ส่องข้อกำหนดมีอะไรใหม่ใน ISO/IEC 27002:2022

โดย สถาบันมาตรฐานอังกฤษ

bsi.

หัวข้อการพูดคุย

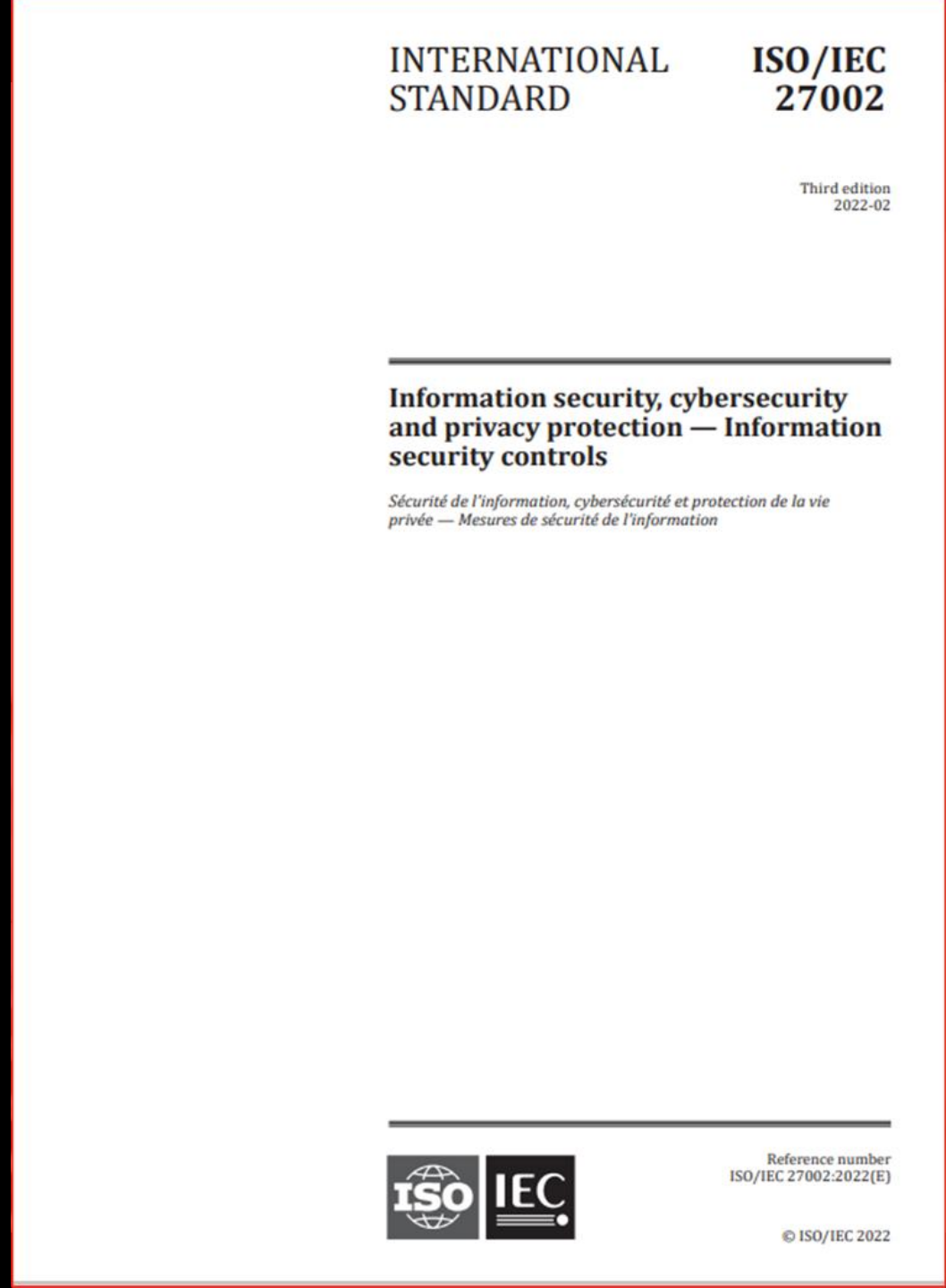
- Overview ISO/IEC 27002:2022
- ข้อกำหนดใหม่ ใน ISO/IEC 27002:2022
- ผลกระทบของการเปลี่ยนแปลง ISO/IEC 27002:2022 ต่อการขอการรับรอง ISO/IEC 27001

bsi.

