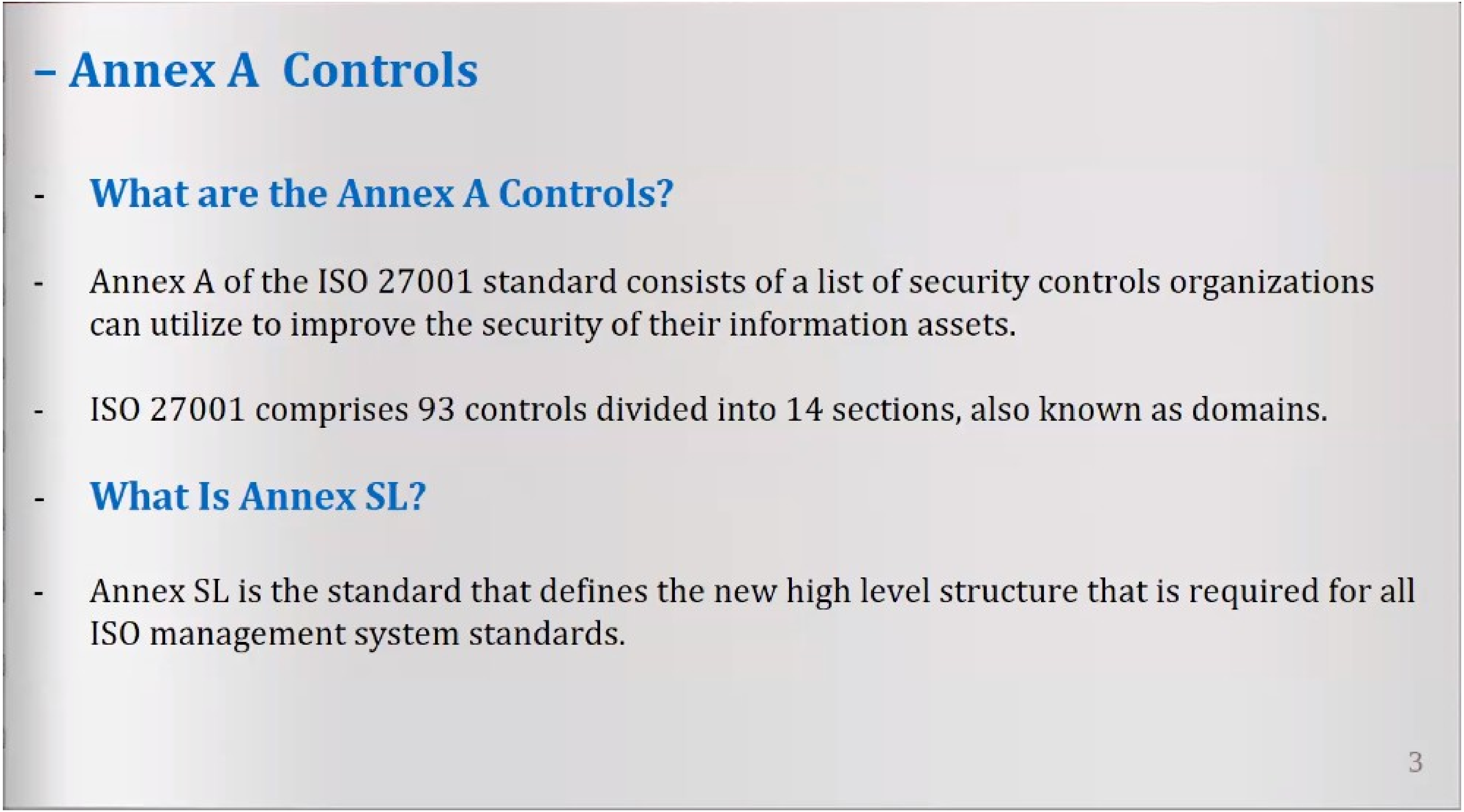
ISO27001:2022
Lec4

Annex A

- When working toward certification to ISO/IEC 27001, your organization will select relevant controls to implement from a checklist called Annex A.
- Think of Annex A as a catalog of information. Like a portfolio or archive, Annex A consists of a detailed list of security controls that organizations can use to improve their Information Security Management System (ISMS).

- Objectives and information security controls Listed in ANNEX A (A5 to A18) of ISO27001 are aligned with the security objectives and security controls listed in the pervious clauses.



