22445VIC

Advanced Diploma of Cyber Security

(Version 2)

This course has been accredited under Parts 4.4 of the Education and Training Reform Act 2006.

Accredited for the period: 1st October 2017 to 31st March 2023

Version	Date	Comment
Version 1	1st October 2017	Initial accreditation (1st October 2017 to 30th September 2022)
Version 2	9th May 2022	VRQA approved short term (6 months) extension to the course accreditation period. (1st October 2017 to 31st March 2023)

No new students may be enrolled after 31 March 2023. Continuing students may complete their studies and receive the qualification for successful completion according to the transition arrangements specified by the relevant VET regulator.

Disclaimer

In compiling the information contained in and accessed through this resource, the Department of Education and Training (DET) has used its best endeavours to ensure that the information is correct and current at the time of publication but takes no responsibility for any error, omission or defect therein.

To the extent permitted by law DET, its employees, agents and consultants exclude all liability for any loss or damage (including indirect, special or consequential loss or damage) arising from the use of, or reliance on the information contained herein, whether caused or not by any negligent act or omission. If any law prohibits the exclusion of such liability, DET limits its liability to the extent permitted by law, for the resupply of the information.

Third party sites

This resource may contain links to third party websites and resources. DET is not responsible for the condition or content of these sites or resources as they are not under its control.

Third party material linked from this resource is subject to the copyright conditions of the third party. Users will need to consult the copyright notice of the third party sites for conditions of usage.

Contents

Section A: Copyright and Course Classification Information

1. Copyright owner of the course

Copyright of this course is held by the Department of Education and Training, Victoria

2. Address

Executive Director
Executive Director
Higher Education and Workforce Division
Higher Education and Skills
Department of Education and Training (DET)
GPO Box 4367
Melbourne 3001

Organisational Contact:

Executive Director
Higher Education and Workforce Division
Higher Education and Skills
Department of Education and Training (DET)
GPO Box 4367
Melbourne 3001

Email: course.enquiries@edumail.vic.gov.au

Day-to-Day Contact:

Curriculum Maintenance Manager-Engineering Industries
Box Hill Institute of TAFE
Private Bag 2014
Box Hill, Victoria 3128
Ph: 03 92286 9880
Email: gadda@bhtafe.edu.au

3. Type of submission

Accreditation

4. Copyright

Copyright of this material is reserved to the Crown in the right of the

acknowledgement State of Victoria.

© State of Victoria (Department of Education and Training) 2017.

The following unit of competency:

BSBWOR502	Lead and manage team effectiveness

is from the BSB Business Services training Package administered by the Commonwealth of Australia

The following units of competency:

ICTNWK502	Implement secure encryption technologies
ICTNWK503	Install and maintain valid authentication processes
ICTNWK509	Design and implement a security perimeter for ICT networks
ICTNWK513	Manage system security
ICTNWK525	Configure an enterprise virtual computing environment
ICTNWK531	Configure an internet gateway
ICTNWK607	Design and implement wireless network security
ICTSAS501	Develop, implement and evaluate an incident response plan
ICTSAS505	Review and update disaster recovery and contingency plans
ICTTEN811	Evaluate and apply network security

are from the ICT Information and Communications Technology Training Package administered by the Commonwealth of Australia.

© Commonwealth of Australia

5. Licensing and franchise

Copyright of this material is reserved to the Crown in the right of the State of Victoria.

© State of Victoria (Department of Education and Training) 2017.

This work is licensed under a Creative Commons Attribution-NoDerivs 3.0 Australia licence (http://creativecommons.org/licenses/by-nd/3.0/au/).

You are free to use copy and distribute to anyone in its original form as long as you attribute Higher Education and Skills Group, Department of Education and Training (DET) as the author and you license any devitative work you make available under the same license.

Request for other use should be addressed to:

Executive Director

Higher Education and Workforce Division

Higher Education and Skills

Department of Education and Training (DET)

GPO Box 4367

Melbourne 3001

Email: course.enquiry@edumail.vic.gov.au

Copies of this publication can be downloaded free of charge for the DET website at:

www.education.vic.gov.au/training/providers/rto/Pages/courses.aspx

6. Course accrediting body

Victorian Registration and Qualifications Authority (VRQA)

Website: http://www.vrqa.vic.gov.au/

7. AVETMISS information

ANZSCO code:	313199	ICT Support Technicians
ASCED code:	0299	Other Information Technology
National course code:		22445VIC

8. Accreditation period

1st October 2017 to 31st March 2023

Section B: Course Information

1. Nomenclature *Standard 1 AQTF Standards for Accredited Courses*

1.1 Name of the qualification	Advanced Diploma of Cyber Security
1.2 Nominal duration of the course	945 - 1210 hours

2. Vocational or educational outcomes *Standard 1 AQTF Standards for Accredited Courses*

2.1 Purpose of the course	The Advanced Diploma of Cyber Security is a para professional qualification that will provide graduates with the knowledge and skills that will equip them to provide a comprehensive set of technical services such as: - performing a security risk assessment for an organisation - implementing best practice for identity management - evaluating an organisation's compliance with relevant cyber security standards, laws and codes of practice - evaluating and implementing security protection devices and software - managing a cyber security environment - assessing and securing cloud services - performing digitial forensic investigations on workstations and mobile devices Graduates of the course will be able to seek employment as cyber security para professionals in a range of commercial enterprises/organisations and government bodies seeking to improve their cyber security or, work independently as freelance cyber security consultants.

