Compliance with policies, rules and standards for information security

ISO 27002 Control 5.36

Control

Compliance with the organization's information security policy, topic-specific policies, rules and standards should be regularly reviewed

Purpose

To ensure that information security is implemented and operated in accordance with the organization's information security policy, topic-specific policies, rules and standards

Why is it important?

- It ensures controls and requirements defined in policies are actually being met in operation
- It provides input and assurance for overall governance processes and independent reviews
- Failure to comply can introduce risks and undermine the Information Security Management System

Are there technical ways of implementation ?

- Automated policy compliance scanning tools (vulnerability scanners, configuration auditors)
- SIEM systems monitoring policy violations in real-time
- Configuration management enforcing security baseline compliance
- Policy-as-code frameworks validating infrastructure compliance automatically

How is it evidenced ?

- Documented methods used by managers/owners to review compliance (e.g., checklists, reports from automated tools)
- Records of reviews conducted by managers/owners
- Records of corrective actions taken, including verification of effectiveness

Link with other frameworks

- NIST 800-53 rev5 : All XX-1 controls, CA-2
- NIST CSF 2.0 : ID.RA-01, PR.PS-02

Renaud Dardenne
Asphalia Consulting