การเตรียมพร้อม เพื่อปรับสู่ NEW Version ISO/IEC 27001:2022 (Check requirement ISO/IEC 27001:2022)

bsi Group (Thailand)

By Royal Charter

Discussion items

ภาพรวมการเปลี่ยนแปลง ข้อกำหนด ISO/IEC 27001:2022 (Requirement 4-10)

ภาพรวมการเปลี่ยนแปลง ข้อกำหนด ISO/IEC 27001:2022 (Security Control Annex A)

bsi.

ภาพรวมการเปลี่ยนแปลง ข้อกำหนด ISO/IEC 27001:2022 (Requirement 4-10)

ISO/IEC 27001:2022 change highlights

- 'International Standard' replaced with document throughout
- Re-arranging of some English to allow for easier translation
- Minor numbering re-structure to align with the harmonized approach
- Requirement to define your process needs and their interactions as part of your ISMS
- Explicit requirement to communicate organizational roles relevant to information security within in the organization

bsi.

ISO/IEC 27001:2022 change highlights

Removal of reference to control objectives as they no longer exist either in Annex A or ISO/IEC 27002

New requirement to monitor information security objectives

New Clause 6.3 – Planning of changes

New requirement to ensure the organization determines how to communicate as part of Clause 7.4

ISO/IEC 27001:2022 change highlights

New requirements to establish criteria for operational processes and implementing control of the processes

Internal audit and management review clauses aligned with harmonized approach

Clause 10.1 Continual Improvement and Clause 10.2 now nonconformity and corrective action but requirements remain the same

Clause 4.4

Confidentiality

Integrity

Availability

Effective implementation of the system

Internal audit

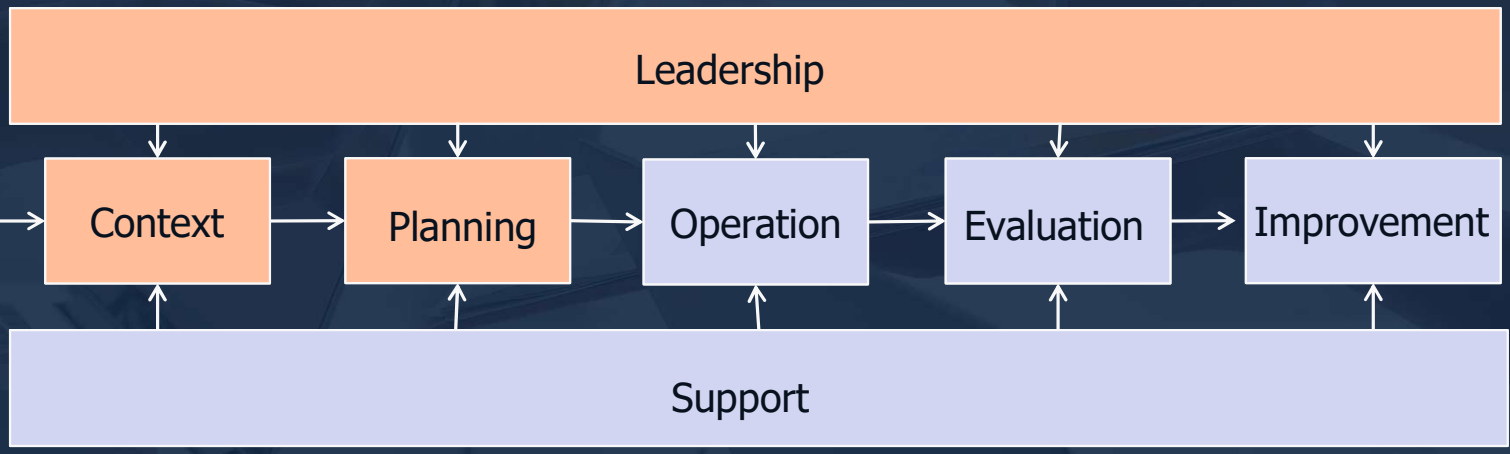
Management review

Clause 4.4

Intended outcomes

Strategic Direction

A **process** is a series of interrelating and interacting activities that use inputs to achieve an intended result