3. Development of the course *Standards 1 and 2 AQTF Standards for Accredited Courses*

3.1 Industry / enterprise/ community needs	The recent Australian cyber security strategy paper released May 2016; *Australia's Cyber Security Strategy – enabling innovation, growth & prosperity,* states the following: *"Like many nations Australia is suffering from a cyber security skill shortage. These particular skills are essential in our connected technology – enabled world and they are fundamental to this nation's success. At the global level in the information security sector it is expected to see a deficit of 1.5 million professionals by 2020".*[1] *"For Australia to have the cyber security skills and knowledge to thrive in the digital age the Federal Government is:* • *addressing the shortage of cyber security professionals in the workforce through targeted actions at all levels of Australia's education system, starting with academic centres of cyber security excellence in universities and by increasing diversity in the workforce*

[1] **Australian Cyber Security Strategy Page 51 Para 1**

	- *working with the private sector and international partners to raise awareness of the importance of cyber security across the community".*[2] Many Australian organisations are unaware of the risks they face in cyberspace. The government is committed to equipping Australians with the right cyber security skills and raising levels of cyber security awareness so all Australians can benefit from the opportunities presented in cyber space. "*Demand in Australia for cyber security services and related jobs such as legal services, insurance and risk management is expected to grow by at least 21 per cent over the next five years. There will be significant employment and career opportunities for those with appropriate skills. Currently there is a short fall in the number of people with the appropriate skills and a number of job vacancies in the private and public sectors are not being filled. The take up of ICT related university degrees (often a precursor for cyber security professionals), has halved over the last decade and graduation rates have dropped".*[3] The above statement, also from *Australia's Cyber Security Strategy – enabling innovation, growth & prosperity,* highlights there is insufficient awareness of the employment opportunities as well as the types of courses currently available to obtain the appropriate skills. The shortfall in appropriate skills is further emphasised by the *Telstra Cyber Security Report - 2016* with the following quote: *"This year's survey highlighted the growing shortage of skilled security staff required to perform increasingly complex security tasks as one of the major challenges for organisations. 62% of organisations stated that they have too few information security professionals to implement security activities within their organisations. Skills that entailed security risk assessments and conducting forensic investigations were among the most lacking across all verticals with an average of 54.3% organisations indicating a shortage of skills in these areas. Asian organisations lacked more than their Australian counterparts across all areas on average.* *Our research reveals that the reasons for the hiring shortfall are less about funding, than an insufficient pool of suitable candidates. While the sophistication of cyber-threats and a broadening landscape that requires security oversight e.g. mobile devices, cloud-based services, and the Internet of Things and the skills to identify, analyse, manage and prevent cyber-related attacks are becoming more demanding.* *Despite increased industry demand for specific ICT skills, the take-up of ICT related tertiary courses in Australia over the last decade has halved. A 2014 analysis by the Australian Financial Review of university course take-up by domestic undergraduate students since 2001 shows a 36% decline in students. While the mismatch between the needs of industry and tertiary graduate qualifications is a general one impacting the whole of the ICT industry, it particularly affects dynamic and rapidly changing areas of technologies which is specifically relevant for cyber security"*[4] To address the skill shortage the government's Australian cyber security strategy paper states: *"To build tomorrow's workforce, the Federal Government will work in partnership with the private sector and academic institutions to improve cyber security education at all levels of the education system. This will help to ensure Australia develops a workforce with the right skills and expertise*

[2] **Australian Cyber Security Strategy Page 50**

[3] **Australian Cyber Security Strategy Page 52 Para 1 Col 1**

[4] **Telstra Cyber Security report 2016 Page 9 Col 1 Para 2**

	that can help all Australian take full advantage of the opportunities in cyber space. The most urgent need is for highly skilled cyber security professionals. Academic centres of excellence will enhance the quality of cyber security courses, teachers and professionals in Australia. The centres will deliver undergraduate and postgraduate cyber security education through a consistent curriculum and quality teaching. The profile of these centres will also help to inspire students to think about careers in cyber security and study STEM subjects (science, technology, engineering and mathematics) at school. In addition, the Government will work with the private sector, the States and Territories and Skill Service Organisations to support the expansion of cyber security training in Registered Training Organisations (RTOs) including TAFEs and potentially include the development of a cyber security apprenticeship.’[5] As part of the Government initiatives Box Hill Institute received a substantial funding grant to develop, promote and enhance delivery of cyber security training and increase the placement of its IT graduates into cyber security jobs. The Institute initially customised the current Certificate IV in IT course (ICT40115) to strengthen the cyber security focus. An extensive training needs analysis was undertaken by the Institute in conjunction with industry organisations resulting in the development of recently accredited 22334VIC - Certificate IV in Cyber Security. This initiative has been followed by the development of the Advanced Diploma of Cyber Security. The advanced diploma level qualifcation in the ICT Training Package was also found to be lacking in cyber security content and other units were considered by the Project Steering Committee to be out of date. To sufficiently address the industry requirements at this level a new course was deemed to be necessary. The Advanced Diploma of Cyber Security contains a significant number of new units of competency based on the outcome of a DACUM session undertaken with key industry stakeholders. It also includes a selection of existing Diploma/Advance Diploma ICT units. Details of the DACUM session are available as a separate document. Following the development of the 20 new units, a knowledge/skills and unit of competency matrix was prepared to demonstrate how both the new and imported units support the knowledge and skills identified in the DACUM session (refer Appendix 1). A summary of the knowledge and Skills outcomes of this course are as follows: • manage and maintain cyber security in an organisation which includes: – monitoring the risk of cyber security attacks – gathering, analysing and interpreting threat data – protecting critical infrastructure and configuring security devices – evaluating and implementing appropriate security software – implementing and using a range of tools and procedures to mitigate cyber security threats – protecting an organisation from insider security breaches

[5] **Australian Cyber Security Strategy Page 52 Col 2 Para 6**

  - developing systems to minimise network vulnerabilities and risks

- coordinate security projects which could include both internal and external expertise and resources
- ensure an organisation's security policies, processes, procedures and codes of practice are consistent and inline with relevant security standards, laws and codes of practice

It is most likely that a cyber security practitioner at this level would be working as part of a team in a medium or large oraganisation or providing freelance security consultancy services to a small enterprise which would not have the resource to employ full time cyber security staff.

It is envisaged the learners undertaking this course will have varying backgrounds. Some will be post Yr.11/12 students seeking to study for a career in the IT/cyber security industry. Other participants will be undertaking the course as a pathway to a career change. The third group of participants will be those seeking formal recognition of their work experience in the cyber security field and will be combining RPL and further training to gain a recognised qualification.

