Networks security

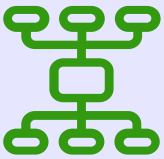
ISO 27002 Control 8.20

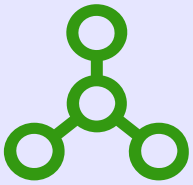
Control

Networks and network devices should be secured, managed and controlled to protect information in systems and applications

Purpose

To protect information in networks and its supporting information processing facilities from compromise via the network



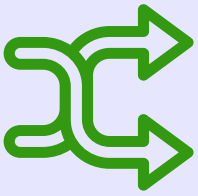


Why is it important?

- Ensures consistent application of controls across the infrastructure
- Protecting data confidentiality/integrity over public networks is critical
- Segregation of duties for network management is often appropriate
- Virtualized networks can provide logical separation for security

How to implement it?

- Implement controls to ensure security of information in networks (e.g., using cryptography)
- Establish responsibilities and procedures for equipment management
- Maintain up-to-date documentation (diagrams and configuration files)
- Restrict and filter system connection to the network (firewalls)
- Segregate network administration channels from other network traffic



Attention should be given to

- Separating operational responsibility for networks from ICT system operations should be done where appropriate
- Critical subnetworks can be temporarily isolated (e.g., with drawbridges) if the network is under attack
- Vulnerable network protocols should be disabled
- Physical cabling should be protected

Link with other frameworks

- NIST 800-53 rev5 : AC-3, AC-18, AC-20, SC-7, SC-8, SC-10
- NIST CSF 2.0 : PR.AA-03, PR.AA-05, PR.AA-06, PR.DS-02, PR.IR-01

Renaud Dardenne
Asphalia Consulting