



Australian Government

ICTSS00126 Advanced Cyber Incident Threat Detection and Prevention Skill Set

Release 1

ICTSS00126 Advanced Cyber Incident Threat Detection and Prevention Skill Set

Modification History

Release	Comments
Release 1	This version first released with the Information and Communications Technology Training Package Version 8.0. Newly created to equip learners with skills across in-demand technologies.

Description

This skill set addresses the skills and knowledge required to respond to complex cyber security risks in organisations in information and communications technology (ICT) environments.

Pathways Information

The units provide credit towards ICT40120 Certificate IV in Information Technology, ICT60220 Advanced Diploma of Information Technology, and other qualifications that allow for selection of these units.

Licensing/Regulatory Information

No licensing, legislative or certification requirements apply to this skill set at the time of publication.

Skill Set Requirements

- ICTCYS406 Respond to cyber security incidents
- ICTCYS602 Implement cyber security operations
- ICTCYS603 Undertake penetration testing for organisations
- ICTCYS607 Acquire digital forensic data
- ICTCYS608 Perform cyber security risk assessments

Target Group

This skill set is for individuals who work in cyber security roles, including network and server administrators, cyber security architects, network security specialists, cyber security engineers, and other related roles responsible for maintaining cyber security and responding to cyber incidents.

Suggested words for Statement of Attainment

These units of competency from the ICT Information and Communications Technology Training Package meet industry requirements for advanced cyber incident threat detection and prevention in ICT contexts.