It is envisaged initial enrolment numbers in the new course will be approximately 80 to 100 applicants per year. However, as greater awareness of cyber security employment opportunities grows through the various Government initiatives and business demand for practitioners, the number of applicants per year is expected to increase.

The course development work was guided by a Steering Committee representing a number of major organisations which have a vested interest in cyber security training. The committee met four times during the life of the project.

Membership of the Steering Committee comprised:

- Grant McKechnie (Chair) - NBN Co
- Andreas Dannert – Information Systems, Audit and Control Association (ISACA)
- Pamela O'Shea – BAE Systems
- Russell Brown/Helaine Leggat – Australian Information Security Association (AISA)
- Dominic Schipano – Communication, Information and Technology Training (CITT)
- Jamie Rossato – NAB
- Robert Cumming – REA Group
- Karol Szwed – Telstra
- Matt Carling – Cisco (Web ex)

In attendance:

- George Adda - CMM - Engineering Industries
- Stephen Besford– Box Hill Institute
- Jane Young – Box Hill Institute

The Advanced Diploma in Cyber Security is not covered by a suitable qualification within a training package nor does it duplicate by title or coverage the outcomes of any endorsed unit/s of competency from a training package.

3.2 Review for re-accreditation	Not applicable
4. **Course outcomes**	***Standards 1, 2, 3, 4, 5 and 6 AQTF Standards for Accredited Courses***
4.1 Qualification level	*Standards 1, 2 and 3 AQTF Standards for Accredited Courses* This course is aligned with Level 6 of the Australian Qualifications Framework (AQF) in that: **Knowledge:** Graduates will have a specialised and integrated technical and theoretical knowledge with depth in the field of cyber security. **Skills:** Graduates of the Advanced Diploma will have: • Cognitive and communication skills to identify, analyse and act on cyber security risks, threats and incidents in an organisation • Cognitive and communication skills to transfer knowledge and skills to others concerning cyber security risks in workplace practices • and to demonstrate specialised knowledge in mitigation strategies • Cognitive and communication skills to formulate responses to complex cyber security problems such as protecting critical infrastructure • Wide-ranging specialised technical, creative or conceptual skills to express ideas and perspectives on compliance issues and design methodologies to improve an organisation's cyber security **Application of knowledge and skills:** Graduates of the Advanced Diploma of Cyber Security will demonstrate the application of knowledge and skills: • With depth in areas of organisational data security in a context subject to ongoing change • With initiative and judgement plan, design and manage cyber security projects with some direction • To adapt a range of fundamental principles and complex techniques to known and unknown cyber security situations • Across a broad range of technical cyber security functions with accountability for personal and/or team outputs within an organisational context. ***Volume of Learning:*** The Volume of Learning for the Advanced Diploma in Cyber Security is typically 1.5 - 2 years. This incorporates structured training delivery and opportunities for practice and reinforcement of skills including: self-directed study, research, project work and written assignments.
4.2 Employability skills	*Standard 6 AQTF Standards for Accredited Courses* The Employability Skills for the Advanced Diploma in Cyber Security are summarised in Table 1

Table 1: Summary of the Employability Skills for the Advanced Diploma in Cyber Security

The following table contains a summary of the employability skills for this course. This table should be interpreted in conjunction with the detailed requirements of each unit of competency packaged in this course. The outcomes described here are broad industry requirements.

Employability Skills	**Industry/enterprise requirements for this qualification include the following facets. On successful completion of the course a graduate should be able to:**
Communication	• Research, organise, analyse and communicate complex information from reference texts, vendor catalogues and cyber security magazines, websites, use of phone, email and fax • Communicate effectively across a range of communication networks in the workplace • Write technical reports for appropriate management that includes analysis and/or research • Present information to appropriate management in a systematic and concise manner • Use cyber security terminology and language appropriate to the situation and target audience • Contribute to the enhancement of the organisation’s instruction response plan
Teamwork	• Work alone or as part of a team that may include other security practitioners, engineers and management personnel • Provide clear and precise information to team members • Delegate and supervise work where appropriate • Contribute effectively to the teams problem solving requirements
Problem solving	• Analyse information and data from log files, data streams, and test results including determining trends from databases, data lists or graphical data. In conjunction with collegues and/or supervisors recommend solutions to cyber security related problems • Where appropriate apply mathematical techniques and scientific principles to logged data sets • Effectively contribute to the teams troubleshooting methodology
Initiative and enterprise	• Apply statistical processes to make recommendations solutions for equipment and process improvements • Make modifications to work plans and schedules to overcome unforeseen difficulties or developments • Escalate incidents according to company policies
Planning and organising	• Organise, sort, categorise and sequence information • Select and use planning techniques and tools to plan, sequence and prioritise work operations • Prepare, monitor and review work plans, schedules, programs and contribute to budgeting issues

Self-management	• Carry out work within given timeframe, process and quality constraints • Carry out work safely and in accordance with company policy and procedures and legislative requirements • Monitor work to ensure compliance with legislation, codes and national standards
Learning	• Adapt own competence in response to change • Update own knowledge and skills required for cyber security and related disciplines
Technology	• Use test equipment to perform risk assessment and protect critical infrastructure • Use computers and printers to prepare reports • Implement and monitor the application of OH&S procedures • Implement and use security protection devices and software • Secure cloud services • Perform digital forensic investigation on workstations and mobile devices.
4.3 Recognition given to the course	*Standard 5 AQTF Standards for Accredited Courses* Not applicable
4.4 Licensing/ regulatory requirements	*Standard 5 AQTF Standards for Accredited Courses* There are no licensing or regulatory requirements relating to this course.