– Annex A Controls

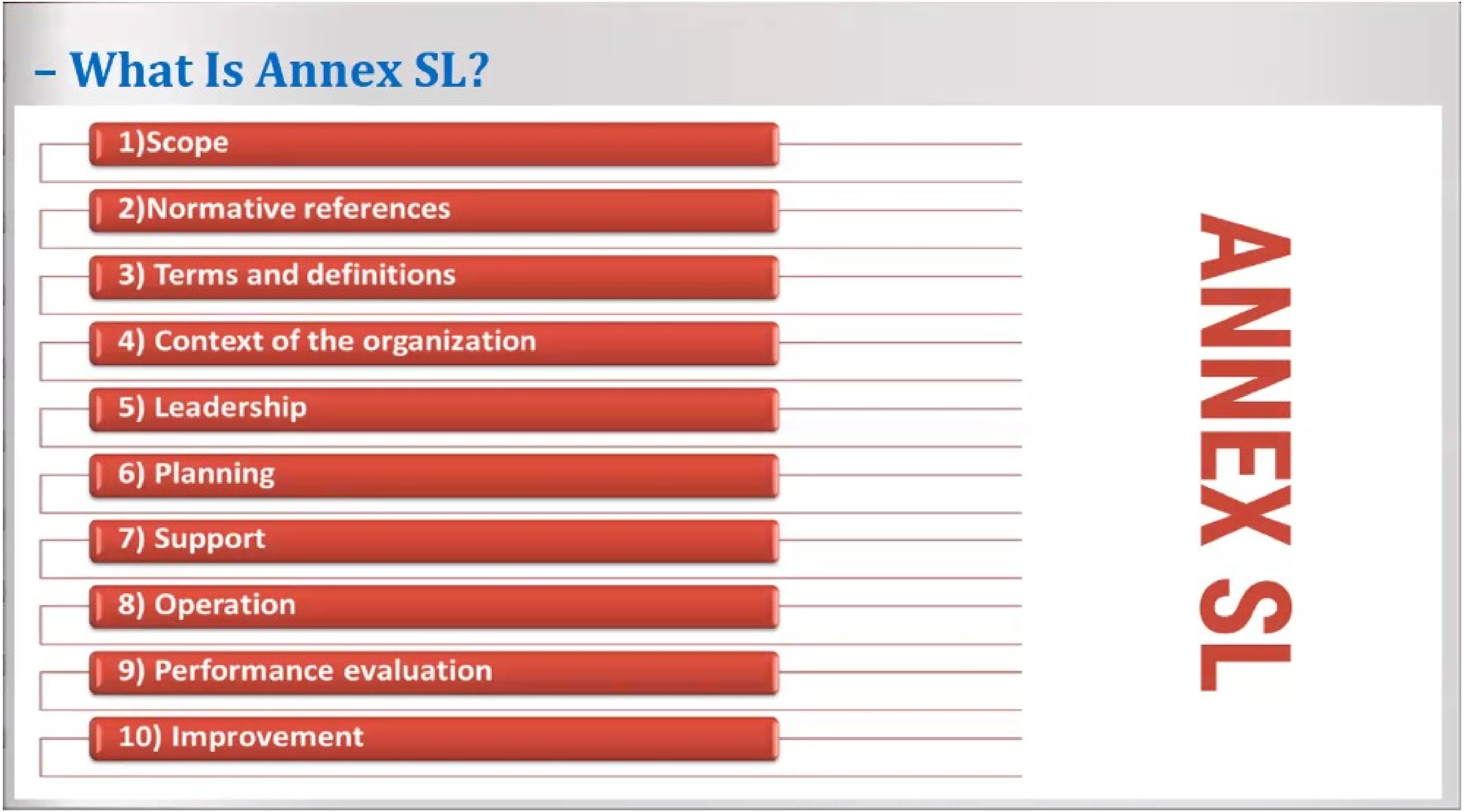
- **What are the Annex A Controls?**

- Annex A of the ISO 27001 standard consists of a list of security controls organizations can utilize to improve the security of their information assets.

- ISO 27001 comprises 93 controls divided into 14 sections, also known as domains.

- **What Is Annex SL?**

- Annex SL is the standard that defines the new high level structure that is required for all ISO management system standards.



– What Is Annex SL?

