Australian Government

Assessment Requirements for ICTNWK503 Install and maintain valid authentication processes

Release: 1

Assessment Requirements for ICTNWK503 Install and maintain valid authentication processes

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:

- design and deploy authentications solutions to the business technology environment and business needs
- configure authentication software or tools
- monitor and test authentication process after implementation
- ensure authentication solutions are current.

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:

- summarise the problems and challenges dealing with organisational authentication issues, including resource accounting through authentication
- discuss common virtual private network (VPN) issues, including:
  - quality of service (QoS) considerations
  - bandwidth
  - dynamic security environment
  - function and operation of VPN concepts
- outline authentication adaptors
- summarise biometric authentication adaptors
- summarise digital certificates, such as VeriSign, X.509, and SSL
- explain the function and operation of authentication controls including:
  - passwords
  - personal identification numbers (PINs)
  - smart cards

  - biometric devices
  - other authentication protocols
- outline network authentication services, such as Kerberos and NT LAN Manager (NTLM)
- summarise the features of common password protocols, such as:
  - challenge handshake authentication protocol (CHAP)
  - challenge phrases
  - password authentication protocol (PAP)
  - remote authentication dial-in user service (RADIUS) authentication
- describe the principles of security tokens.

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 or prototype where network authentication may be implemented and managed
- network support tools currently used in industry
- organisational security policies related to authentication
- manufacturers recommendations
- current authentication standards, including biometric authentication adaptors.

Assessors must satisfy NVR/AQTF assessor requirements.

Links

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