5. Course rules

Standards 2, 6,7 and 9 AQTF Standards for Accredited Courses

5.1 Course structure

To be awarded the Advanced Diploma of Cyber Security participants must complete a total of twenty (20) units consisting of:

- nine (9) core units*, plus*
- eleven (11) elective units

A minimum of two units must be selected from each of the four (4) elective streams (General, Intrusion Analyst, Penetration Testing and Security Engineering streams). The remaining three (3) units may be selected from the four (4) elective streams or from any endorsed Training Package or accredited course at Diploma level or above where they are consistent with the vocational outcomes of the course.

Units selected from other training packages or accredited courses must not duplicate units selected from the core or elective streams

Participants who do not complete all the requirements for the course will be issued with a Statement of Attainment listing the unit(s) attained.

Table 2: Course structure

Unit code	Field of Education code (six-digit)	Unit Title	Pre-requisite	Nominal hours
Core units:				
BSBWOR502		Lead and manage team effectiveness	Nil	60
ICTNWK525		Configure an enterprise virtual computing environment	Nil	60
VU22240	029901	Communicate cyber security incidents within the organisation	Nil	40
VU22241	029901	Interpret and utilise key security frameworks, policies and procedures for an organisation	Nil	40
VU22242	029901	Assess and secure cloud services	Nil	80
VU22243	029901	Develop software skills for the cyber security practitioner	Nil	80
VU22244	029901	Implement best practices for identity management	Nil	40
VU22245	029901	Plan and implement a cyber security project	VU22240 VU22243 VU22244	80
VU22246	029901	Evaluate an organisation's compliance with relevant cyber security standards and law	Nil	40
			Total core unit hours	**520**

Elective units: Select eleven (11) consistent with the above packaging requirements				
General:				
VU22247	029901	Acquire digital forensic data from workstations	Nil	40
VU22248	029901	Acquire digital forensic data from mobile devices	Nil	40
VU22249	029901	Perform a security risk assessment for an organisation	Nil	40
ICTNWK607		Design and implement wireless network security	Nil	60
ICTNWK531		Configure an internet gateway	Nil	40
ICTSAS505		Review and update disaster recovery and contingency plans	Nil	30
ICTNWK502		Implement secure encryption technologies	Nil	20
ICTNWK503		Install and maintain valid authentication processes	Nil	25
Stream A: Intrusion Analysis				
VU22250	029901	Respond to cyber security incidents	Nil	40
VU22251	029901	Gather, analyse and interpret threat data	Nil	40
VU22252	029901	Implement cyber security operations	Nil	60
ICTSAS501		Develop, implement and evaluate an incident response plan	Nil	30
ICTNWK513		Manage system security	Nil	50
Stream B: Penetration Testing				
VU22253	029901	Undertake penetration testing of the security infrastructure for an organisation	Nil	80
VU22254	029901	Undertake advanced penetration testing for web site vulnerabilities	Nil	80
VU22255	029901	Evaluate threats and vulnerabilities of Internet of Things (IoT) devices	Nil	40
Stream C: Security Engineering				
VU22256	029901	Protect critical infrastructure for an organisation	Nil	40
VU22257	029901	Configure security devices for an organisation	Nil	80
VU22258	029901	Design and implement a virtualised cyber security infrastructure for an organisation	ICTNWK525	80
VU22259	029901	Utilise design methodologies for security architecture	Nil	40
ICTNWK509		Design and implement a security perimeter for ICT networks	Nil	60
ICTTEN811		Evaluate and apply network security	Nil	60
			Range of elective nominal hours	**425 - 690**
			Total nominal hours for the course	**945 - 1210**

5.2 Entry requirements	*Standard 9 AQTF Standards for Accredited Courses* There are no formal entry requirements for this course however, participants are best equipped to achieve the course outcomes if they have completed: – 22334VIC Certificate IV in Cyber Security or equivalent or – Minimum 2 years cyber security work experience In addition, participants should have demonstrated capacity in the learning, reading, writing and numeracy competencies to Level 3 of the Australian Core Skills Framework (ACSF). See http://education.gov.au/search/site/ACSF Applicants who have a lower level of language, literacy and numeracy skills may require additional support to successfully complete the course
6. Assessment	**Standards 10 and 12 AQTF Standards for Accredited Courses**
6.1 Assessment strategy	All assessment, including Recognition of Prior Learning (RPL) must be compliant with: • Standard 1.2/1.5 of the Australian Quality Training Framework (AQTF): *Essential Conditions and Standards for Initial/Continuing Registration* or; • Standard 1, Clauses 1.1 and 1.8 of the *Standards for Registered Training Organisations (RTOs) 2015,* see http://www.asqa.gov.au/about/australias-vet-sector/standards-for-registered-training-organisations-(rtos)-2015.html or; • The relevant Standards for Registered Training Organisations in effect at the time of assessment. Assessment strategies must therefore ensure that: • all assessments are valid, reliable, flexible and fair • learners are informed of the context and purpose of the assessment and the assessment process • feedback is provided to learners about the outcomes of the assessment process and guidance given for future options • time allowance to complete a task is reasonable and specified to reflect the industry context in which the task takes place. Assessment strategies should be designed to: • cover a range of skills and knowledge required to demonstrate achievement of the course aim • collect evidence on a number of occasions to suit a variety of contexts and situations • be appropriate to the knowledge, skills, methods of delivery and needs and characteristics of learners • be equitable to all groups of learners. Assessment methods are included in each unit and include: • oral and/or written questioning • inspection of final process outcomes • portfolio of documentary on-site work evidence • practical demonstration of required physical tasks