ISO/IEC 27002:2022

Information security, cybersecurity and privacy protection — Information security controls

By Royal Charter



Module 1: ISO 27002:2022 overview

ISO 27002:2022 Title and scope

ISO 27002:2022 clauses

Clause 5 - Organizational controls
37 controls, 34 existing, 3 new

Clause 6 - People controls
8 controls, all existing

Clause 7 - Physical controls
14 controls, 13 existing, 1 new

Clause 8 - Technological controls
34 controls, 27 existing, 7 new

bsi.

Control structure

- Addition of selectable and searchable attributes
- Attributes are not mandatory
- An organization may create their own attributes to meet their needs
- Purpose replaces control objectives

New controls (11)

Control Identifier	Control Name
5.7	Threat intelligence
5.23	Information security for use of cloud services
5.30	ICT readiness for business continuity
7.4	Physical security monitoring
8.9	Configuration management
8.10	Information deletion
8.11	Data masking
8.12	Data leakage prevention
8.16	Monitoring activities
8.23	Web filtering
8.28	Secure coding

Updated controls (58)

- 58 updated controls
- Majority of existing controls remain relevant
- Many needed updating to reflect latest best practices and removal of obsolete technologies
- Link between corresponding control numbers

ISO/IEC 27002:2013	ISO/IEC 27002:2022	ISO/IEC 27001:2013	ISO/IEC 27002:2022	ISO/IEC 27001:2013	ISO/IEC 27002:2022
06.1.1	5.02	18.2.1	5.35	09.2.3	8.02
06.1.2	5.03	12.1.1	5.37	09.4.1	8.03
07.2.1	5.04	07.1.1	6.01	09.4.5	8.04
06.1.3	5.05	07.1.2	6.02	09.4.2	8.05
06.1.4	5.06	07.2.2	6.03	12.1.3	8.06
08.1.4	5.11	07.2.3	6.04	12.2.1	8.07
08.2.1	5.12	07.3.1	6.05	12.3.1	8.13
08.2.2	5.13	13.2.4	6.06	17.2.1	8.14
09.2.1	5.16	06.2.2	6.07	12.4.4	8.17
15.1.1	5.19	11.1.1	7.01	09.4.4	8.18
15.1.2	5.20	11.1.3	7.03	13.1.1	8.20
15.1.3	5.21	11.1.4	7.05	13.1.2	8.21
16.1.1	5.24	11.1.5	7.06	13.1.3	8.22
16.1.4	5.25	11.2.9	7.07	14.2.1	8.25
16.1.5	5.26	11.2.1	7.08	14.2.5	8.27
16.1.6	5.27	11.2.6	7.09	14.2.7	8.30
16.1.7	5.28	11.2.2	7.11	14.3.1	8.33
18.1.2	5.32	11.2.3	7.12	12.7.1	8.34
18.1.3	5.33	11.2.4	7.13		
18.1.4	5.34	11.2.7	7.14		

bsi.

Merged controls (24)

- 24 merged controls
- Merged where existing controls are inseparable or closely related

ISO/IEC 27002:2013	ISO/IEC 27002:2022	ISO/IEC 27002:2013	ISO/IEC 27002:2022
05.1.1, 05.1.2	5.01	16.1.2, 16.1.3	6.08
06.1.5, 14.1.1	5.08	11.1.2, 11.1.6	7.02
08.1.1, 08.1.2	5.09	08.3.1, 08.3.2, 08.3.3, 11.2.5	7.10
08.1.3, 08.2.3	5.10	06.2.1, 11.2.8	8.01
13.2.1, 13,2,2, 13.3.3	5.14	12.6.1, 18.2.3	8.08
09.1.1, 09.2.2	5.15	12.4.1, 12.4.2, 12.4.3	8.15
09.2.4, 09.2.5, 09.2.6	5.17	12.5.1, 12.6.2	8.19
09.2.2, 09.2.5, 09.2.6	5.18	10.1.1, 10.1.2	8.24
15.1.1, 15.1.2	5.22	14.1.2, 14.1.3	8.26
17.1.1, 17.1.2, 17.1.3	5.29	14.2.8, 14.2.9	8.29
18.1.1, 18.1.5	5.31	12.1.4, 12.2.6	8.31
18.2.2, 18.2.3	5.36	12.1.2, 14.2.2, 14.2.3, 14.2.4	8.32

Control correspondence

Table B.1

ISO/IEC 27002 control identifier	ISO/IEC 27002:2013 control identifier	Control name
5.1	05.1.1, 05.1.2	Policies for information security

Table B.2

ISO/IEC 27002:2013 control identifier	ISO/IEC 27002 control identi	Control name
5		Information security policies
5.1		Management direction for information security
5.1.1	5.1	Policies for information security

