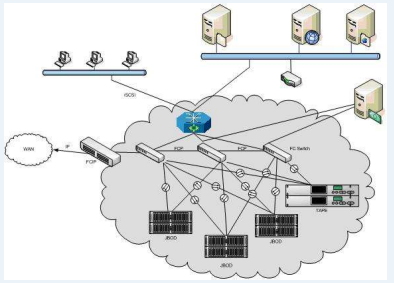
ISO/IEC 27001:2013 Information security management systems
-Network security management-

Security category – 13.1. Network security management



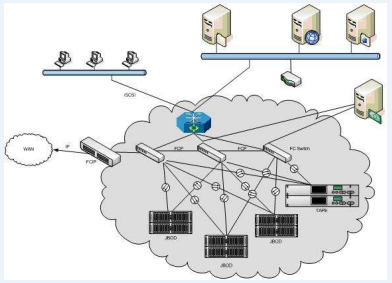
Control – 13.1.1. Network controls
The networks have to be controlled and managed so that the information in systems and applications is protected.

Networks are vulnerable to unauthorized access, to misuse or abuse and to unintentional fallings of technology.

ISO/IEC 27001 requires the organization to implement controls to ensure the security of information passing through networks and the protection of devices connected to the networks.

ISO/IEC 27001:2013 Information security management systems

-Network security management-



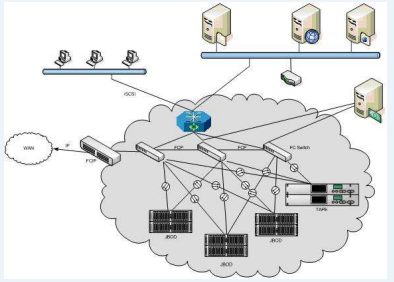
General guidelines from ISO/IEC 27002 on network security management:

- define responsibilities and procedures for the management of network equipment;
- define and apply some supplementary controls to protect the confidentiality and integrity of data passing over public networks or through wireless networks – as the risks are considerably higher;
- constantly monitor of the network ;
- ensure the authentication of systems connected to the network and restrict connections.

ISO/IEC 27033 – about network security

ISO/IEC 27001:2013 Information security management systems
-Network security management-

Control – 13.1.2. Security of network services
The organization should identify and include in network service agreements security mechanisms, service levels and management requirements for all network services. This is applicable irrespective whether the network services are provided in-house or by a third party.



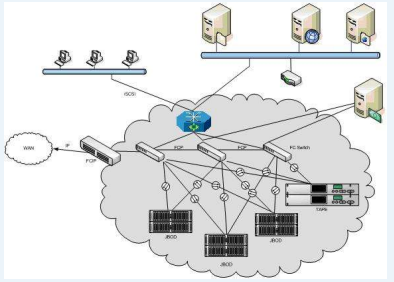
Third party supplied network services carry a risk of unauthorized access attempts that may lead to security breaches.

Network services may include – provision of connections, private network services, security solutions for the networks (like firewalls or intrusion detection systems)…

The organization should agree with the service provider (and document in the contracts) on the security features for the services it provides and should monitor the services to see if they meet requirements.

ISO/IEC 27001:2013 Information security management systems
-Network security management-

Control – 13.1.3. Segregation in networks
Groups of information services, users and information systems should be segregated on networks.

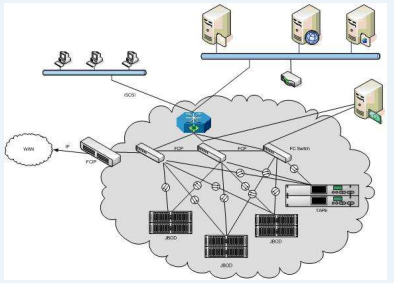


The bigger the network, the higher the risk.

Security can be managed easier if the network is divided into physical or logical domains and security measures are implemented to manage the gateways between the domains.

The segregation can be done using physically different networks or by applying connection and routing controls.

ISO/IEC 27001:2013 Information security management systems
-Network security management-



The perimeter for each domain should be well defined and the access between network domains should be controlled using a gateway.

Wireless networks - difficult to define exactly the perimeter – ISO/IEC 27002 recommends for sensitive environments (where critical data is stored or processed) to treat all wireless access as external connections and to segregate this access from internal networks and pass the wireless access through a gateway before accessing internal systems.

The domains and their relationship should be documented in a ***network map*** or similar document.

Special care for networks that spread beyond organization's boundaries.