	• investigative research and case study analysis. A holistic approach to assessment is encouraged. This may be achieved by combining the assessment of more than one unit where it better replicates working practice. Units maybe assessed on the job, off the job or a combination of both. Where assessment occurs off the job, then an appropriate simulation must be used where the range of conditions reflects realistic workplace situations. Assessment of the imported unit must reflect the requirements of the Assessment Guidelines for the relevant Training Package.
6.2 Assessor competencies	*Standard 12 AQTF Standards for Accredited Courses* Assessment must be undertaken by a person or persons with competencies compliant with: • Standard 1.4 of the AQTF: *Essential Conditions and Standards for Initial/Continuing Registration,* or • Standard 1, Clauses 1.13, 1.14, 1.15, 1.16 and 1.17 of the *Standards for Registered Training Organisations 2015 (RTOs),* or • The relevant Standards for Registered Training Organisations in effect at the time of assessment. Assessors of the endorsed unit of competence must meet the requirements for assessors specified in the relevant Training Package
7. Delivery	***Standards 11 and 12 AQTF Standards for Accredited Courses***
7.1 Delivery modes	*Standard 11 AQTF Standards for Accredited Courses* The following range of delivery methods may be considered: • work-based training and assessment; • RTO-based training and assessment; • part RTO and part work based training and assessment; • recognition of prior learning combined with further training as required; • full time or part time study. There are no restrictions on offering the program on either a full-time or part-time basis. Delivery methods should encourage collaborative problem solving incorporating practical applications and outcomes and include team based exercises where possible. Some areas of content may be common to more than one element/performance criteria and therefore some integration of delivery may be appropriate. Due to the potential for a dispersed distribution of learners, course providers may wish to consider non-traditional strategies in the delivery of training. The facilitation of distance learning and the achievement of competencies through workplace activities or off-the- job training should be fostered and encouraged where possible.
7.2 Resources	*Standard 12 AQTF Standards for Accredited Courses* General facilities, equipment and other resources required to deliver

	the Advanced Diploma of Cyber Security include: - training facilities and equipment; - access to computers and internet; - access to relevant standards, codes of practice texts and references; - appropriate environmental safeguards - health and safety facilities and equipment; - workplace or a simulated workplace environment, appropriate to the assessment tasks. Training must be undertaken by a person or persons with competencies compliant with: - Standard 1.4 of the *AQTF: Essential Conditions and Standards for Initial/Continuing Registration*, or - Standard 1, Clauses 1.13, 1.14, 1.15, 1.16 and 1.17 of the *Standards for Registered Training Organisations 2015* (SRTOs), or - The relevant Standards for Registered Training Organisations in effect at the time of assessment. Imported units must reflect the requirements for trainers specified in the relevant training package.
8. Pathways and articulation	*Standard 8 AQTF Standards for Accredited Courses* There are no formal arrangements for articulation to other accredited courses or the higher education sector. When arranging articulation providers should refer to the: *AQF Second Edition 2013 Pathways Policy* This course contains nationally endorsed units of competencies. Participants who successfully complete any of these units will be able to gain credit into other qualifications containing these units in any future studies. Likewise, participants who have already completed relevant imported units from previous training, will be granted a credit for the unit/s.
9. Ongoing monitoring and evaluation	*Standard 13 AQTF Standards for Accredited Courses* The Advanced Diploma of Cyber Security will be maintained and monitored by the Curriculum Maintenance Manager (CMM) - Engineering Industries. A formal review of the course will take place at least once during the period of accreditation and will be informed by feedback from : - course participants and graduates - teaching and assessing staff - industry representatives and associations. Any significant changes to the course resulting from course monitoring and evaluation procedures will be reported to the VRQA. Course maintenance and review procedures may also indicate that the course in total should be expired if a suitable qualification becomes available through the development, review or continuous improvement process of a training package.

Section C: Units of competency

Imported units of competency from Training Packages:

BSBWOR502	Lead and manage team effectiveness
ICTNWK502	Implement secure encryption technologies
ICTNWK503	Install and maintain valid authentication processes
ICTNWK509	Design and implement a security perimeter for ICT networks
CTNWK513	Manage system security
ICTNWK525	Configure an enterprise virtual computing environment
ICTNWK531	Configure an internet gateway
ICTNWK607	Design and implement wireless network security
ICTSAS501	Develop, implement and evaluate an incident response plan
ICTSAS505	Review and update disaster recovery and contingency plans
ICTTEN811	Evaluate and apply network security

Units of competency:

VU22240	Communicate cyber security incidents within the organisation
VU22241	Interpret and utilise key security frameworks, policies and procedures for an organisation
VU22250	Respond to cyber security incidents
VU22242	Assess and secure cloud services
VU22247	Acquire digital forensic data from workstations
VU22248	Acquire digital forensics data from mobile devices
VU22255	Evaluate threats and vulnerabilities of Internet of Things (IoT) devices
VU22256	Protect critical infrastructure for an organisation
VU22257	Configure security devices for an organisation
VU22258	Design and implement a virtualised cyber security infrastructure for an organisation
VU22253	Undertake penetration testing of the security infrastructure for an organisation
VU22251	Gather, analyse and interpret threat data
VU22254	Undertake advanced penetration testing for web site vulnerabilities
VU22243	Develop software skills for the cyber security practitioner

VU22244	Implement best practices for identity management
VU22245	Plan and implement a cyber security project
VU22252	Implement cyber security operations
VU22246	Evaluate an organisation’s compliance with relevant cyber security standards and law
VU22249	Perform a security risk assessment for an organisation
VU22259	Utilise design methodologies for security architecture

VU22240 - Communicate cyber security incidents within the organisation

Unit Descriptor	This unit provides the knowledge and skills for a practitioner to communicate the effects of cyber security incidents to appropriate personnel in the organisation. This involves understanding communication styles, setting up and contributing to the team that deals with cyber security incidents for the organisation. It also includes gathering and sorting the appropriate information and presenting it using the appropriate communication style for different groups and personnel in the organisation. No licensing or certification requirements apply to this unit at the time of accreditation.
Employability Skills	This unit contains employability skills.
Application of the Unit	This unit is applicable to individuals working as cyber security practitioners and will support their requirement to communicate effectively in the organisation
Prerequisite Unit/s	Nil

