Secure system architecture and engineering principles

ISO 27002 Control 8.27

Control

Principles for engineering secure systems should be established, documented, maintained and applied to any information system development activities

Purpose

To ensure information systems are securely designed, implemented and operated within the development life cycle

Why is it important?

- Ensures security is integrated into all architecture layers (business, data, application, technology)
- Security by design leads to more robust, cost-effective solutions
- Zero trust principles provide strong protection in modern, non-perimeter-focused environments
- Analysis of control integration ensures a comprehensive set of controls

What are the main related concepts ?

- Secure system architecture and engineering principles
- Security by design
- Defence in depth
- Zero trust principles
- Least privilege
- Secure virtualization techniques

Important small details

- Principles should cover the full range of security controls
- Systems should be designed to assume breach and not rely on perimeter security alone
- Formal acknowledgment is required for security controls that do not fully meet requirements

Link with other frameworks

- NIST 800-53 rev5 : SA-8
- NIST CSF 2.0 : ID.AM-08, PR.PS-06

Renaud Dardenne
Asphalia Consulting