ข้อกำหนดISO/IEC 27002 ฉบับใหม่ กับการเตรียมการรับการปรับเปลี่ยน ISO/IEC 27001

โดย สถาบันมาตรฐานอังกฤษ

Kittipong Keatniyomrung

สถาบันมาตรฐานอังกฤษ / BSI Group Thailand

2022/01/17

By Royal Charter

bsi.

หัวข้อการพูดคุย

- โครงสร้างข้อกำหนด ISO/IEC 27002
- สรุปข้อกำหนด ISO/IEC 27002
- ผลกระทบของการเปลี่ยนแปลง ISO/IEC 27002 ต่อ ISO/IEC 27001
- สิ่งที่ต้องเตรียมปรับเปลี่ยน ISO/IEC 27001

โครงสร้างข้อกำหนด ISO/IEC 27002

โครงสร้างข้อกำหนด ISO/IEC 27002

Contents

bsi.

โครงสร้างข้อกำหนด ISO/IEC 27002

5. Organizational controls

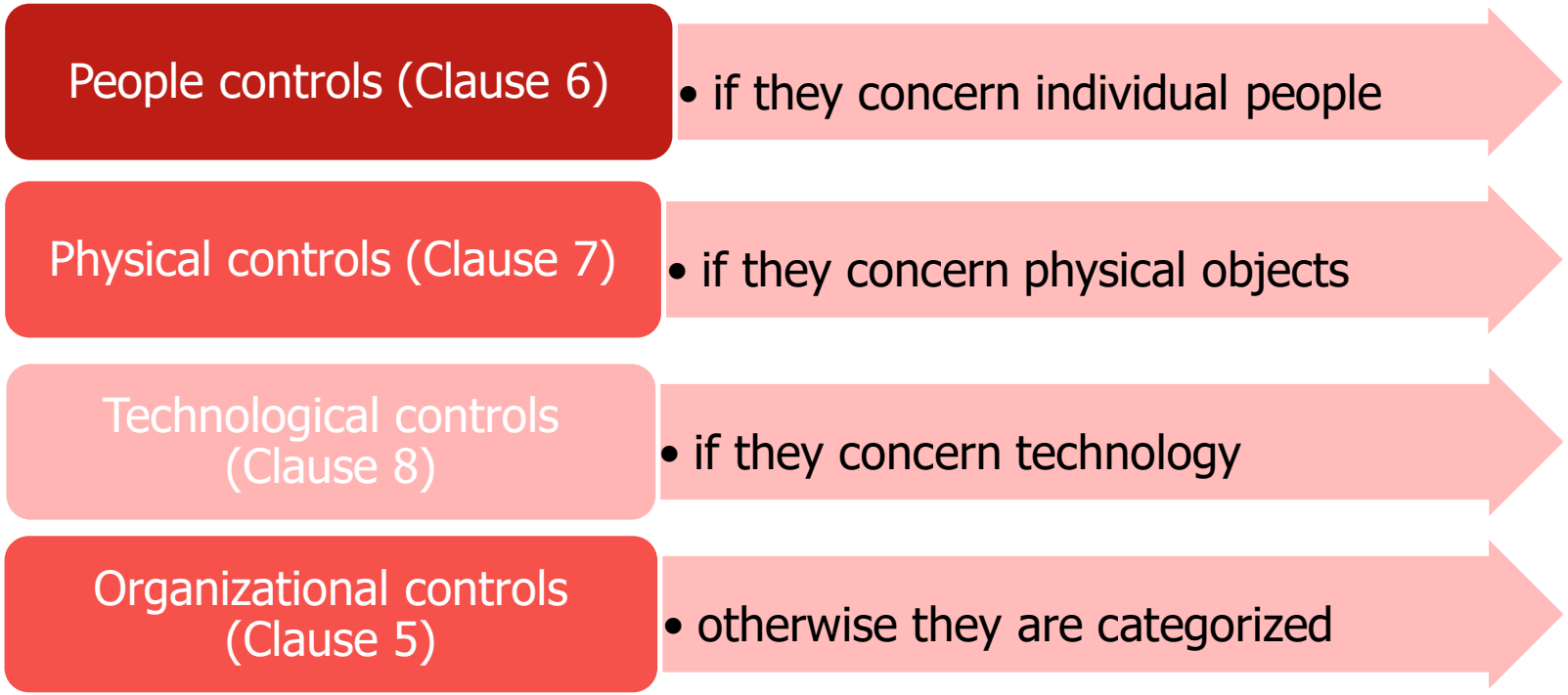
6. People controls

7. Physical controls

8. Technological controls

Summary Structure

- 4 Pillars :



สรุปข้อกำหนด ISO/IEC 27002

By Royal Charter

bsi.

5. Organizational controls

No.	Control Title
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

No.	Control Title
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

bsi.

5. Organizational controls

No.	Control Title
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

No.	Control Title
5.30	ICT readiness for business continuity
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	Conformance with policies, rules and standards for information security
5.37	Documented operating procedures

bsi.

