Australian Government

Assessment Requirements for ICTNWK502 Implement secure encryption technologies

Release: 1

Assessment Requirements for ICTNWK502 Implement secure encryption technologies

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:

- analyse enterprise data security requirements
- create or review existing security plan to determine the appropriate encryption methods
- rank and document appropriate encryption methods
- implement encryption systems and inform users of any impacts
- monitor and document encryption issues and compromises, and notify appropriate person.

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:

- explain certificate related infrastructure (certificate authorities, registration authorities, repository services)
- summarise common asymmetric key algorithms and their usage
- explain common symmetric key algorithms and their usage, such as:
  - advanced encryption standard (AES)
  - data encryption standard (DES)
  - triple data encryption algorithm (triple DES)
  - Blowfish
- explain encryption strength
- summarise various encryption types, including public key, secret key, hash key
- summarise the functions and features of:
  - access control permissions
  - digital signatures
  - symmetric encryption, asymmetric encryption and one-way encryption

  - timestamps
- explain one-way message digests, such as message digest algorithm 5 (MD5) and secure hash algorithm (SHA)
- explain public key infrastructure (PKI), pretty good privacy (PGP) and GNU Privacy Guard (GnuPG)
- outline replay security
- outline possible sources of security threats, including eavesdropping, data interception, data corruption, data falsification and authentication issues
- explain transmission control protocol or internet protocol (TCP/IP) protocols and applications
- summarise security problems and challenges that arise from organisational issues
- outline wired equivalent privacy (WEP), Wi-Fi protected access (WPA) and Wi-Fi protected access 2 (WPA2).

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 encryption installation may be conducted
- a live network
- servers
- encryption software
- encryption tools.

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