1)Scope

2)Normative references

3) Terms and definitions

4) Context of the organization

5) Leadership

6) Planning

7) Support

8) Operation

9) Performance evaluation

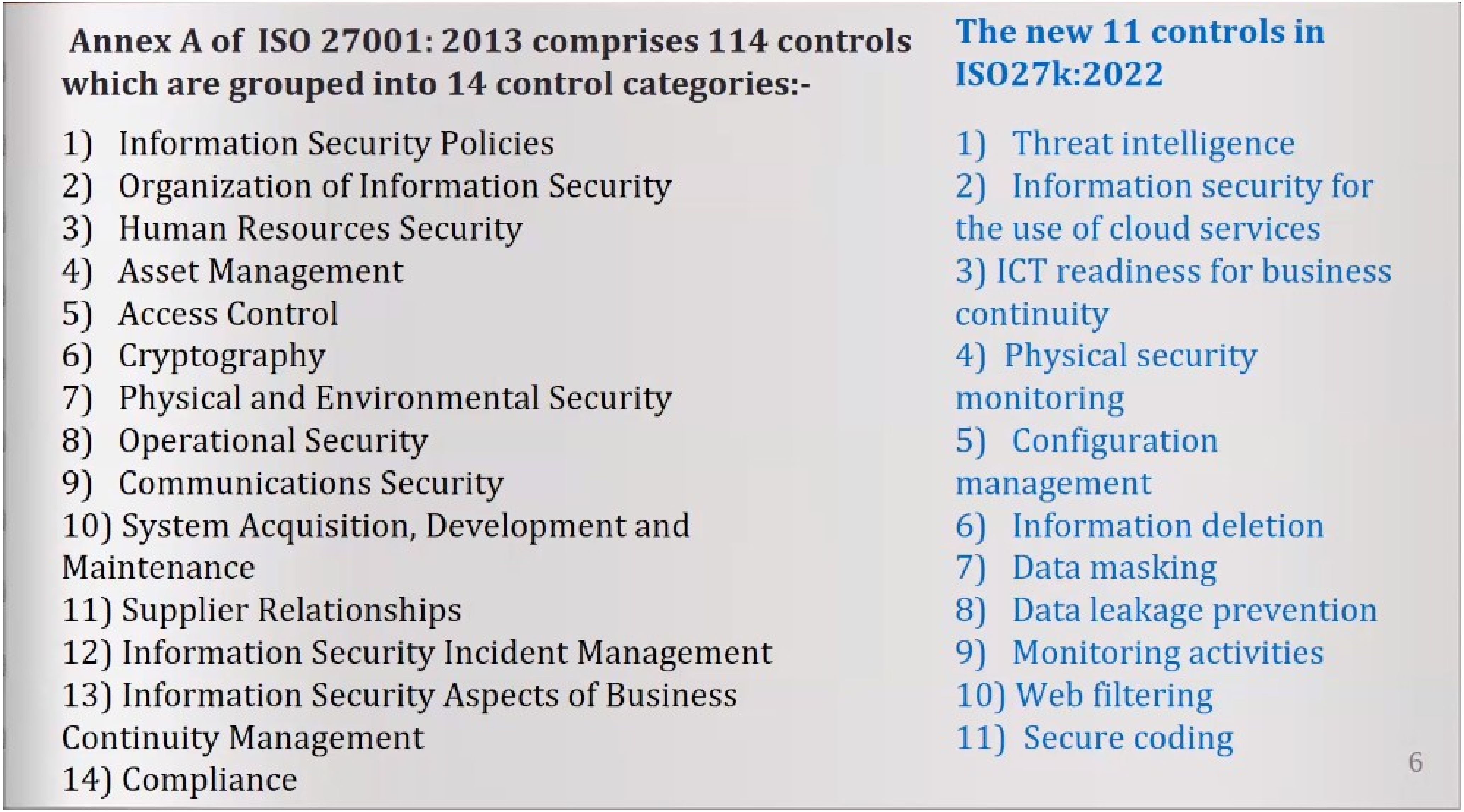
10) Improvement

ANNEX SL

Annex A Controls - Continued

Annex A contains a list of the security objectives and controls

A.5	Information security policies
A.6	Organization of information security
A.7	Human resource security
A.8	Asset management
A.9	Access control
A.10	Cryptography
A.11	Physical and environmental security
A.12	Operations security
A.13	Communications security
A.14	System acquisition, development and maintenance
A.15	Supplier relationships
A.16	Information security incident management
A.17	Information security aspects of business continuity management
A.18	Compliance



Annex A of ISO 27001: 2013 comprises 114 controls which are grouped into 14 control categories:-

