

Configuration management

ISO 27002 Control 8.9

Control

Configurations, including security configurations, of hardware, software, services and networks should be established, documented, implemented, monitored and reviewed

Purpose

To ensure hardware, software, services and networks function correctly with required security settings, and configuration is not altered by unauthorized or incorrect changes

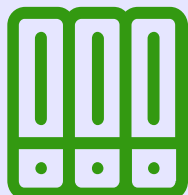


Why is it important?

- Improper configuration is a major weakness exploited by attackers
- Enforcement of standard secure templates ensures consistency across the organization
- Ensures security settings are maintained over the system lifetime
- Changing vendor default authentication information immediately is critical for security

What are good examples of hardening ?

- Disable unnecessary services and ports
- Remove default/unused accounts
- Enforce strong password policies with MFA
- Apply security patches regularly
- Implement least privilege access controls
- Enable firewall and intrusion detection
- Encrypt sensitive data at rest and in transit



To which other concepts does it relate to ?

- Configuration management
- Secure configuration
- Standard templates
- System hardening
- Vendor default authentication information

Link with other frameworks

- NIST 800-53 rev5 : CM-1, CM-2, CM-2(3)*, CM-3, CM-3(7), CM-3(8), CM-4, CM-5, CM-6, CM-8, CM-9, CM-9(1)*, SA-10
- NIST CSF 2.0 : ID.RA-07, PR.PS-01



Renaud Dardenne
Aspalia Consulting