ELEMENT	**PERFORMANCE CRITERIA**
Elements describe the essential outcomes of a unit of competency	Performance criteria describe the required performance needed to demonstrate achievement of the element – they identify the standard for the element. Where bold/italicised text is used, further information or explanation is detailed in the required skills and knowledge and/or the range statement. Assessment of performance is to be consistent with the evidence guide.
1. Compile information on key groups who need to be notified on security breeches	1.1 Information on the organisation's ethical practices and security policies is sought and examined 1.2 Organisational personnel structure documents are identified and collated 1.3 Decision making responsibilities for each organisational group are interpreted and clarified 1.4 Process of escalating an incident to appropriate organisational group/s is identified 1.5 Negotiation process with appropriate groups to address cyber incidents is implemented
2. Collate information on communication styles	2.1 Common communication styles are identified 2.2 Appropriate communication style is identified to explain impact of the incident to different ***organisational groups***
3. Address cyber security incidents	3.1 ***Data sources*** to detect incidents are selected 3.2 Risk impact of the incident is assessed 3.3 Functional tasks within the team are allocated 3.4 Communication expectations within the incident team are determined 3.5 Process for engaging external skilled personnel to deal with incidents is clarified

4. Monitor the teams effectiveness and communication during an incident	4.1	Team functionality is monitored
	4.2	Decision making and communication within the team is monitored
	4.3	Group decision making processes are evaluated and monitored and changes implemented if required
	4.4	Effectiveness of utilising external or extra specific skilled personnel to deal with incidents is assessed
	4.5	Welfare of the staff involved with the incident is monitored
5. Formulate and present appropriate presentations and reports to the organisation	5.1	Appropriate presentations and reports are prepared and for each defined organisational decision making group
	5.2	Effects of high risk incidents are communicated to relevant organisational decision making groups-
	5.3	Feedback from individuals and groups regarding the effectiveness of the incident handling process is reviewed in order to affect incident handling policy changes if required

REQUIRED SKILLS AND KNOWLEDGE

This describes the essential skills and knowledge and their level required for this unit.

Required skills:

- Articulating relevant issues encountered in the work environment
- Reading and accurately interpret documents and reports
- Operating a personal computer
- Assembling, participating in and coordinating a work team
- Problem solving within a team environment
- Evaluating the performance of a work team
- Contributing to the process of enhancing team performance
- Developing a project implementation plan including realistic timelines and allocation of tasks for team members
- Establishing project risk assessment
- Gathering, testing and allocating project resources
- Installing and using software packages
- Preparing technical documentation and reports
- Making presentations

Required knowledge:

- Ethics and communication techniques
- Process of coordinating and managing an incident
- Group collaboration & decision making
- Presentation skills to decision making group
- Data gathering processes
- Identification of data sources
- Communication Styles
- Organisation roles and responsibilities
- Organisation policies and procedures
- Incident response processes
- Escalation practices
- Engaging external contractors

Range Statement

The Range Statement relates to the unit of competency as a whole. It allows for different work environments and situations that may affect performance. Bold / italicised wording in the Performance Criteria is detailed below

Organisational groups *includes but not limited to:*

- Incident response (IR) management or other IR teams
- External consultants
- IT team
- Finance team
- HR team
- Management team

Data sources *includes but not limited to:*

- Log files
- IR software monitoring
- Malware outputs
- Operating system alerts and flags

EVIDENCE GUIDE

The evidence guide provides advice on assessment and must be read in conjunction with the Performance Criteria, Required Skills and Knowledge, the Range Statement and the Assessment section in Section B of the accreditation submission.

Critical aspects for assessment and evidence required to assess competency in this unit

To be considered competent in this unit assessors must be satisfied the candidate can demonstrate the achievement of all of the elements of the competency to the level defined by the associated performance criteria

Specifically they must be able to:

- use appropriate communication style for different decision making groups in the organisation;
- develop communication strategies for the Incident Response (IR) team and relevant organisational groups;
- monitor IR teams communication and performance effectiveness;
- prepare relevant presentations and reports to key organisation decision making groups.

Context of and specific resources for assessment

Evidence should show competency working in a realistic environment and a variety of conditions. The candidate must have access to all tools, equipment, materials and documentation required. The candidate will be permitted to refer to any relevant workplace procedures, product and manufacturing specifications, codes, standards, manuals and reference materials.

This unit may be assessed on the job, off the job or a combination of both. Where assessment occurs off the job, an appropriate simulation must be used where the range of conditions reflects realistic workplace situations. The competencies covered by this unit would be demonstrated by an individual working alone or as part of a team. The assessment environment should not disadvantage the candidate.

Method of assessment

Evidence can be gathered in a variety of ways including:

- observation of processes and procedures

- oral and/or written questioning on required knowledge and skills
- testimony from supervisors, colleagues, clients and/or other appropriate persons
- inspection of the final product or outcome
- portfolio of documented evidence.

Where performance is not directly observed and/or is required to be demonstrated over a period of time and/or in a number of locations, any evidence should be authenticated by colleagues, supervisors, clients or other appropriate persons.

VU22241 - Interpret and utilise key security frameworks, policies and procedures for an organisation

Unit Descriptor	This unit provides the knowledge and skills to recognise and utilise key security standards, organisations and bodies that offer resources and support to an organisation addressing cyber security risk. Resources are reviewed for potential implementation within the organisation. No licensing or certification requirements apply to this unit at the time of accreditation.
Employability Skills	This unit contains employability skills.
Application of the Unit	This unit is applicable to individuals working as cyber security paraprofessionals who will select, interpret and implement existing frameworks, policies and standards in the organisation.
Prerequisite Unit/s	Nil

