Secure development life cycle

ISO 27002 Control 8.25

Control

Rules for the secure development of software and systems should be established and applied

Purpose

To ensure information security is designed and implemented within the secure development life cycle of software and systems.

Why is it important?

- Secure development is a prerequisite for building a secure service or system
- Early consideration of security requirements leads to more effective and cost-efficient solutions
- It mandates the structured approach to security testing and environment separation

Which topics should be addressed ?

- Establishing and applying rules for the secure development of software and systems
- Integration of security requirements early in the specification and design phase
- Guidance on security in the software development methodology
- Testing throughout the life cycle
- Management of repositories for source code and configuration

How to implement it ?

- Establish and apply rules for secure development
- Integrate security requirements and risk assessment checkpoints early in the project life cycle
- Implement technical controls like separation of environments and secure repositories
- Obtain assurance that outsourced development complies with the organization's rule

Link with other frameworks

- NIST 800-53 rev5 : SA-3, SA-15, SA-17
- NIST CSF 2.0 : ID.AM-08, PR.PS-06

Renaud Dardenne
Asphalia Consulting