ภาพรวมการเปลี่ยนแปลง ข้อกำหนด ISO/IEC 27001:2022 (Security Control Annex A)

ISO/IEC 27001:2022 Annex A

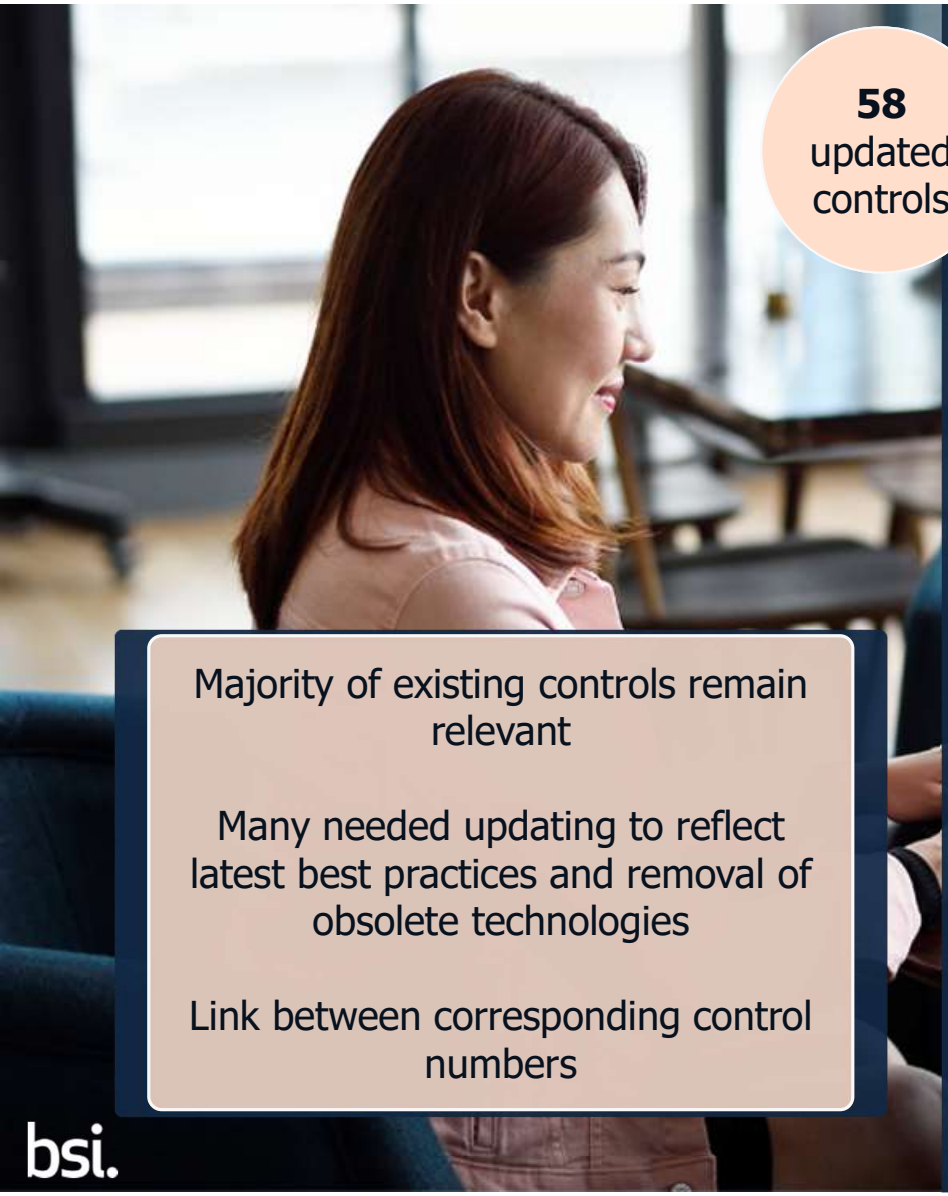
Clause 5	Organizational controls 37 controls, 34 existing, 3 new
Clause 7	Physical controls 14 controls, 13 existing, 1 new
Clause 6	People controls 8 controls, all existing
Clause 8	Technological controls 34 controls, 27 existing, 7 new

bsi.