ELEMENT	**PERFORMANCE CRITERIA**	
Elements describe the essential outcomes of a unit of competency.	Performance criteria describe the required performance needed to demonstrate achievement of the element – they identify the standard for the element. Where bold/italicised text is used, further information or explanation is detailed in the required skills and knowledge and/or the range statement. Assessment of performance is to be consistent with the evidence guide.	
1. Collate security frameworks, risk mitigation strategies and other supportive documents	1.1	***Key standards bodies and organisations that provide useful cyber security resources*** that improve an organisation’s security capability are identified
	1.2	***Key Australian cyber security mitigation strategies*** that improve an organisation’s security are collated
	1.3	***Key overseas cyber security incident mitigation strategies*** that improve an organisation’s security are accessed and collated
	1.4	***Current working frameworks or practices*** that can support an organisation to improve its security capabilities are identified
	1.5	***Current Australian cyber security legal and ethics documents*** are identified
	1.6	Emerging ***guidelines for security relating to Internet of Things (IOT)*** are identified
2. Evaluate key information from these documents that will support the organisation to improve its security infrastructure	2.1	Australian compliance standards are identified and evaluated for an organisation
	2.2	Compulsory Australian cyber security legal and ethics documents are identified for the organisation
	2.3	Key strategies to mitigate cyber security risks are identified and evaluated
	2.4	Good practice frameworks for the organisation are identified and evaluated

3. Select relevant security frameworks, cyber security incident mitigation strategies and other supportive documents	3.1	In consultation with key personnel, necessary key incident response strategies for the organisation are selected
	3.2	In consultation with key personnel, appropriate working practices for the organisation are selected
4. Implement the security frameworks and cyber security incident mitigation strategies	4.1	In consultation with key personnel, appropriate compliance standards for the organisation are implemented
	4.2	In consultation with key personnel, current Australian cyber security legal and ethics documents are implemented
	4.3	In consultation with key personnel, organisational processes and procedures to implement key incident response strategies are adopted or altered
	4.4	In consultation with key personnel, training for organisational staff to adopt new or alter current working practices to improve the security culture is planned and implemented
	4.5	In consultation with key personnel, appropriate working practices for the organisation are implement
5. Monitor the effectiveness of the organisation's implementation of the security frameworks and cyber security incident mitigation strategies	5.1	List of criteria that measures the effectiveness of implemented changes to working practices is created
	5.2	Effectiveness of changes to organisational processes and procedures that deal with strategies that address incident responses are monitored
	5.3	Effectiveness of changes made to working practices for the organisation are monitored

REQUIRED SKILLS AND KNOWLEDGE

This describes the essential skills and knowledge and their level required for this unit.

Required skills:

- Articulating relevant issues encountered in the work environment
- Reading and accurately interpret documents and reports
- As part of a team determine changes required to work practices to implement new policies and procedures
- Assembling, participating in and coordinating a work team
- Problem solving within a team environment
- Contributing to the process of enhancing team performance
- Establishing project risk assessment
- Gathering, testing and allocating project resources
- Preparing technical documentation

Required knowledge:

- Australian Signals Directorate (ASD) Top 8 (https://www.asd.gov.au/infosec/mitigationstrategies.htm)
- Relevant aspects of the Australian Cybercrime Act
- Relevant aspects of the Australian Telecommunications Act
- German Federal Office for Security in Information Technology (BSI) Grundschutz Catalogue (https://www.bsi.bund.de/EN/Topics/ITGrundschutz/ITGrundschutzCatalogues/itgrundschutzcatalogues_node.html)
- Relevant aspects of the National Institute of Standards and Technology (NIST) Cybersecurity Framework
- Relevant aspects of the European Union Agency for Network and Information Security (ENISA) https://www.enisa.europa.eu
- Security standards, frameworks and resources including:
  - ISO/IEC 2700X
  - Control Objectives for Information and Related Technologies (COBIT)
  - Information Technology Infrastructure Library (ITIL)
  - Open Web Application Security Project (OWASP)
  - Cloud Security Alliance (CSA)
  - Australian Signals directorate (ASD) Information Security Manual (ASD ISM)
- IoT Alliance Australia: Internet of Things Security Guideline (https://static1.squarespace.com/static/573853ed1d07c093e27aefd2/t/58ab9bf8ebbd1a2b74e2aa2d/1487641596432/IoTAA+Security+Guideline+V1.0.pdf)
- Legal aspects of relevant standards and procedures
- Differences between security frameworks, policies, standards, procedures and guidelines
- Standard frameworks within a business context
- Policies, standards and procedures effectiveness (Continuous improvement)
- New technologies in context of industry standards and frameworks (e.g. Applying Cloud Security Alliance Security, Trust & Assurance Registry (CSA STAR), Information security Manual (ISM) principles)

Range Statement

The Range Statement relates to the unit of competency as a whole. It allows for different work environments and situations that may affect performance. Bold / italicised wording in the Performance Criteria is detailed below

Key standards bodies and organisations that provide useful cyber security resources *includes but not limited to:*

- Australian Signals Directorate (ASD)
- ISO/IEC
- National Institute of Standards and Technology (NIST)
- European Union Agency for Network and Information Security (ENISA)
- BSI Grundschutz
- Australian Centre for Cyber Security (ACCS)
- IoT Alliance Australia etc.

Key Australian cyber security mitigation strategies *includes but not limited to:*

- Australian Signals Directorate (ASD) Strategies to mitigate cyber security incidents https://www.asd.gov.au/infosec/mitigationstrategies.htm

Key overseas cyber security incident mitigation strategies *includes but not limited to:*

- European Union Agency for Network and Information Security (ENISA) https://www.enisa.europa.eu
- BSI Grundschutz Catalogue (https://www.bsi.bund.de/EN/Topics/ITGrundschutz/ITGrundschutzCatalogues/itgrundschutzcatalogues_node.html

Current working frameworks or practices *includes but not limited to:*

- Control Objectives for Information and Related Technologies (COBIT)
- Information Technology Infrastructure Library (ITIL)

Current Australian cyber security legal and ethics documents *includes but not limited to:*

- Australian Cybercrime Act
- Australian Centre for Cyber Security - Australian Cyber Strategy, Law and Policy

Guidelines for security relating to Internet of Things (IOT) *includes but not limited to:*

- IoT Alliance Australia: Internet of Things Security Guideline (https://static1.squarespace.com/static/573853ed1d07c093e27aefd2/t/58ab9bf8ebbd1a2b74e2aa2d/1487641596432/IoTAA+Security+Guideline+V1.0.pdf

EVIDENCE GUIDE

The evidence guide provides advice on assessment and must be read in conjunction with the Performance Criteria, Required Skills and Knowledge, the Range Statement and the Assessment section in Section B of the accreditation submission.