1) Information Security Policies
2) Organization of Information Security
3) Human Resources Security
4) Asset Management
5) Access Control
6) Cryptography
7) Physical and Environmental Security
8) Operational Security
9) Communications Security
10) System Acquisition, Development and Maintenance
11) Supplier Relationships
12) Information Security Incident Management
13) Information Security Aspects of Business Continuity Management
14) Compliance

The new 11 controls in ISO27k:2022

1) Threat intelligence
2) Information security for the use of cloud services
3) ICT readiness for business continuity
4) Physical security monitoring
5) Configuration management
6) Information deletion
7) Data masking
8) Data leakage prevention
9) Monitoring activities
10) Web filtering
11) Secure coding

A.5 - Information Security Policies – ISO27k:2013

- The objective of this category is to provide management direction and support for information security in line with the organization's requirements and relevant regulations.

- This is achieved by documenting a set of information security policies, which must be approved, published, communicated and reviewed, at planned intervals.

A.5.7) Threat intelligence – ISO27k:2022
A.5.23) Information security for use of cloud services – ISO27k:2022
A.5.30) ICT readiness for business continuity – ISO27k:2022

A.5.7 - Threat intelligence – ISO27k:2022 in details:-

Description:

This control requires you to gather information about threats and analyze them, in order to take appropriate mitigation actions. This information could be about particular attacks, about methods and technologies the attackers are using, and/or about attack trends. You should gather this information internally, as well as from external sources like vendor reports, government agency announcements, etc.

Technology:

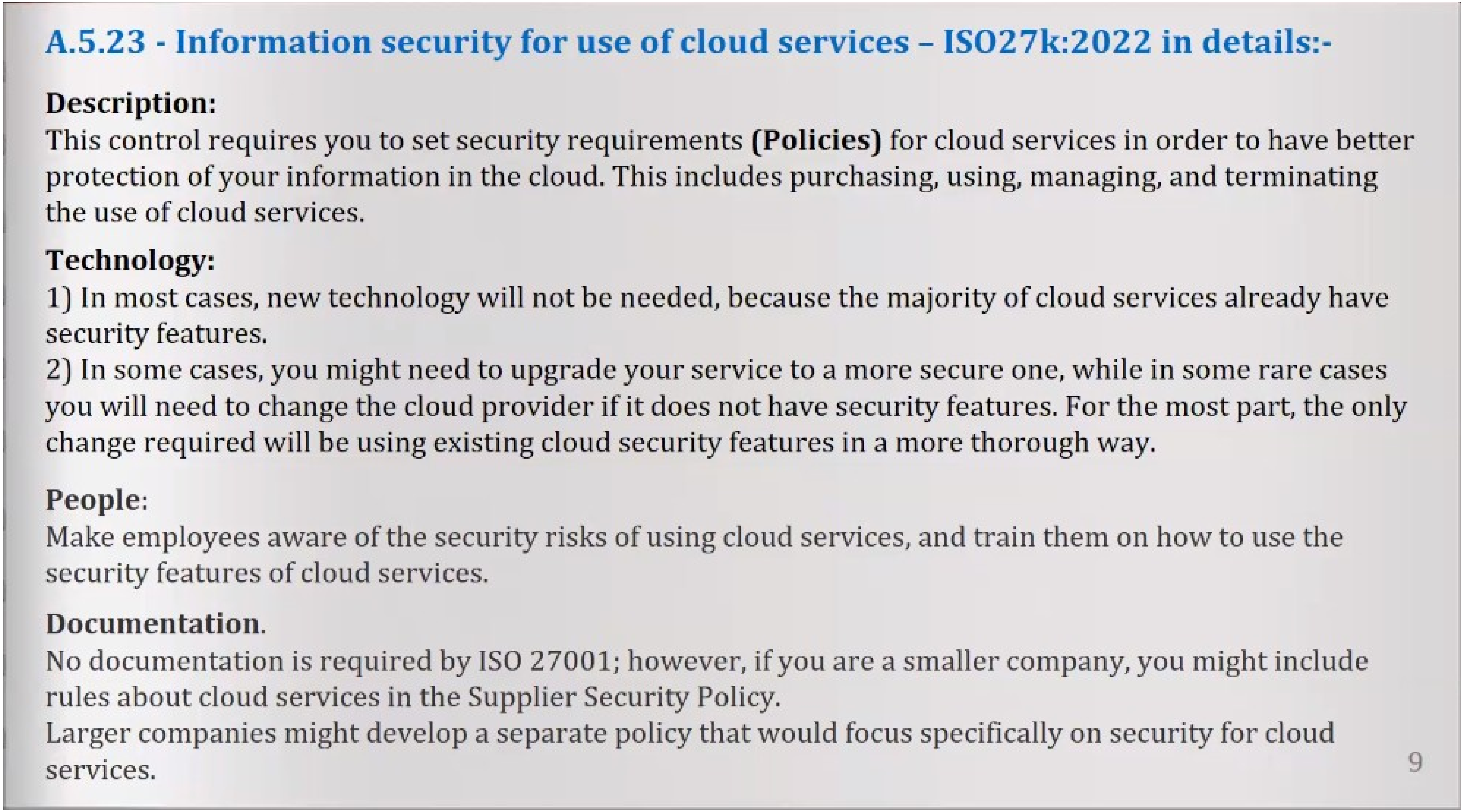
1) Smaller companies probably do not need any new technology related to this control; rather, they will have to figure out how to extract the threat information from their existing systems.
2) larger companies will need to acquire a system that will alert them to new threats.
3) Companies of any size will have to use threat information to harden their systems.

