



Australian Government

Assessment Requirements for ICTNWK513 Manage system security

Release: 1

Assessment Requirements for ICTNWK513 Manage system 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:

- implement and manage security functions on a system
- conduct risk assessment
- set up effective controls to manage risk
- develop security plan and security recovery plan
- monitor risks and controls
- review risk analysis process.

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 general features of specific security technologies
- describe risk analysis techniques, with a focus on their general features, and depth in security procedures
- describe the common security requirements of a client's organisation, including:
 - threats
 - security techniques and technologies
- outline systems management and process control in relation to security
- explain systems technologies, including a broad summary of their general features and capabilities.

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 system security may be implemented and managed
- use of utility tools currently used in industry
- organisational security policies
- manufacturer recommendations
- security standards.

Assessors must satisfy NVR/AQTF assessor requirements.

Links

Companion Volume implementation guides are found in VETNet -

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