Australian Government

Assessment Requirements for ICTNWK406 Install, configure and test network security

Release: 1

Assessment Requirements for ICTNWK406 Install, configure and test network security

Modification History

Release	Comments
Release 1	This version first released with ICT Information and Communications Technology Training Package Version 1.0.

Performance Evidence

Evidence of the ability to:

- assess and identify security threats, vulnerabilities and risks
- determine appropriate countermeasure for threat, vulnerability or risk
- implement countermeasure per threat or risk
- install, configure and test network elements to ensure perimeter security
- test and verify function and performance of selected security measures
- monitor network for suspicious activity and take appropriate action where necessary
- document newly discovered threats, vulnerabilities and risks, including change recommendations for approval.

Note: If a specific volume or frequency is not stated, then evidence must be provided at least once.

Knowledge Evidence

To complete the unit requirements safely and effectively, the individual must:

- outline authentication issues
- summarise the security requirements of the client business domain, including:
  - organisation structure and business functionality
  - features and capabilities of networking technologies
  - privacy issues and privacy legislation
  - security information sources
  - risk analysis
- outline common virtual private network (VPN) issues, including bandwidth and dynamic security environment
- explain how to configure routers and switches

© Commonwealth of Australia, 2018

- summarise current industry accepted hardware and software security products, including general features and capabilities
- outline the function and operation of VPN concepts, including encryption, firewalls, packet tunnelling and authentication
- outline network protocols and operating systems
- summarise organisational issues surrounding security
- outline security perimeters and their functions
- describe security protocols, standards and data encryption
- summarise security threats, including eavesdropping, data interception, data corruption and data falsification
- outline types of VPNs, including site-to-site and user-to-site internet traffic and extranets
- summarise the systems and procedures related to:
    - audit and intrusion detection systems
    - auditing and penetration testing techniques
    - cryptography
    - local area network (LAN), wireless local area network (WLAN) and wide area network (WAN)
    - screened subnets
    - transmission control protocols or internet protocols (TCPs/IPs) and applications
    - use of virus detection software.

Assessment Conditions

Gather evidence to demonstrate consistent performance in conditions that are safe and replicate the workplace. Noise levels, production flow, interruptions and time variances must be typical of those experienced in the network industry, and include access to:

- a site where secure network installation may be conducted
- network security documentation
- equipment specifications
- network components
- hardware and software
- firewalls (hardware and software)
- a live network
- organisational guidelines
- networked (LAN) computers
- WAN service point of presence.

Assessors must satisfy NVR/AQTF assessor requirements.

© Commonwealth of Australia, 2018

Links

Companion Volume implementation guides are found in VETNet - https://vetnet.education.gov.au/Pages/TrainingDocs.aspx?q=a53af4e4-b400-484e-b778-71c9e9d6aff2

© Commonwealth of Australia, 2018