6. People controls

No.	Control Title
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

7. Physical controls

No.	Control Title
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

No.	Control Title
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

bsi.

8. Technological controls

No.	Control Title
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

No.	Control Title
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
8.17	Clock synchronization
8.18	Use of privileged utility programs
8.19	Installation of software on operational systems
8.20	Networks security

bsi.

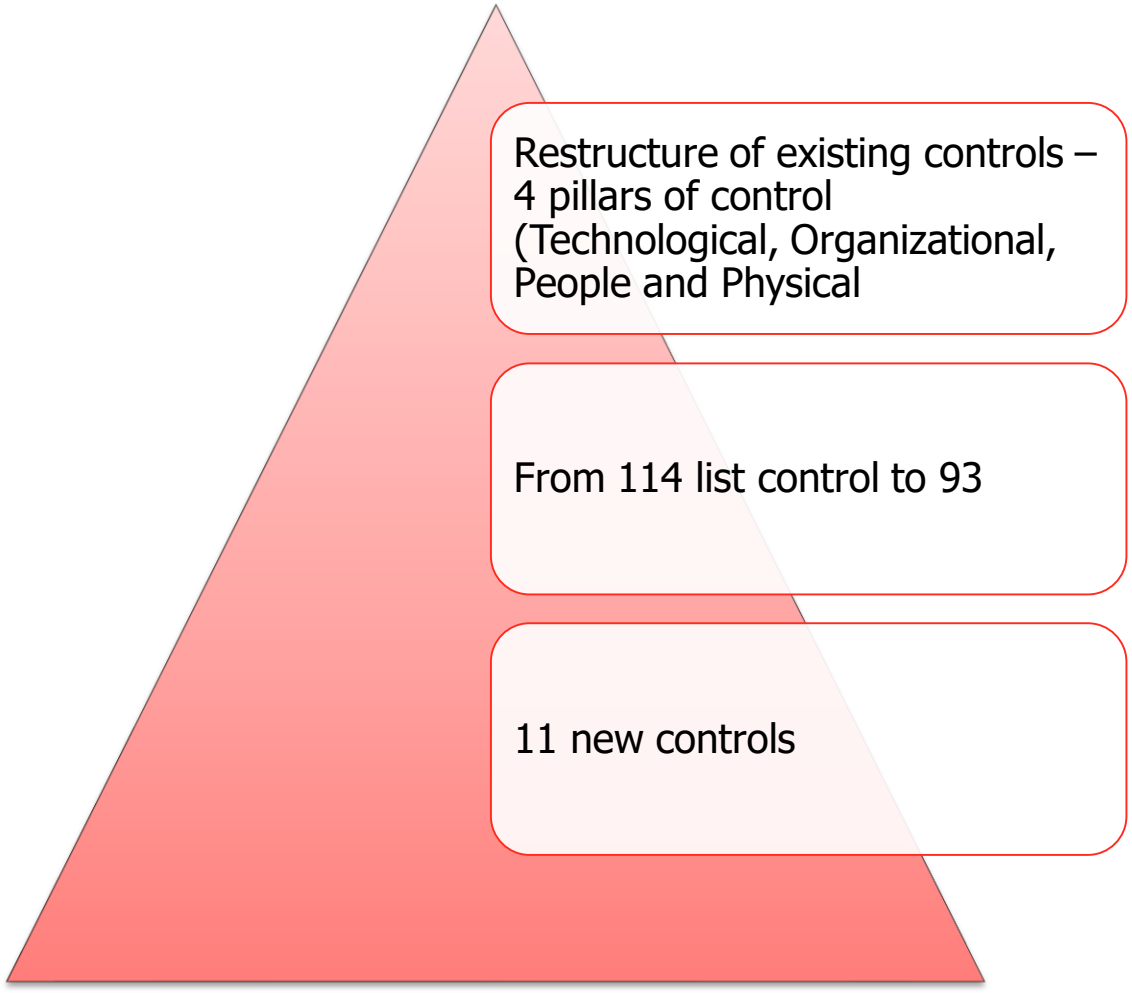
8 Technological controls

No.	Control Title
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

No.	Control Title
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

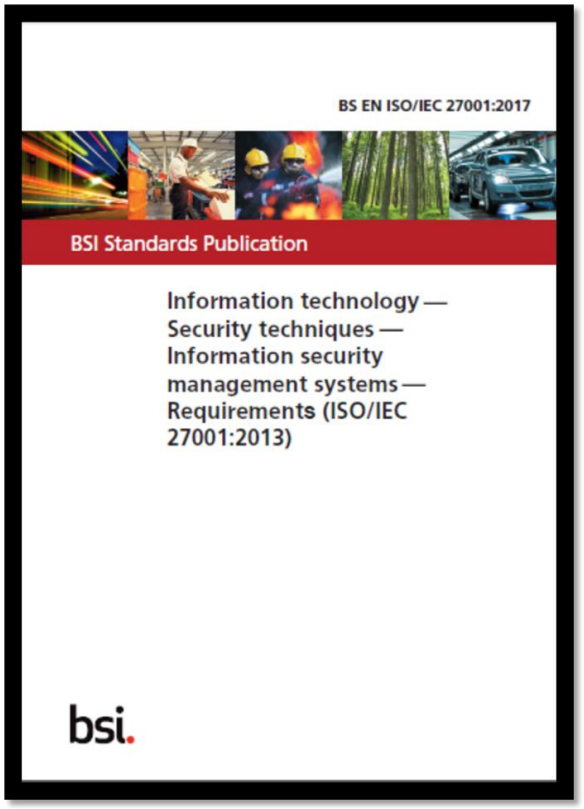
bsi.

