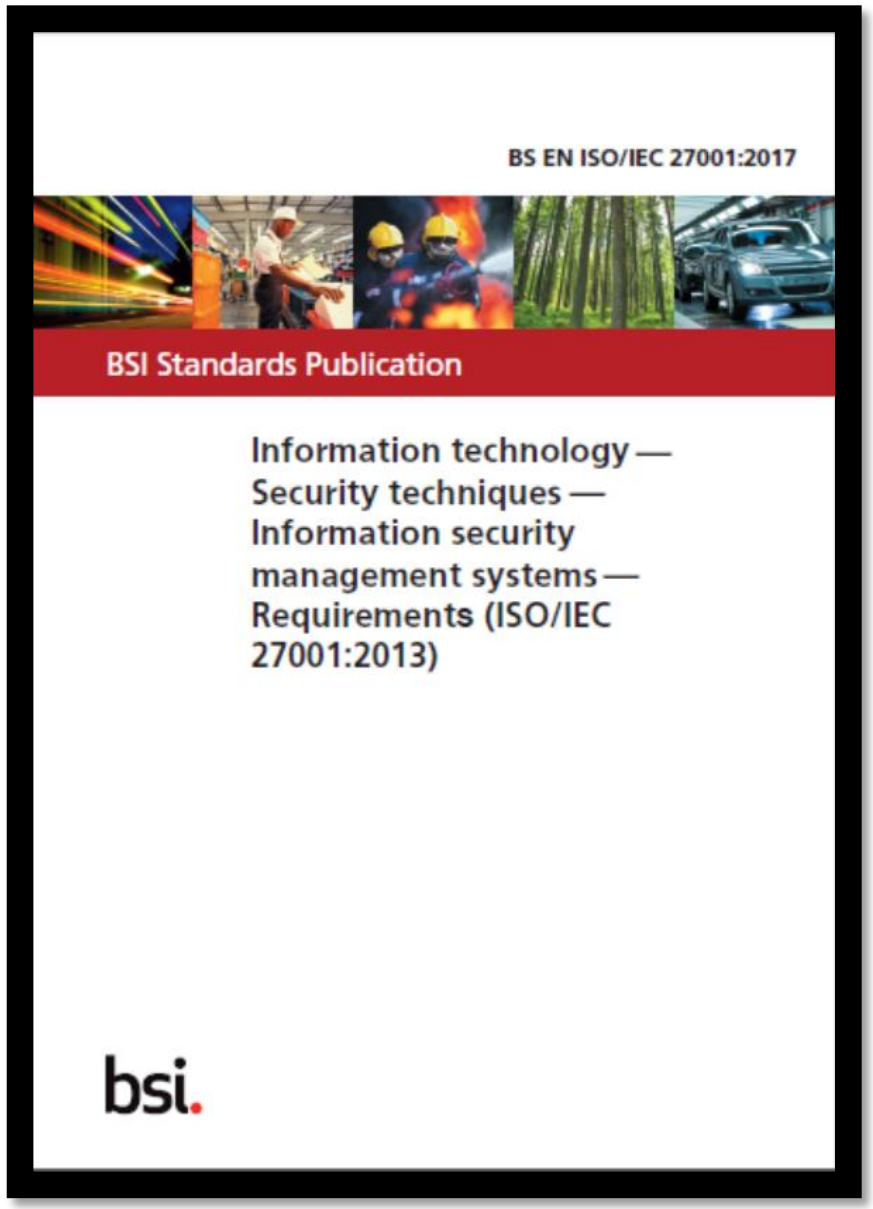
Information



Information Security



ISO/IEC 27001 Implementation structure

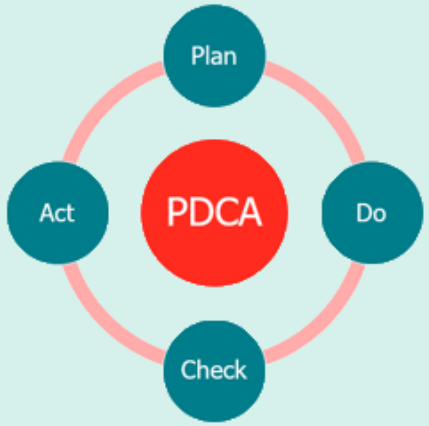


bsi.