New controls

11 new controls

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



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

Updated controls

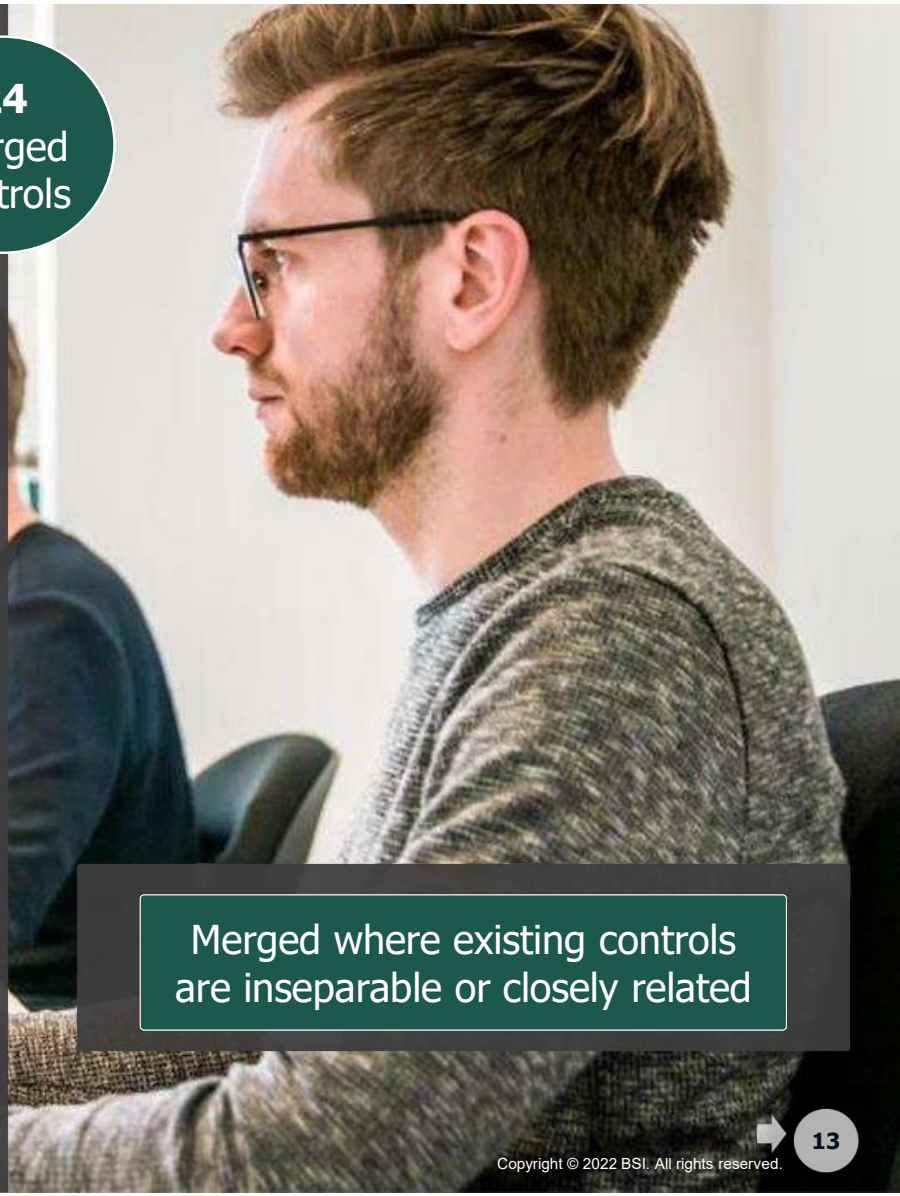
ISO/IEC 27001:2013	ISO/IEC 27001:2022	ISO/IEC 27001:2013	ISO/IEC 27001:2022	ISO/IEC 27001:2013	ISO/IEC 27001:2022
A6.1.1	A5.02	**A18.2.1**	A5.35	**A09.2.3**	A8.02
A6.1.2	A5.03	**A12.1.1**	A5.37	**A09.4.1**	A8.03
A7.2.1	A5.04	**A07.1.1**	A6.01	**A09.4.5**	A8.04
A6.1.3	A5.05	**A07.1.2**	A6.02	**A09.4.2**	A8.05
A6.1.4	A5.06	**A07.2.2**	A6.03	**A12.1.3**	A8.06
A8.1.4	A5.11	**A07.2.3**	A6.04	**A12.2.1**	A8.07
A8.2.1	A5.12	**A07.3.1**	A6.05	**A12.3.1**	A8.13
A8.2.2	A5.13	**A13.2.4**	A6.06	**A17.2.1**	A8.14
A9.2.1	A5.16	**A06.2.2**	A6.07	**A12.4.4**	A8.17
A15.1.1	A5.19	**A11.1.1**	A7.01	**A09.4.4**	A8.18
A15.1.2	A5.20	**A11.1.3**	A7.03	**A13.1.1**	A8.20
A15.1.3	A5.21	**A11.1.4**	A7.05	**A13.1.2**	A8.21
A16.1.1	A5.24	**A11.1.5**	A7.06	**A13.1.3**	A8.22
A16.1.4	A5.25	**A11.2.9**	A7.07	**A14.2.1**	A8.25
A16.1.5	A5.26	**A11.2.1**	A7.08	**A14.2.5**	A8.27
A16.1.6	A5.27	**A11.2.6**	A7.09	**A14.2.7**	A8.30
A16.1.7	A5.28	**A11.2.2**	A7.11	**A14.3.1**	A8.33
A18.1.2	A5.32	**A11.2.3**	A7.12	**A12.7.1**	A8.34
A18.1.3	A5.33	**A11.2.4**	A7.13		
A18.1.4	A5.34	**A11.2.7**	A7.14		