Control attributes

Control attributes	Attribute values
Control type	#Prevenative, #Detective, #Corrective
Information security property	#Confidentiality, #Intergrity, #Availability
Cybersecurity concepts	#Identify, #Protect, #Detect, #Respond, #Recover
Operational capabilities	#Governance, #Asset_management, #Information_protection, #Human_resource_security, #Physical_security, #System_and_network_security, #Application_security, #Secure_configuration, #Identity_and_access_management, #Threat_and_vulnerability_management, #Continuity, #Supplier_relationships_security, #Legal_and_compliance, #Information_security_event_management, #Information_security_assurance
Security domains	#Governance_and_Ecosystem, #Protection, #Defence, #Resilience

Control type

#Preventive

#Detective

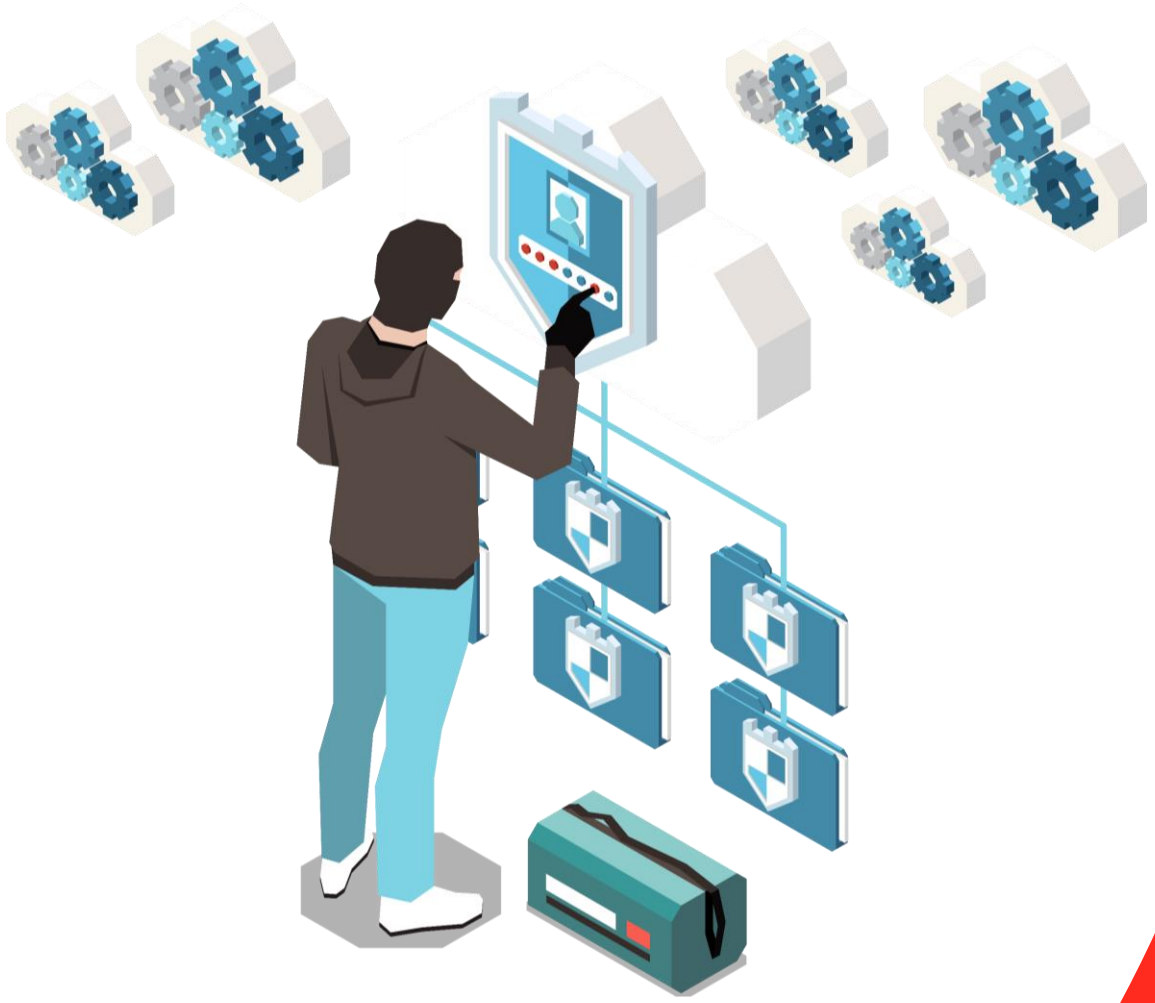
#Corrective

Information security properties

#Confidentiality

#Integrity

#Availability



ISO/IEC TS 27110:

#Identify

#Protect

#Detect

#Respond

#Recover

Operational capabilities

#Governance

#Asset_management

#Information_protection

#Human_resource_security

#Physical_security

#System_and_network security

#Application_security

#Secure_configuration

#Identity_and_access management

#Threat_and_vulnerability management

#Continuity

#Supplier_relationships _security

#Legal_and_compliance

#Information_security_ event_management

#Information_security _assurance

Security domains

- #Governance_and_ecosystem
- #Protection
- #Defence
- #Resilience

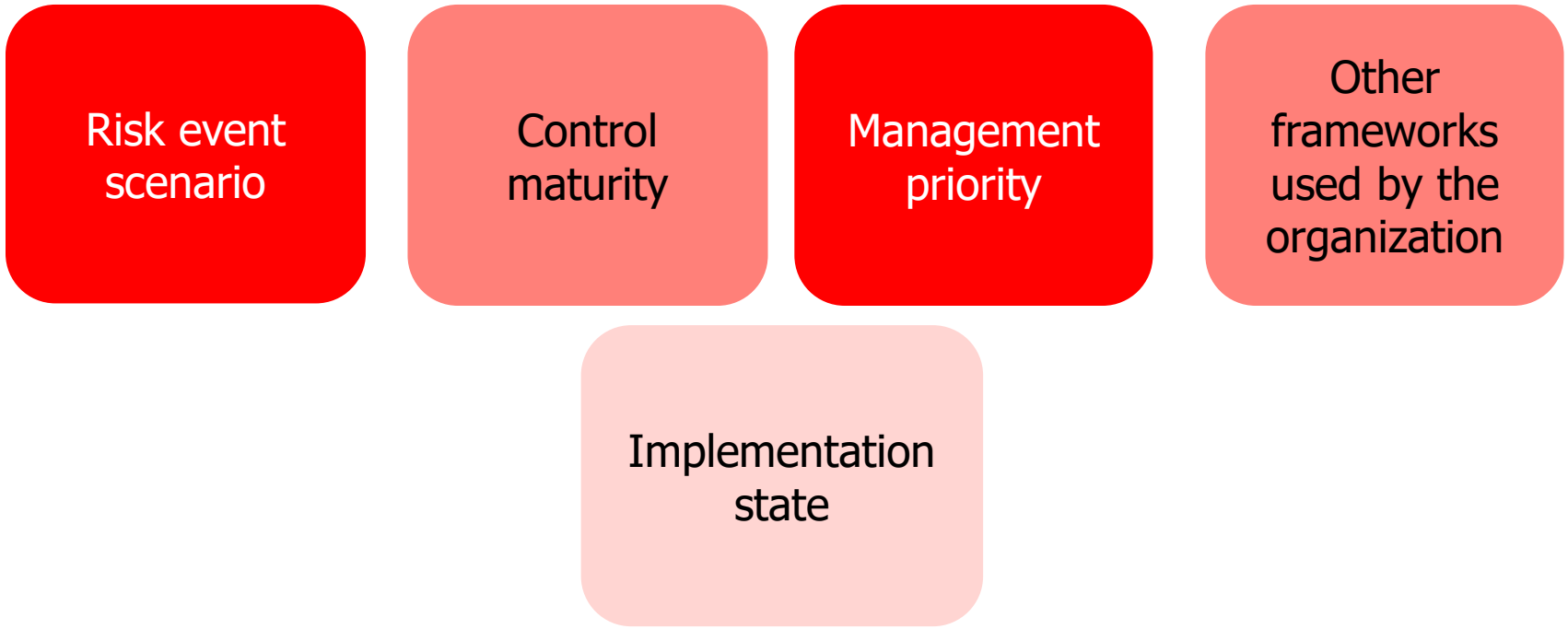
Control layout

5.1 Policies for information security

Control Type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
Preventative	Confidentiality Integrity Availability	Identify	Governance	Governance and Ecosystem Resilience

- Control
- Purpose
- Guidance
- Other information

Organizational attributes



Module 2: Clause 5 controls

Clause 5 - Organizational controls

37 controls, 34 existing, 3 new

5.7 – Threat intelligence

5.23 – Information security for use on cloud services

5.30 – ICT readiness for business continuity

Clause 5.7 Threat intelligence

- Layered threat intelligence
- Intelligence should be relevant, insightful, contextual and actionable
- Establish activities to identify, vet, select, collect, process, analyse and communicate relevant information
- Consider internal and external threats