ISO/IEC 27001
Implementation structure

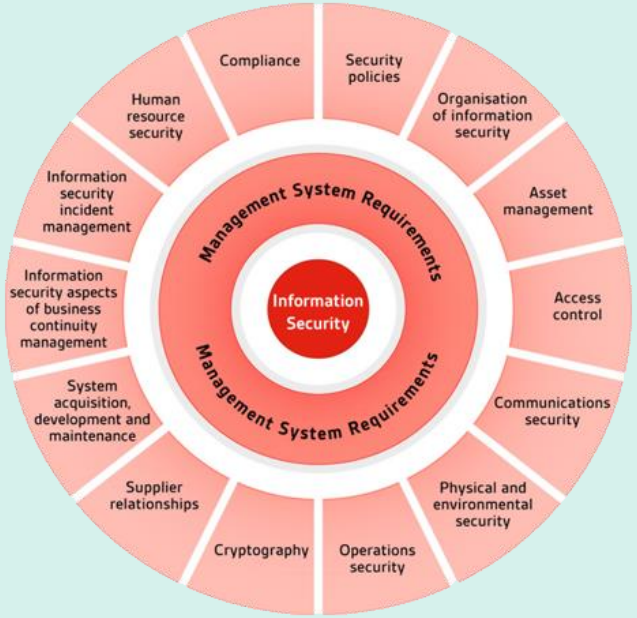
ISO/IEC 27001
Information Security Management System requirement

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



Information Security Control Annex A (A5-A18)

ISO/IEC 27002
Code of practice for information security controls
Information Security control
Practice
Requirement 5 – 18



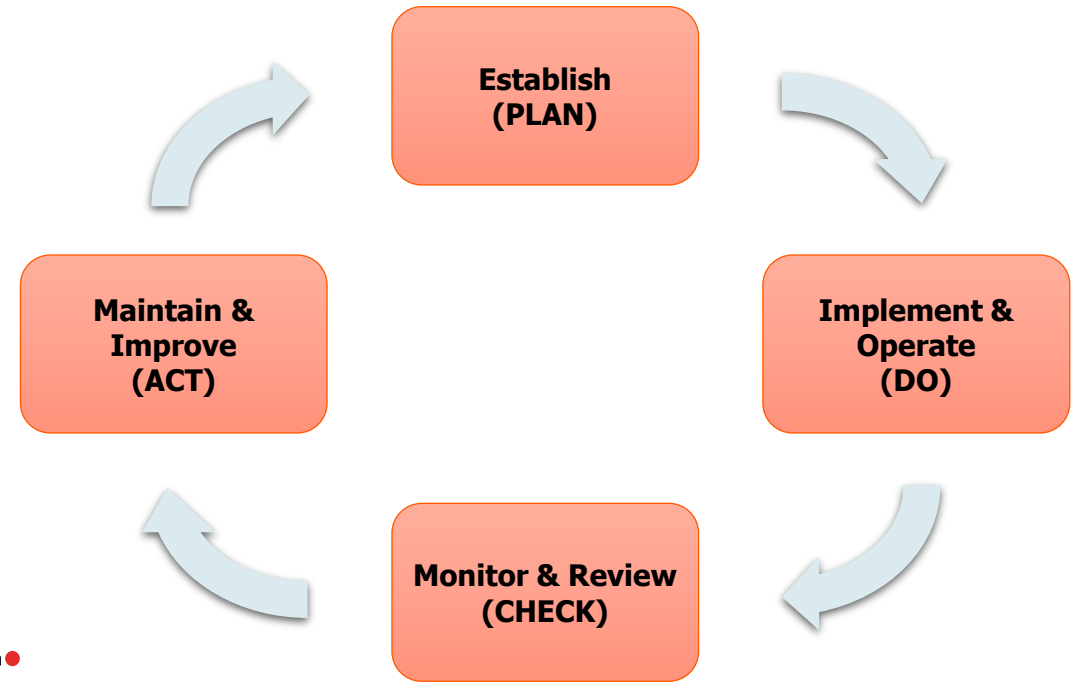
ISMS Requirement and PDCA Cycle

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

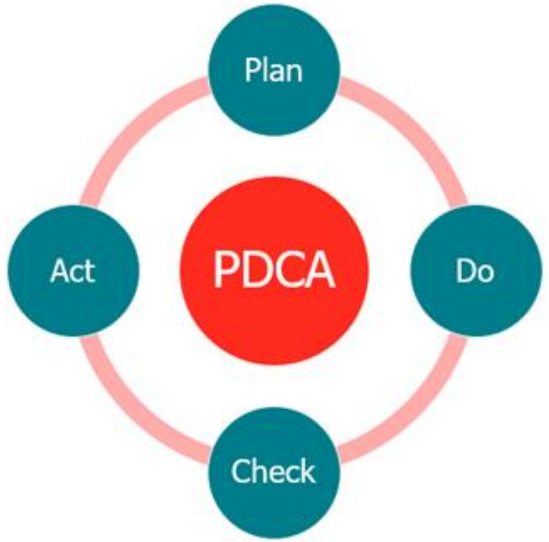
ACT

- 10 Improvement

bsi.