bsi.

Merged controls

24 merged controls

ISO/IEC 27001:2013	ISO/IEC 27001:2022	ISO/IEC 27001:2013	ISO/IEC 27001:2022
A05.1.1, A05.1.2	A5.01	**A16.1.2, A16.1.3**	A6.08
A06.1.5, A14.1.1	A5.08	**A11.1.2, A11.1.6**	A7.02
A08.1.1, A08.1.2	A5.09	**A08.3.1, A08.3.2, A08.3.3, A11.2.5**	A7.10
A08.1.3, A08.2.3	A5.10	**A06.2.1, A11.2.8**	A8.01
A13.2.1, A13,2,2, A13.3.3	A5.14	**A12.6.1, A18.2.3**	A8.08
A09.1.1, A09.2.2	A5.15	**A12.4.1, A12.4.2, A12.4.3**	A8.15
A09.2.4, A09.2.5, A09.2.6	A5.17	**A12.5.1, A12.6.2**	A8.19
A09.2.2, A09.2.5, A09.2.6	A5.18	**A10.1.1, A10.1.2**	A8.24
A15.1.1, A15.1.2	A5.22	**A14.1.2, A14.1.3**	A8.26
A17.1.1, A17.1.2, A17.1.3	A5.29	**A14.2.8, A14.2.9**	A8.29
A18.1.1, A18.1.5	A5.31	**A12.1.4, A12.2.6**	A8.31
A18.2.2, A18.2.3	A5.36	**A12.1.2, A14.2.2, A14.2.3, A14.2.4**	A8.32



Merged where existing controls are inseparable or closely related

bsi.

