Security of network services

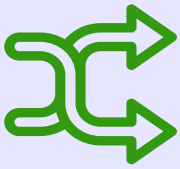
ISO 27002 Control 8.21

Control

Security mechanisms, service levels and service requirements of network services should be identified, implemented and monitored

Purpose

To ensure security in the use of network services

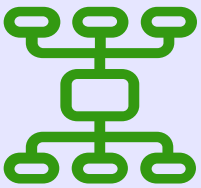


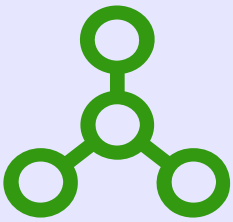
Why is it important?

- Network services often provide crucial connectivity and infrastructure
- Regular monitoring ensures the provider complies with agreed service levels
- The right to audit the provider (or review attestations) is necessary for assurance

Best practices

- Identifying and implementing necessary security features (authentication, encryption, connection controls)
- Regularly monitoring the ability of the network service provider to manage agreed services securely
- Requiring the right to audit or third-party attestations from the provider





What is important ?

- Network services range from simple unmanaged bandwidth to complex value-added offerings (e.g., firewalls)
- Caching parameters (e.g., in a content delivery network) should be considered in line with confidentiality and availability requirements
- The means used to access services (e.g., VPN or wireless network) must be covered by rules
- The organization should also consider monitoring the use of network services

Link with other frameworks

- NIST 800-53 rev5 : CA-3, SA-9
- NIST CSF 2.0 : NA

Renaud Dardenne
Asphalia Consulting