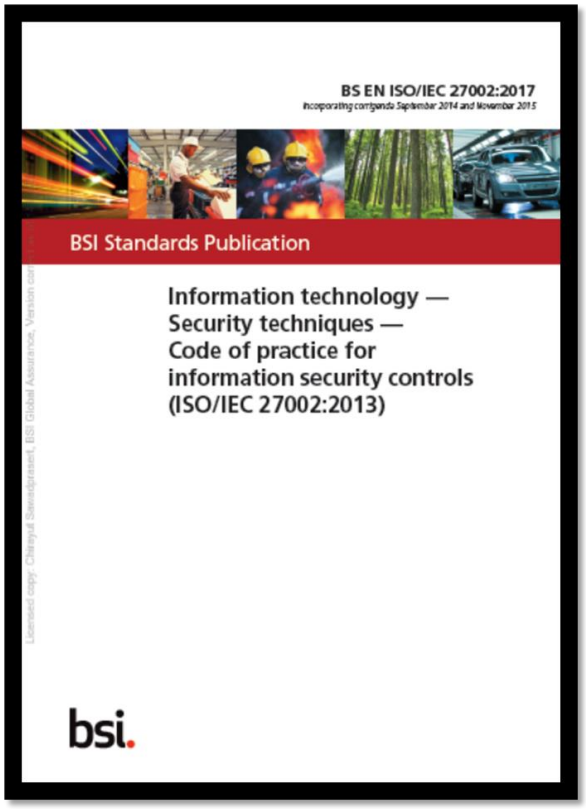
Summary changes ISO/IEC 27002



ผลกระทบของการเปลี่ยนแปลง ISO/IEC 27002 ต่อ ISO/IEC 27001

ผลกระทบของการเปลี่ยนแปลง ISO/IEC 27002 ต่อ ISO/IEC 27001





ผลกระทบของการเปลี่ยนแปลง ISO/IEC 27002 ต่อ ISO/IEC 27001

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

Changed

ISO/IEC 27002
Code of practice for information security controls

Version 2022

Changed in Security control

ผลกระทบของการเปลี่ยนแปลง ISO/IEC 27002 ต่อ ISO/IEC 27001

O/IEC 27002 วางแผนว่าจะออกอย่างเป็นทางการ ประมาณเดือน มกราคม/กุมภาพันธ์ 2022 (2565)

ISO/IEC 27001 วางแผนว่าปรับเปลี่ยนต้นปี 2022 (2565) โดยอาจจะปรับเปลี่ยนในส่วน Annex A (Information Security control) เพื่อสอดรับกับ ISO27002 ที่กำลังจะประกาศ

หลังจากนั้น มาตราฐานอื่นๆ ที่มีการอ้างอิง ISO/IEC 27002 จะมีการปรับเปลี่ยน ตามมาเช่น ISO/IEC 27799, ISO/IEC 27017, ISO/IEC 27018, ฯลฯ

bsi.

สิ่งที่ต้องเตรียมปรับเปลี่ยน
ISO/IEC 27001

By Royal Charter

bsi.

สิ่งที่ต้องเตรียมปรับเปลี่ยน ISO/IEC 27001

- ศึกษาทำความเข้าใจ ข้อกำหนด ISO/IEC 27002 version 2022
- ทบวนการประมินความเสี่ยงให้ครอบคลุมในประเด็นต่างๆ
- ทบทวน security control ที่มีอยู่ปัจจุบันและในอนาคตเพื่อครอบคลุม ISO/IEC 27002 version 2022
- ทบทวนปรับปรุง Statement Of Applicability (SOA) เพื่อสอดรับกับ security control ใหม่ที่จะถูกปรับเปลี่ยนตาม ISO/IEC 27002 version 2022
- Implement Security control ตามที่กำหนดใน Statement Of Applicability (SOA)

หากมีข้อสงสัยต่างๆ ติดต่อ Technical Team ของ BSI

bsi.

By Royal Charter

bsi.

Contact Information

Address: BSI Group (Thailand) Co., Ltd.
127/25 Panjathani Tower, 24th Fl.
Nonsee Road, Chongnonsee, Yannawa, Bangkok 10120
Tel: 02 294 4889-92
Fax: 02 294 4467
Email: infothai@bsigroup.com
Web: www.bsigroup.com/en-th

By Royal Charter

bsi.