



Australian Government

Assessment Requirements for UEECS0009

Design and implement security for internetworking systems

Release: 1

Assessment Requirements for UEECS0009 Design and implement security for internetworking systems

Modification History

Release 1. This is the first release of this unit of competency in the UEE Electrotechnology Training Package.

Performance Evidence

Evidence required to demonstrate competence in this unit must be relevant to and satisfy all of the requirements of the elements, performance criteria and range of conditions on at least one or more separate occasions and include:

- applying relevant work health and safety (WHS)/occupational health and safety (WHS/OHS) requirements, including the use of risk control measures
- arranging work team/group of relevant persons
- dealing with unplanned events
- designing internetworking system with economical design solutions
- developing a design brief for advanced security technologies in an internetworking system design brief
- developing a disaster recovery plan
- documenting and presenting design for approval
- documenting internetworking installation and configuration activities
- identifying and rectifying system malfunctions and performance issues
- implementing internetworking system design
- monitoring quality of work
- negotiating alterations to internetworking system design
- planning work activities including requirements for work team/group
- presenting and discussing internetworking system design with relevant person/s
- selecting relevant development tools and software.

Knowledge Evidence

Evidence required to demonstrate competence in this unit must be relevant to and satisfy all of the requirements of the elements, performance criteria and range of conditions and include knowledge of:

- access control lists (ACLs)
- ACLs for firewalls
- cryptographic services
- virtual private network (VPN)
- firewalls

- internet protocol (IP) security
- intrusion detection systems (IDS)
- network security testing
- relevant network security industry standards
- relevant manufacturer specifications
- relevant WHS/OHS legislated requirements
- relevant workplace documentation
- network security policies
- secure network design
- securing perimeter routers.

Assessment Conditions

Assessors must hold credentials specified within the Standards for Registered Training Organisations current at the time of assessment.

Assessment must satisfy the Principles of Assessment and Rules of Evidence and all regulatory requirements included within the Standards for Registered Training Organisations current at the time of assessment.

Assessment must occur in suitable workplace operational situations where it is appropriate to do so; where this is not appropriate, assessment must occur in simulated suitable workplace operational situations that replicate workplace conditions.

Assessment processes and techniques must be appropriate to the language, literacy and numeracy requirements of the work being performed and the needs of the candidate.

Resources for assessment must include access to:

- a range of relevant exercises, case studies and/or simulations
- relevant and appropriate materials, tools, facilities and equipment currently used in industry
- resources that reflect current industry practices in relation to designing and implementing security for internetworking systems
- applicable documentation, including workplace procedures, equipment specifications, regulations, codes of practice and operation manuals.

Links

Companion Volume implementation guides are found in VETNet - -

<https://vetnet.gov.au/Pages/TrainingDocs.aspx?q=b8a8f136-5421-4ce1-92e0-2b50341431b6>