



Australian Government

Assessment Requirements for ICTNWK421 Install, configure and test network security

Release: 1

Assessment Requirements for ICTNWK421 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 4.0.

Performance Evidence

The candidate must demonstrate the ability to complete the tasks outlined in the elements and performance criteria of this unit; including evidence of the ability to:

- With respect to one network:
 - identify and analyse network security threats and vulnerabilities
 - make recommendations to management to address network security deficiencies and fulfil organisational asset security requirements
 - implement perimeter security, network hardening measures and authentication and user account controls according to identified deficiencies and organisational asset security requirements
 - design and conduct testing to verify the key function and performance measures of network security
 - debug network security according to test results
 - review logs and audit reports to identify and record five security incidents, intrusions and attempts
 - undertake three spot checks and audits to ensure that procedures are not being bypassed
 -

Knowledge Evidence

The candidate must be able to demonstrate knowledge to complete the tasks outlined in the elements and performance criteria of this unit. This includes:

- Security requirements of the organisation, including:
 - organisational structure and functions
 - features and capabilities of networking technologies
 - privacy issues and privacy legislation
 - security information sources
 - risk analysis

- Virtual private network (VPN) issues, including bandwidth and dynamic security environment
- Configuration of routers and switches
- Current hardware and software security products, including general features and capabilities
- Function and operation of VPN concepts including encryption, firewalls, packet tunnelling, and authentication
- Network protocols and operating systems
- Security perimeters and functions
- Security protocols, standards and data encryption
- Security threats including eavesdropping, data interception, data corruption and data falsification
- Types of VPNs including site-to-site and user-to-site internet traffic and extranets
- 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 protocol, internet protocol (TCPs/IPs), and applications
 - virus detection software

Assessment Conditions

Skills must be demonstrated in a workplace or simulated environment where conditions are typical of those in an ICT working environment or ICT workplace. This includes:

- Site where secure network installation, configuration, and monitoring may be conducted
- Network security documentation
- Organisational asset security requirements and information on organisational structure and functions
- Equipment specifications
- Network components
- Testing software
- Individual manager in the organisation
- Firewalls (hardware and software)
- Live network
- Networked (LAN) computers
- WAN service point of presence

Assessors of this unit must satisfy the assessor requirements in applicable vocational education and training legislation, frameworks and/or standards.

Links

Companion Volume Implementation Guides are available from VETNet -

<https://vetnet.gov.au/Pages/TrainingDocs.aspx?q=a53af4e4-b400-484e-b778-71c9e9d6aff2>