Application security requirements

ISO 27002 Control 8.26

Control

Information security requirements should be identified, specified and approved when developing or acquiring applications

Purpose

To ensure all information security requirements are identified and addressed when developing or acquiring applications

Why is it important?

- Applications accessible via networks are subject to various threats (fraudulent activities, disclosure, alteration)
- Detailed risk assessments and careful control determination are indispensable
- Ensures compliance with legal/privacy requirements

What could be the sub controls ?

- Identifying requirements through a risk assessment supported by security specialists
- Specifying resilience requirements against malicious attacks
- Requiring secure encryption of communications between all involved parties
- Defining restrictions around content of "free-text" fields to prevent uncontrolled storage of confidential data
- Implementing input controls, including integrity checks and input validation

How is it proven ?

- Documented list of application security requirements (derived from risk assessment)
- Records showing approval of requirements by management
- Documentation confirming input validation and integrity checks are enforced
- Records showing secure encryption of communications (8.24)

Link with other frameworks

- NIST 800-53 rev5 : AC-3, SC-8*, SC-13
- NIST CSF 2.0 : PR.DS-01, PR.DS-02, PR.DS-10, DE.CM-09

Renaud Dardenne
Asphalia Consulting