Control structure – ISO/IEC 27002:2022

Not mandatory within the document

Addition of five selectable and searchable attributes

An organization may create their own attributes to meet their needs

Purpose replaces control objectives

Control attributes

Five control attributes	Attribute values
Control type	#Preventative, #Detective, #Corrective
Information security property	#Confidentiality, #Integrity, #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

Understanding changes to Annex A Clauses 5 to 7

Clause 5 – Organizational controls

37 controls: 34 existing and 3 new

- 5.7 Threat intelligence
- 5.23 Information security for use on cloud services
- 5.30 ICT readiness for business continuity

bsi.

Control A.5.7 threat intelligence

Collected intelligence

- Strategic
- Operational
- Tactical

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

bsi.

Control A.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

Control A.5.30 ICT readiness for business continuity

Business Impact Analysis (BIA)

Process of analysing the impact over time of a disruption on the organization

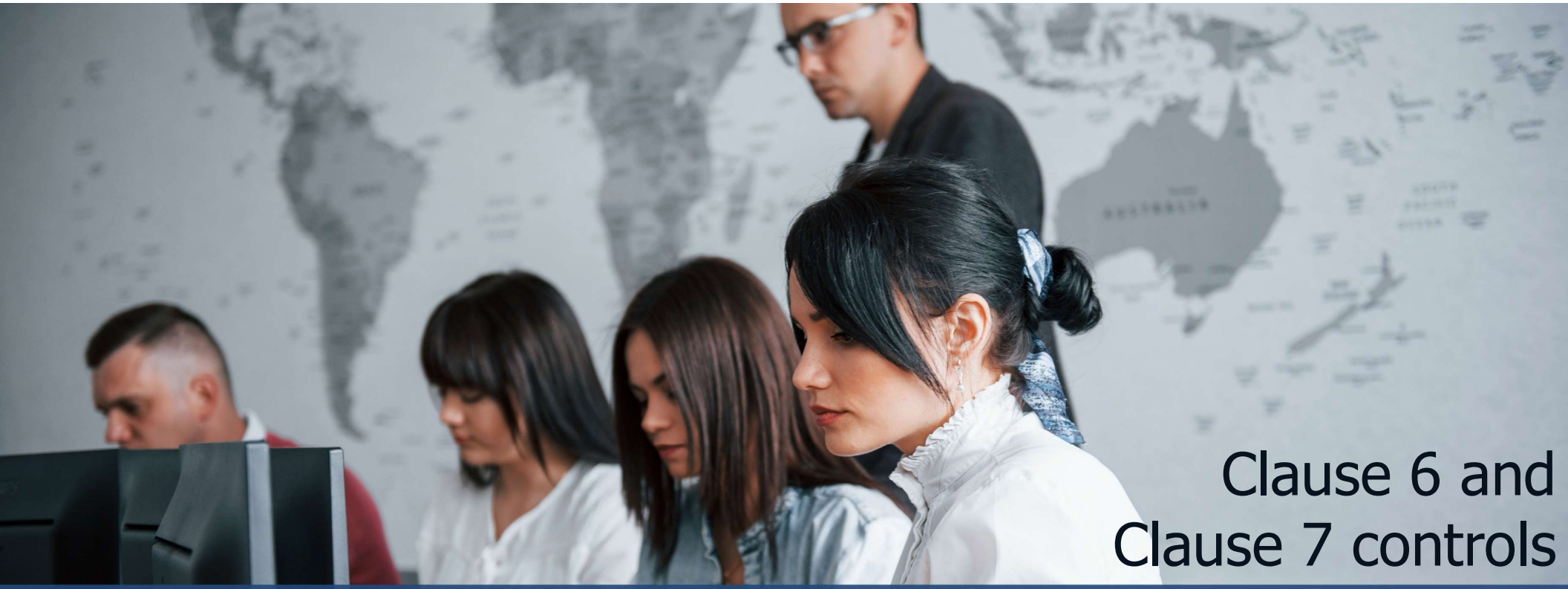
Recovery Point Objective (RPO)

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

bsi.