Clause 5.23 Information security for use of cloud services

Establish processes for acquisition, use management and exit from cloud services

Establish and communicate a topic-specific policy

Identify all information security requirements

Responsibilities of the cloud service provider vs the organization

Manage information security risks in relation to cloud services

23

Clause 5.30 ICT readiness for business continuity

Business Impact Analysis (BIA) – process of analysing the impact over time of a disruption on the organization

Recovery Point Objective (RPO) – point to which information used by an activity is restored to enable the activity to operate on resumption

Recovery Time Objective (RTO) – period of time following an incident within which a product and service or an activity is resumed, or resources are recovered

Module 3: Clause 6 and Clause 7 controls

Clause 6 and Clause 7 controls

Clause 6 - People controls
8 controls, all existing

Clause 7 - Physical controls
14 controls, 13 existing, 1 new

Clause 7.4 – Physical security monitoring

Clause 6 and Clause 7 controls

Clause 6 - People controls
8 controls, all existing

Clause 7 - Physical controls
14 controls, 13 existing, 1 new

Clause 7.4 – Physical security monitoring

Module 4: Clause 8 controls

Clause 8 - Technological controls

34 controls, 27 existing, 7 new

8.9 – Configuration management

8.10 – Information deletion

8.11 – Data masking

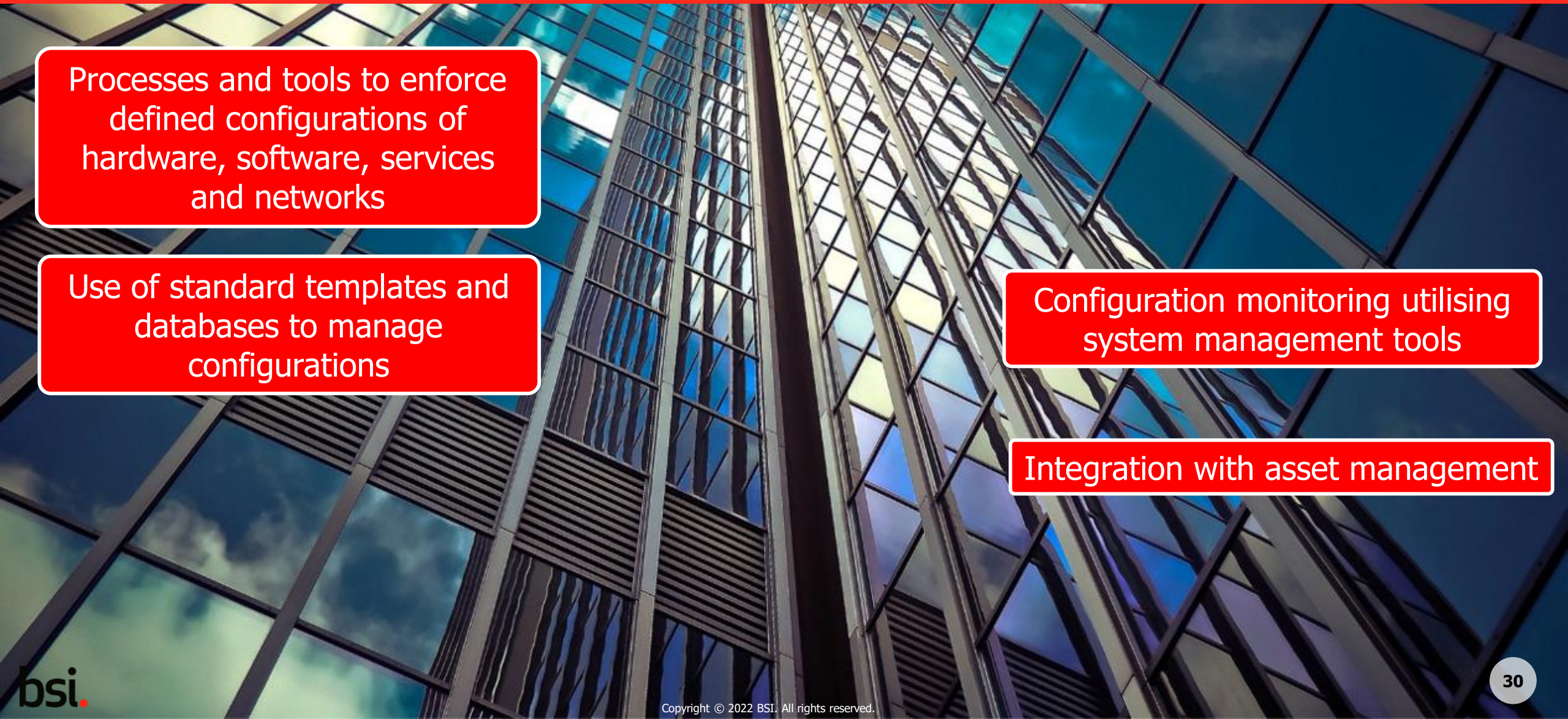
8.12 – Data leakage prevention

8.16 – Monitoring activities

8.23 – Web filtering

8.28 – Secure coding

Clause 8.9 Configuration management



Processes and tools to enforce defined configurations of hardware, software, services and networks

Use of standard templates and databases to manage configurations

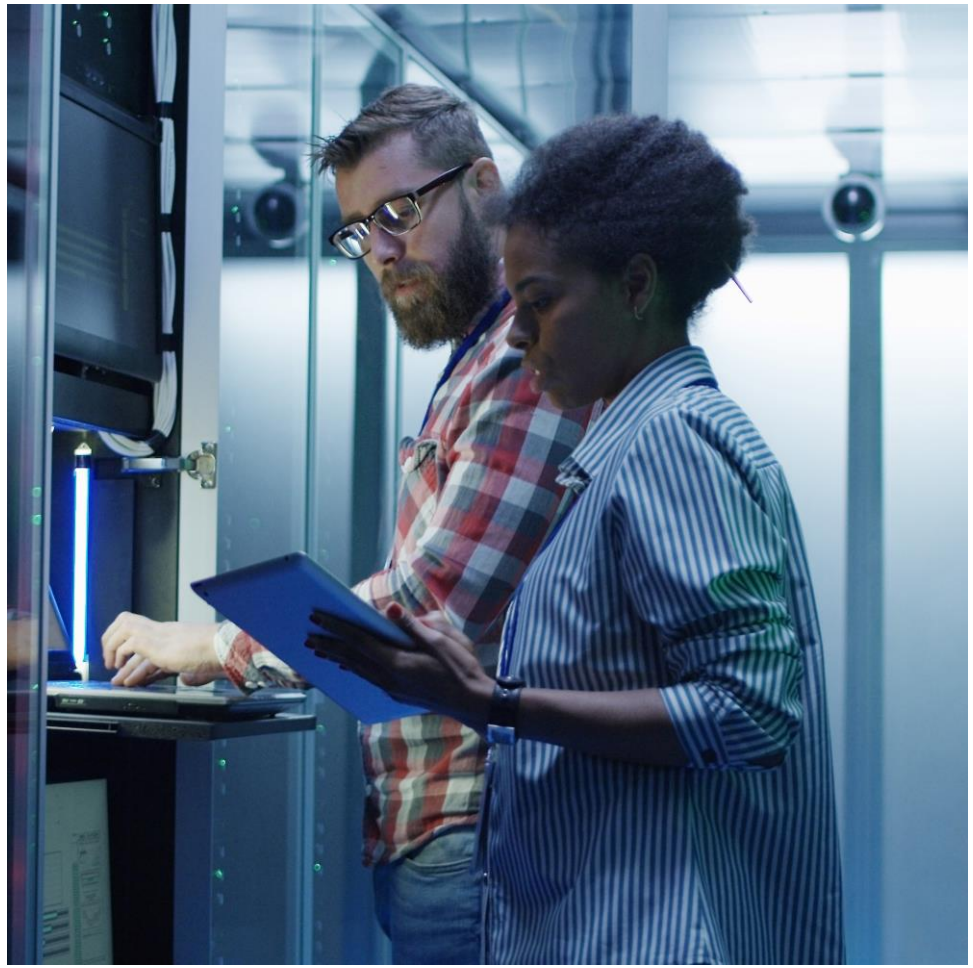
Configuration monitoring utilising system management tools

Integration with asset management

Configuration management					
Element	**CI**	**Not CI**	**Element**	**CI**	**Not CI**
Information			Vending machine		
Data centre			Software		
Head of IT			Databases		
IP addresses			Hardware		
Operating systems			Cloud-based servers		
Services			Call centre		

Clause 8.10 Information deletion

- Prevent unnecessary exposure of sensitive information
- Consider deletion methods
- Record deletion
- Consider third parties storing information on the organization’s behalf



Clause 8.11 data masking

Limit the exposure of sensitive data including PII

Consider the use of different data masking techniques to disguise the true data, including the identity of PII principals

Consider legal, regulatory and contractual obligations when considering techniques

bsi.

