ISO27001:2022
Lec5

A.8 - Asset Management – ISO27k:2013 (Holding)

Its role in upholding accountability for and assigning responsibility to information assets. Identifying and implementing the necessary Annex A controls through a risk assessment is the key to **ISO 27001 compliance** and ensures strong information security practices. We will explore Annex A.8 in detail, the requirements for effective asset management, the importance of managing your assets in an integrated manner, and how to build an asset inventory.

A.8.9 - Configuration management – ISO27k:2022
A.8.10 - Information deletion – ISO27k:2022
A.8.11 - Data masking – ISO27k:2022
A.8.12 - Data leakage prevention – ISO27k:2022
A.8.16 - Monitoring activities – ISO27k:2022
A.8.23 - Web filtering – ISO27k:2022
A.8.28 - Secure coding – ISO27k:2022

A.8.9 - Configuration management – ISO27k:2022

Description:
This control requires you to manage the whole cycle of security configuration for your technology to ensure a proper level of security and to avoid any unauthorized changes. This includes configuration definition, implementation, monitoring, and review.

Technology:
- The technology whose configuration needs to be managed could include software, hardware, services, or networks. Smaller companies will probably be able to handle configuration management without any additional tools, whereas larger companies probably need some software that enforces defined configurations.

People:
Make employees aware of why strict control of security configuration is needed, and train them on how to define and implement security configurations.

Documentation: ISO 27001 requires this control to be documented.
If you are a small company, you can document the configuration rules in your Security Operating Procedures.
Larger companies will typically have a separate procedure that defines the configuration process.

A.8.10 - Information deletion – ISO27k:2022

Description:
This control requires you to delete data when no longer required, in order to avoid leakage of sensitive information and to enable compliance with privacy and other requirements. This could include deletion in your IT systems, removable media, or cloud services.

Technology:
- You should be using tools for secure deletion, according to regulatory or contractual requirements, or in line with your risk assessment.
- You should set up a process that will define which data need to be deleted and when, and define responsibilities and methods for deletion.

People:
Make employees aware of why deleting sensitive information is important, and train them on how to do this properly.

Documentation: No documentation is required by ISO 27001.
- Disposal and Destruction Policy – how the information on removable media is deleted.
- Acceptable Use Policy – how regular users need to delete the sensitive information on their computers and mobile devices.
- Security Operating Procedures – how system administrators need to delete the sensitive information on servers and networks

A.8.11 - Data masking – ISO27k:2022

Description:

This control requires you to use data masking together with access control in order to limit the exposure of sensitive information. This primarily means personal data, because they are heavily regulated through privacy regulations, but it could also include other categories of sensitive data.

Technology:

- Companies can use tools for anonymization in order to mask data if this is required by privacy or other regulations. Other methods like encryption or obfuscation can also be used.
- You should set up processes that will determine which data need to be masked, who can access which type of data, and which methods will be used to mask the data.

People:

Make employees aware of why masking data is important, and train them on which data need to be masked and how.

Documentation: No documentation is required by ISO 27001.

- Information Classification Policy – determine which data are sensitive and what categories of data need to be masked.
- Access Control Policy – defines who can access what type of masked or unmasked data.
- Secure Development Policy – defines the technology of masking the data.
- Privacy Policy / Personal Data Protection Policy – overall responsibilities for data masking.
- Anonymization and Pseudonymization Policy – details on how data masking is implemented in the context of privacy regulation.

A.8.12 - Data leakage prevention – ISO27k:2022

Description:

This control requires you to apply various data leakage measures in order to avoid unauthorized disclosure of sensitive information, and if such incidents happen, to detect them in a timely manner. This includes information in IT systems, networks, or any devices.

Technology:

- For this purpose, you could use systems to monitor potential leakage channels, including emails, removable storage devices, mobile devices, etc., and systems that prevent information from leaking – e.g., disabling download to removable storage, email quarantine, restricting copy and paste of data, restricting upload of data to external systems, encryption, etc. **(DLP)**

People:

Make employees aware of what kind of sensitive data is handled in the company and why it is important to prevent leakages, and train them on what is and what isn't allowed when handling sensitive data.

Documentation: No documentation is required by ISO 27001.

- Information Classification Policy – the more sensitive the data are, the more prevention needs to be applied.
- Security Operating Procedures – which systems for monitoring and prevention should be used by administrators.
- Policy on Acceptable Use – what is and what isn't allowed for regular users.

A.8.16 - Monitoring activities – ISO27k:2022

Description:
This control requires you to monitor your systems in order to recognize unusual activities and, if needed, to activate the appropriate incident response. This includes monitoring of your IT systems, networks, and applications.

Technology:

- For your networks, systems, and applications, you could monitor the following: security tool logs, event logs, who is accessing what, activities of your main administrators, inbound and outbound traffic, proper execution of the code, and how the system resources are performing.
- You should set up a process that defines which systems will be monitored; how the responsibilities for monitoring are determined; and the methods of monitoring, establishing a baseline for unusual activities, and reporting events and incidents.**(SIEM)**

People:
Make employees aware that their activities will be monitored, and explain what is and what is not considered normal behavior. Train IT administrators to use monitoring tools.

Documentation: No documentation is required by ISO 27001.

- If you are a small company, you can document the configuration rules in your Security Operating Procedures.
- Larger companies might develop a separate procedure that would describe how to monitor their systems.

A.8.23 - Web filtering – ISO27k:2022

Description:
This control requires you to manage which websites your users are accessing, in order to protect your IT systems. This way, you can prevent your systems from being compromised by malicious code, and also prevent users from using illegal materials from the Internet.

Technology:
- You could use tools that block access to particular IP addresses, which could include the usage of anti-malware software.
- You could also use non-tech methods like developing a list of forbidden websites and asking users not to visit them.
- You should set up processes that determine which types of websites are not allowed, and how the web filtering tools are maintained.**(WAF)**

People:
Make employees aware of the dangers of using the Internet, and also, train your system administrators on how to perform web filtering.

Documentation: No documentation is required by ISO 27001.
- if you are a smaller company, you might include rules about web filtering.
- Larger companies might develop a separate procedure that would describe how to how the web filtering is performed.

A.8.28 - Secure coding – ISO27k:2022

Description:
This control requires you to establish secure coding principles and apply them to your software development in order to reduce security vulnerabilities in the software. This could include activities before, during, and after the coding.

Technology:

- You should set up a process for defining the minimum baseline of secure coding – both for internal software development and for software components from third parties, a process for monitoring emerging threats and advice on secure coding, a process for deciding which external tools and libraries can be used, and a process that defines activities done before the coding, during the coding, after the coding (review and maintenance), and for software modification.

People:
Make your software developers aware of the importance of using secure coding principles, and train them on methods and tools for secure coding.

Documentation: No documentation is required by ISO 27001.

- If you are a smaller company, you might include rules about secure coding in the Secure Development Policy.
- Larger companies might develop separate procedures for secure coding for each of their software development projects.

11 New Controls introduced revision in ISO27k – 2022

THANKS!