Clause 6 and Clause 7 controls

Clause 6 - People controls
8 controls, all existing

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

→

Control A.7.4 - Physical security monitoring

bsi.

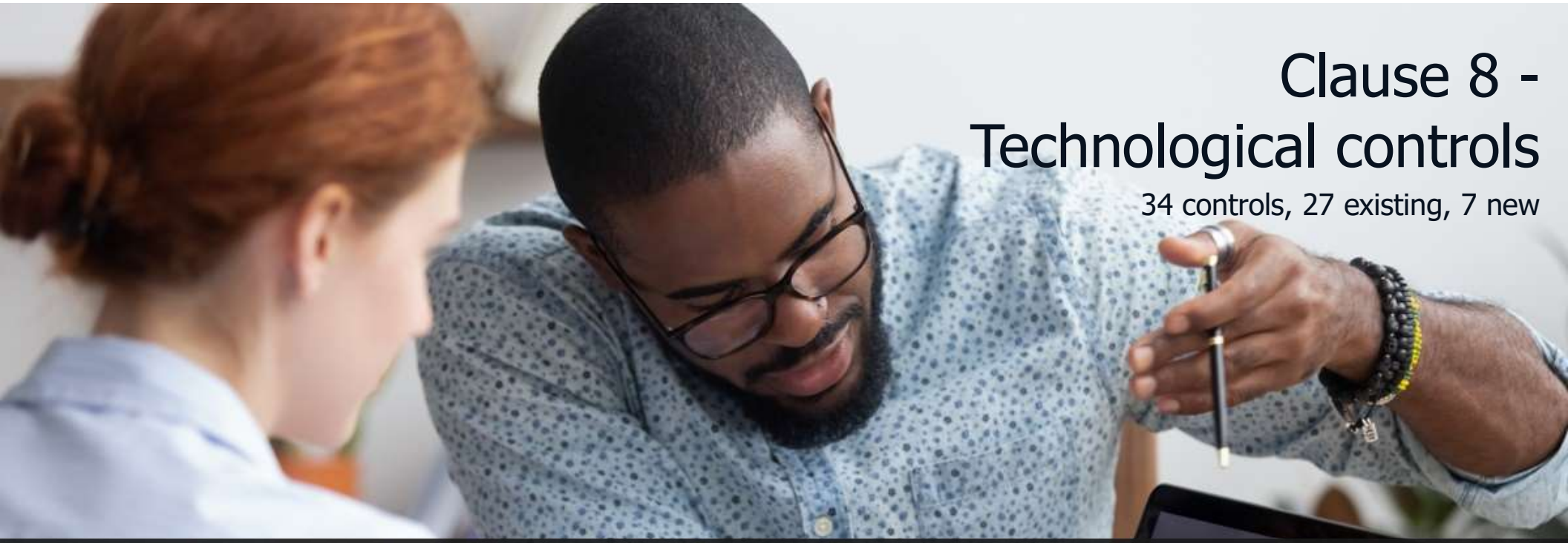
Clause 6 and Clause 7 controls

Clause 6 - People controls
8 controls, all existing

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

Control A.7.4 - Physical security monitoring

Understanding changes to Annex A Clause 8



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

bsi.