Masking Technique	Definition
Data Encryption	Data values are switched within the same dataset. Data is rearranged in each column using a random sequence
Data scrambling	Characters are reorganized in random order, replacing the original content
Nulling out	Make the information unclear or unintelligible
Value variance	Data values are substituted with fake, but realistic, alternative values
Data substitution	Irreversibly alters information in such a way that the subject can no longer be identified directly or indirectly
Data shuffling	Data appears missing when viewed by an unauthorized user
Pseudonymisation	The process of converting information into data or code
Anonymisation	Replaces the identifying information with an alias
Obfuscation	Original data values are replaced by a function, such as the difference between the lowest and highest value in a series

Clause 8.12 Date leakage prevention

Apply to systems, networks and any other devices that process, store or transmit sensitive information

Identify and classify the information, monitor channels and prevent information from leaking

Use data leakage prevention tools

What are you protecting the information against?

Clause 8.16 – Monitoring activities

- Monitor network systems and applications for anomalous behaviour and evaluate potential information security incidents
- Use monitoring tools for continuous monitoring
- Have the ability to adapt to differing threats
- Alert function capability to allow abnormal events to be communicated to relevant interested parties

Clause 8.23 – Web filtering

Protect systems being compromised by malware and access to unauthorized web resources

Identify types of websites personnel should or should not have access to

Establish rules for safe and appropriate use of online resources

Provide training to personnel on secure and appropriate use of online resources

Clause 8.28 – Secure coding

Ensure software is written securely to reduce potential information security vulnerabilities

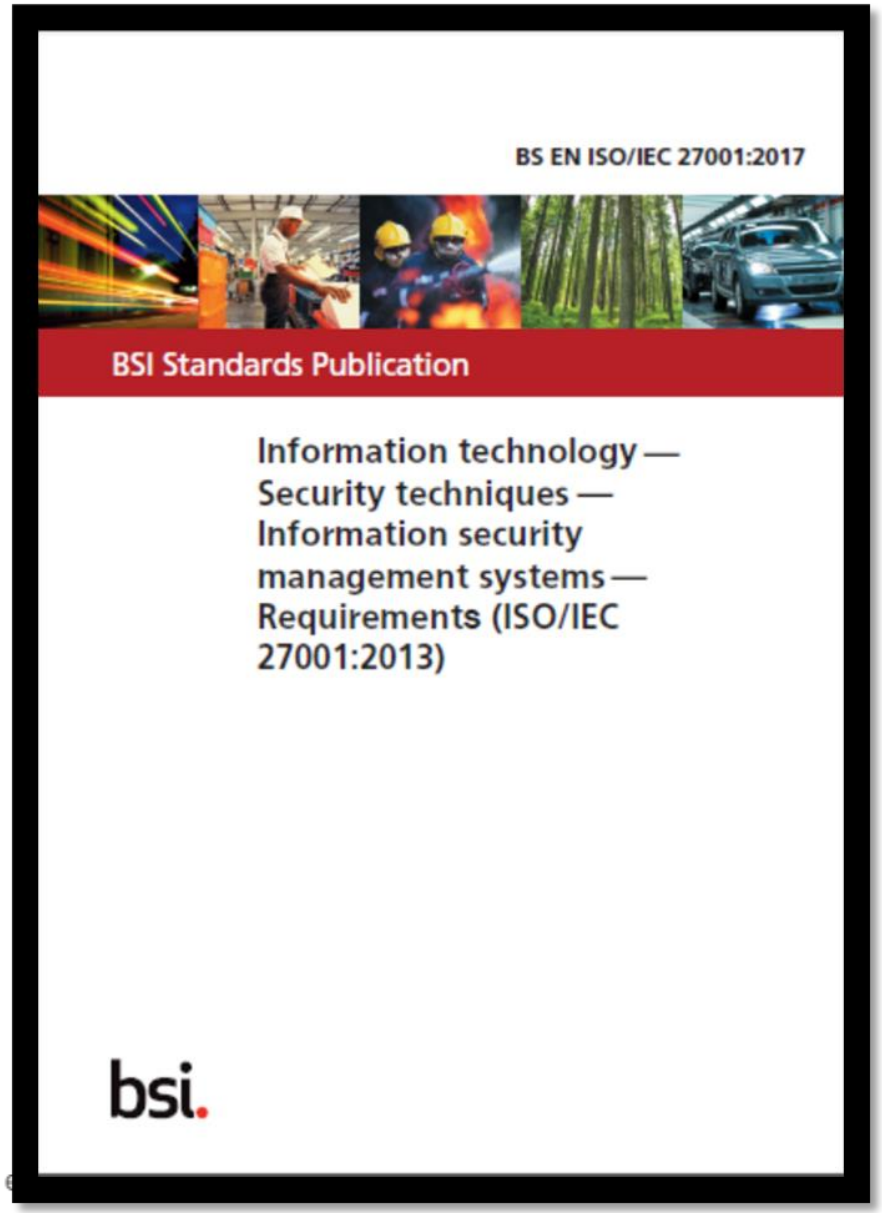
Establish a minimum secure baseline including third parties and open source software