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

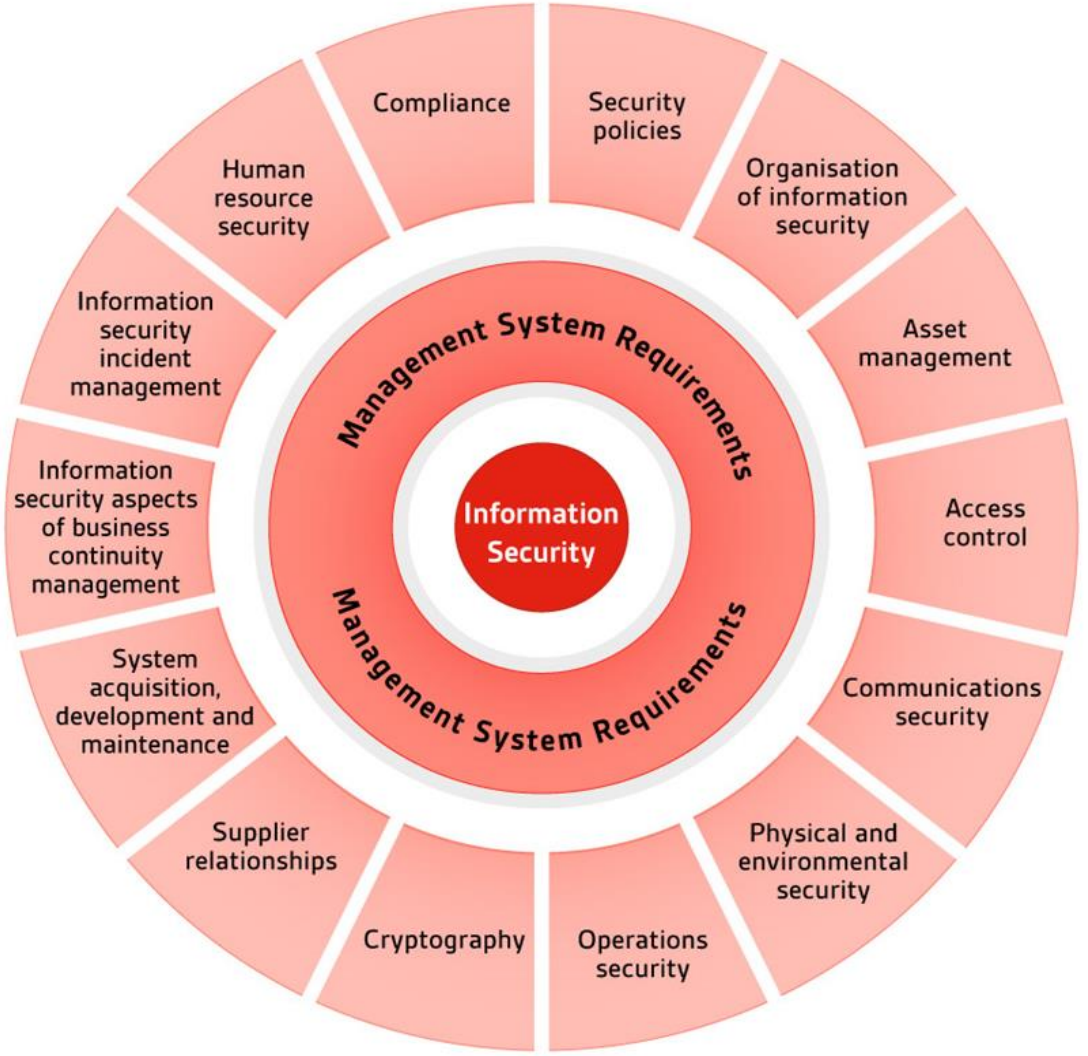


bsi.