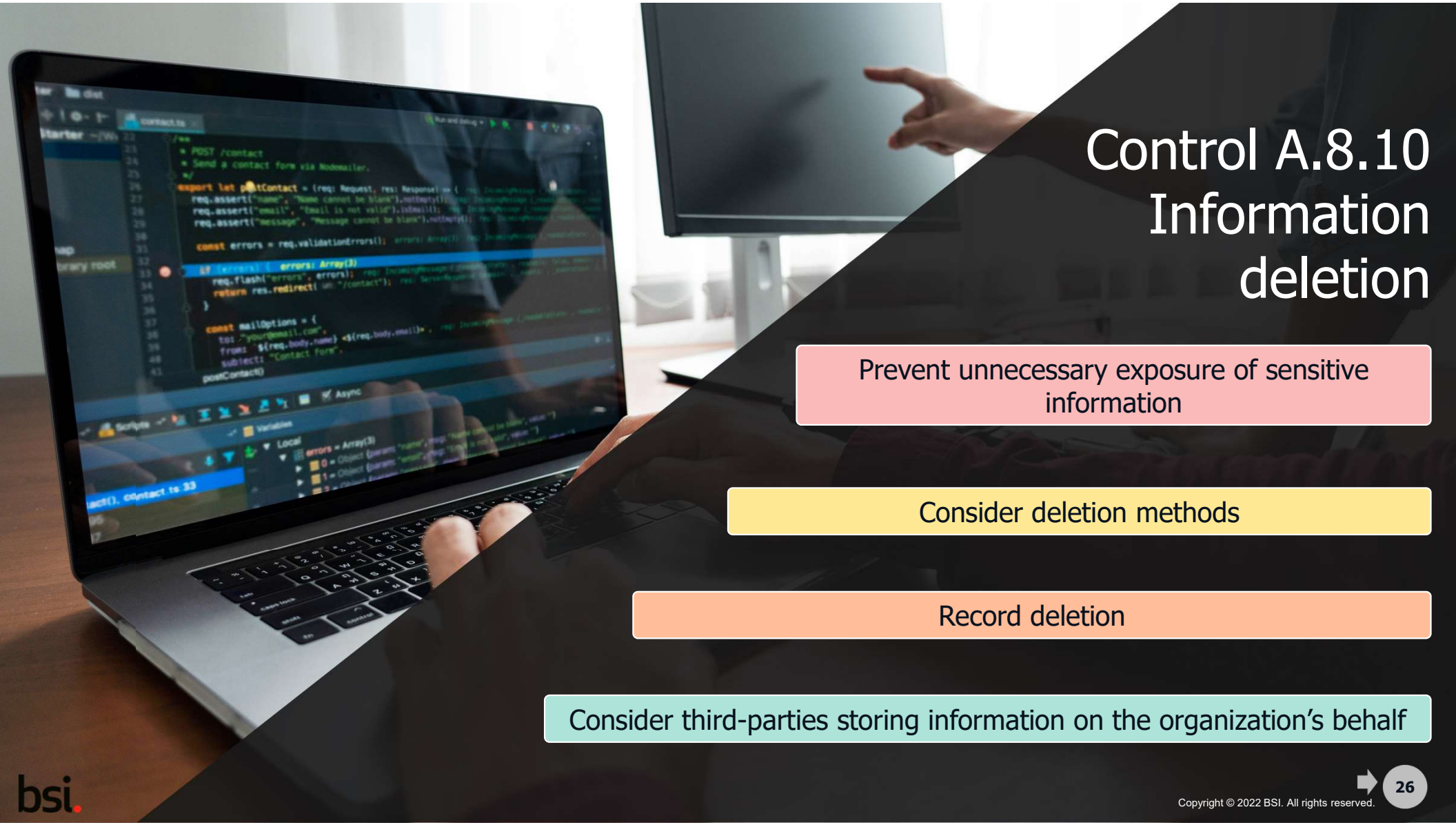
Control A.8.9 Configuration management

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

Use of standard templates and databases to manage configurations

Configuration monitoring utilizing system management tools

Integration with asset management



Control A.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

Control A.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