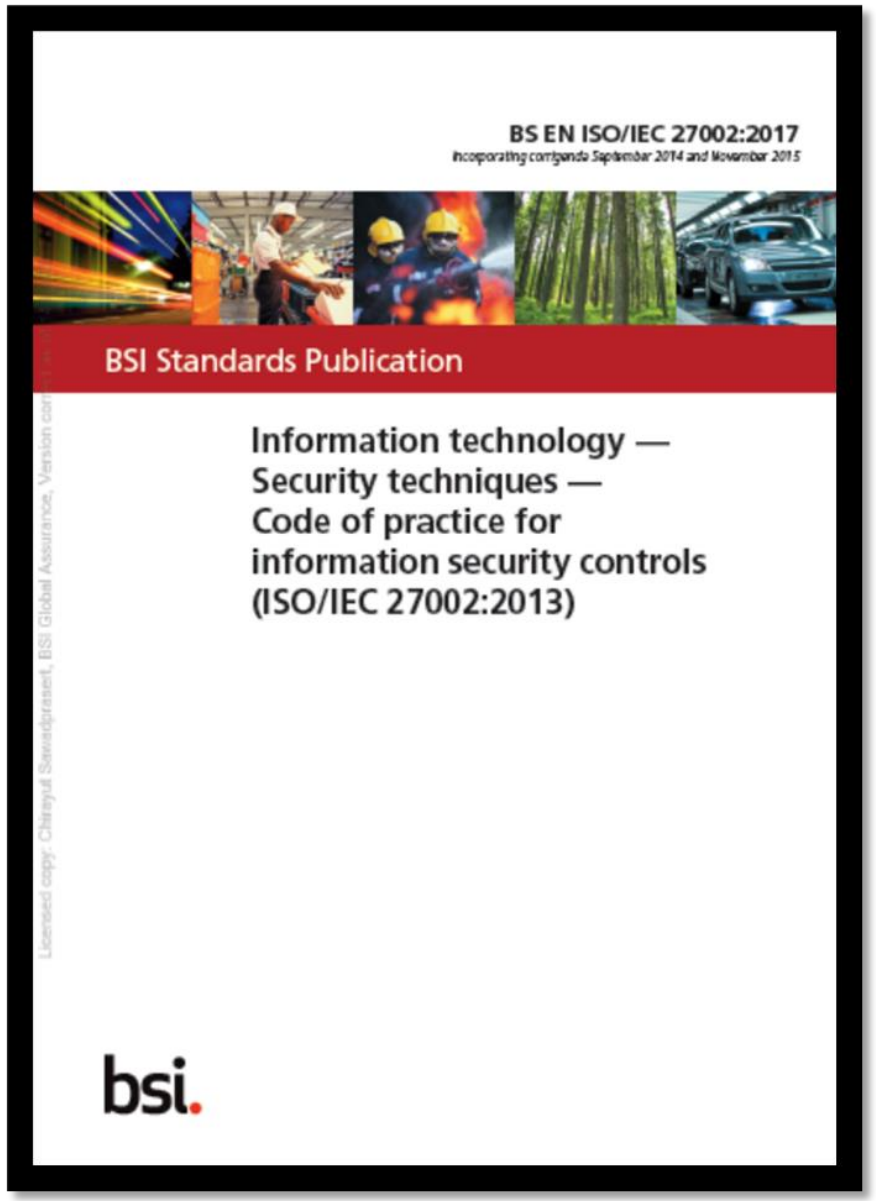
Keep up to date on real world software threats

Consider the whole coding lifecycle including reuse

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 และ มาตรฐานที่เกี่ยวข้อง

ISO/IEC 27002:2022 ออกอย่างเป็นทางการ กุมภาพันธ์ 2022 (2565)

ISO/IEC 27001 version Draft – มีการปรับปรุง notes supporting clause 6.1.3, และ ปรับปรุง Annex A ให้สอดคล้อง ISO/IEC 27002:2022

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

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.

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