Annex A

14 security clause headings (A5 – A18)

114 controls

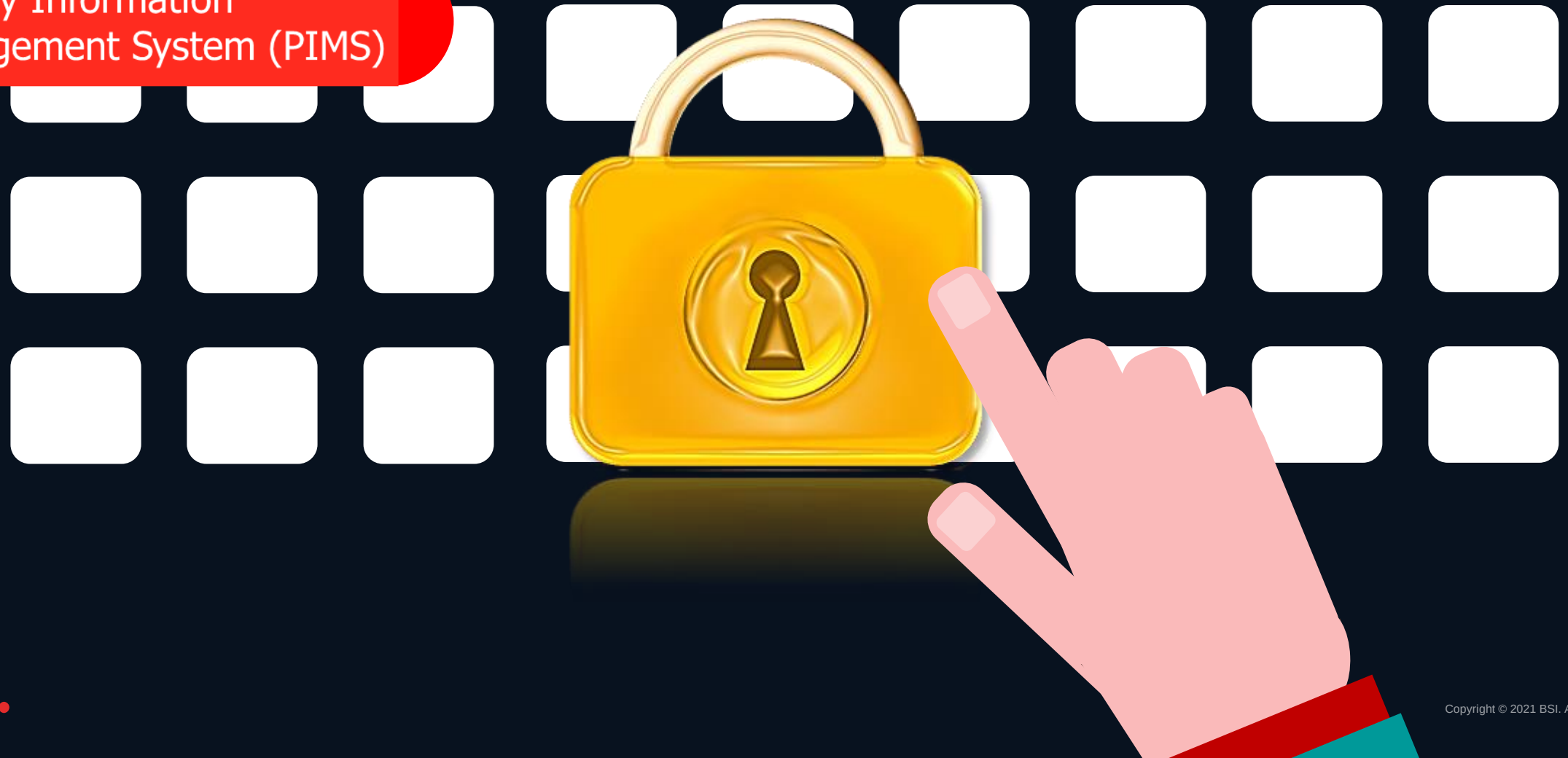


ISO/IEC 27001 (Information Security Management System (ISMS)

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

ภาพรวมมาตรฐาน ISO/IEC 27701

Privacy Information Management System (PIMS)



bsi.

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

bsi.

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

bsi.

Thank you

Summary

Q & A

Further Information & Support

Address: BSI Group (Thailand) Co., Ltd.

127/29 Panjathani Tower, 24th Fl. Nonsee Road, Chongnonsee, Yannawa, Bangkok 10120

Tel: 02 294 4889-92

Fax: 02 294 4467

Email: infothai@bsigroup.com

Website: www.bsigroup.com/en-th