People:

Make employees aware of the importance of sending threat notifications, and train them on how and to whom these threats are to be communicated.

Documentation.

No documentation is required by ISO 27001; however, you might include rules about threat intelligence in the following documents.



A.5.23 - Information security for use of cloud services – ISO27k:2022 in details:-

Description:
This control requires you to set security requirements **(Policies)** for cloud services in order to have better protection of your information in the cloud. This includes purchasing, using, managing, and terminating the use of cloud services.

Technology:
1) In most cases, new technology will not be needed, because the majority of cloud services already have security features.
2) In some cases, you might need to upgrade your service to a more secure one, while in some rare cases you will need to change the cloud provider if it does not have security features. For the most part, the only change required will be using existing cloud security features in a more thorough way.

People:
Make employees aware of the security risks of using cloud services, and train them on how to use the security features of cloud services.

Documentation.
No documentation is required by ISO 27001; however, if you are a smaller company, you might include rules about cloud services in the Supplier Security Policy.
Larger companies might develop a separate policy that would focus specifically on security for cloud services.

A.5.30 - ICT(Instant center tracking) readiness for business continuity – ISO27k:2022 in details:-

Description:

This control requires information and assets are available when needed. This includes readiness planning, implementation, maintenance, and testing.

Technology:

- This requires a range from data backup to redundant communication links.
- These solutions need to be planned based on your risk assessment and how quickly you need your data and your systems to be recovered.

Besides the planning process, the maintenance process for your technology, and the testing process for your disaster recovery and/or business continuity plans.

People:

Make employees aware of potential disruptions that could happen, and train them on how to maintain IT and communication technology so that it is ready for a disruption.

Documentation.

No documentation is required by ISO 27001; you might include in the following documents:

- Disaster Recovery Plan
- Internal Audit Report

A.6 – Organization of Information Security– ISO27k:2013

- The first objective:-

- Information security roles and responsibilities are understood.
- Segregation of duties is understood.
- Information security in project management **(Scope of ISMS)** is established and managed, regardless of the type of project.
- The second objective is to ensure the security of remote working and the use of mobile devices.

- The second objective

- ensure the security of remote working and the use of mobile devices.

A.7 - Human Resources Security – ISO27k:2013

- **pre-employment requirements**, ensuring that individuals understand their responsibilities and are suitable for the roles they are being considered for.
- **Non-disclosure agreement.**
- The organization must ensure that **individuals receive appropriate training.**
- **Formal discipline process**

A.7.4) Physical security monitoring – ISO27k:2022

A.7.4) Physical security monitoring – ISO27k:2022

Description:

This control requires you to **monitor sensitive areas in order to enable only authorized people** to access them. This might include your offices, production facilities, warehouses, and other premises.

Technology:

- Depending on your risks, you might need to implement alarm systems or video monitoring; you might also decide to implement a non-tech solution like a person observing the area (e.g., a guard).
- You should define who is **(responsible for)** of the monitoring of sensitive areas, and what communication channels to use to report an incident.

People:

Make employees aware of the risks of unauthorized physical entry into sensitive areas, and train them how to use the monitoring technology.

Documentation:

- **Regulate Physical Security** – what is monitored, and who is in charge of monitoring.
- **Incident Management Procedure** – how to report and handle a physical security incident.

THANKS!