Security testing in development and acceptance

ISO 27002 Control 8.29

Control

Security testing processes should be defined and implemented in the development life cycle

Purpose

To validate if information security requirements are met when applications or code are deployed to the production environment

Why is it important?

- Security testing is an integral part of system development and acceptance
- Testing must be proportional to the system's importance and potential impact
- Independent acceptance testing ensures objective verification of requirements
- Testing in a production-like environment ensures reliable results

Related concepts

- Security testing
- Acceptance testing
- Vulnerability scanning
- Penetration testing
- Secure coding
- Separation of environments

How is it achieved ?

- Static Application Security Testing (SAST)
- Dynamic Application Security Testing (DAST)
- Software Composition Analysis (SCA)
- Interactive Application Security Testing (IAST)
- Security code reviews and peer audits
- Threat modeling and attack surface analysis
- API security testing (OWASP API Top 10)

Link with other frameworks

- NIST 800-53 rev5 : CA-2, SA-4, SA-11, SR-5(2)*
- NIST CSF 2.0 : ID.IM-02

Renaud Dardenne
Asphalia Consulting