Control A.8.12 Data 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

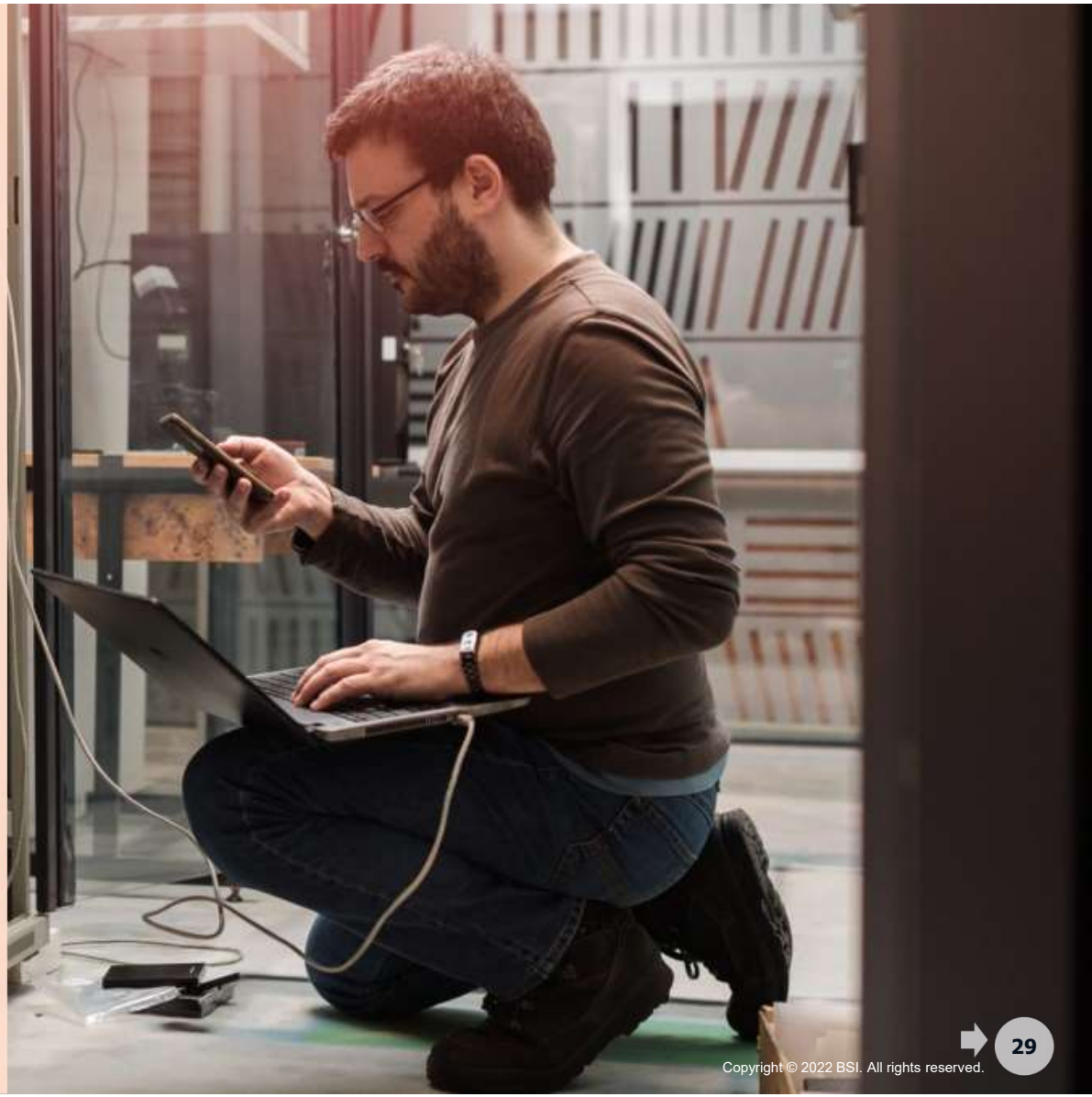
Use data leakage prevention tools

What are you protecting the information against?

bsi.

Control A.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



bsi.

Control A.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

Control A.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 life cycle including reuse

Thank you for participating