Critical aspects for assessment and evidence required to assess competency in this unit

To be considered competent in this unit assessors must be satisfied the candidate can demonstrate the achievement of all of the elements of the competency to the level defined by the associated performance criteria

Specifically they must be able to:

- Collate security frameworks, legislation, cyber security incident mitigation strategies and other supportive documents for the organisation;
- Evaluate and select relevant security frameworks, cyber security incident mitigation strategies and other supportive documents that will improve the organisation's resilience against cyber incidents;
- Implement and monitor the effectiveness of the organisation's implementation of the security frameworks and cyber security incident mitigation strategies.

Context of and specific resources for assessment

Evidence should show competency working in a realistic environment and a variety of conditions. The candidate will have access to all tools, equipment, materials and documentation required. The candidate will be permitted to refer to any relevant workplace procedures, product and manufacturing specifications, codes, standards, manuals and reference materials.

This unit may be assessed on the job, off the job or a combination of both. Where assessment occurs off the job, an appropriate simulation must be used where the range of conditions reflects realistic workplace situations. The competencies covered by this unit would be demonstrated by an individual working alone or as part of a team. The assessment environment should not disadvantage the candidate.

Method of assessment

Evidence can be gathered in a variety of ways including:

- observation of processes and procedures
- oral and/or written questioning on required knowledge and skills
- testimony from supervisors, colleagues, clients and/or other appropriate persons
- inspection of the final product or outcome
- portfolio of documented evidence.

Where performance is not directly observed and/or is required to be demonstrated over a period of time and/or in a number of locations, any evidence should be authenticated by colleagues, supervisors, clients or other appropriate persons.

VU22250 - Respond to cyber security incidents

Unit Descriptor

This unit provides the knowledge and skills for a paraprofessional working as a team member to prepare for and respond to a cyber security incident within an organisation. The unit includes identifying when the incident occurred, developing and implementing an appropriate response' strategy, evaluate the success of the response and any long term effects of the incident.

The unit also includes the knowledge and skills required to accurately document the incident and update the organisation's incident response plan to reduce the risk of further incidents.

No licensing or certification requirements apply to this unit at the time of accreditation.

Employability Skills

This unit contains employability skills.

Application of the Unit

This unit is applicable to a practitioner working as part of a team responsible for preparing and dealing with cyber security incidents in an organisation

Prerequisite Unit/s

Nil

ELEMENT	**PERFORMANCE CRITERIA**
Elements describe the essential outcomes of a unit of competency.	Performance criteria describe the required performance needed to demonstrate achievement of the element – they identify the standard for the element. Where bold/italicised text is used, further information or explanation is detailed in the required skills and knowledge and/or the range statement. Assessment of performance is to be consistent with the evidence guide.
1. Prepare to respond to an incident	1.1 Procedures to address incidents in the organisation's incident response plan (IRP) are identified and reviewed
	1.2 Organisation's processes to deal with incident responses are benchmarked against ***published incident response strategies***
	1.3 ***Incident response team (IRT) members***~~-~~to deal with the incident are identified
	1.3 IRT member's roles and responsibilities are clearly defined
	1.4 IRT member's communication expectations during incidents are clarified
	1.5 IRT reporting and communication procedures to ***relevant organisational groups*** are defined
	1.6 Function and role of cyber security tools and techniques chosen to detect incidents are defined
	1.7 ***Data sources*** to gather incident information are identified
2. Identify the cyber security incident	2.1 System messages and events to identify malicious activity are evaluated
	2.2 Data is collected from appropriate data sources

	2.3	Initial ***triage*** of the incident is performed
	2.4	Risk assessment of the incident is performed
	2.5	Need to escalate the incident is assessed
2. Respond to the incident	3.1	If required additional team members are recruited to deal with the incident
	3.2	If the incident is part of the organisation's incident response strategy plan, the defined incident response strategy is implement
	3.3	If the incident is not part of the organisation's incident response strategy, a strategy to deal with the incident is planned
	3.4	***Mitigation strategies that quarantine the incident*** are planned and implemented
4. Monitor effectiveness of the strategies to deal with the incident	4.1	Effectiveness of the strategies to deal with the incident are monitored, evaluated and if required modified
	4.2	If required additional team members are recruited to develop strategies to deal with the incident
	4.3	The incident response is escalated where appropriate
	4.4	The incident is communicated within the organisation according to defined communication strategies
5. Evaluate the impact of the incident	5.1	Impact of the incident is evaluated with ***appropriate personnel***
	5.2	Strategies to deal with any lost or compromised data or resources are planned and implemented
6. Communicate and document the incident	6.1	The incident is documented according to standard organisational templates
	6.2	The incident is communicated to relevant personnel within the organisation
7. Implement post incident review and actions	7.1	Existing incident response strategies are reviewed, modified and documented as required
	7.2	New incident response strategies developed for the incident are included in the organisation's incident response strategy procedure's document
	7.3	Incident response procedure is stored for future reference and used when inducting new staff
	7.4	Business plans and processes are evaluated for change if required with appropriate personnel
	7.5	Existing security equipment and security infrastructure are reviewed
	7.6	If required, procurement of new security equipment is organised with appropriate personnel

REQUIRED SKILLS AND KNOWLEDGE

This describes the essential skills and knowledge and their level required for this unit.

Required skills:

- Articulating relevant issues encountered in the work environment
- Reading and accurately interpreting documents and reports
- Operating a personal computer
- Assembling, participating in and coordinating a work team
- Problem solving within a team environment
- Evaluating the performance of a work team
- Contributing to the process of enhancing team performance
- Developing a project implementation plan including realistic timelines and allocation of tasks for team members
- Establishing project risk assessment
- Gathering, testing and allocating project resources
- Installing and using software packages
- Preparing technical documentation
- Making presentation to clients
- Communicating and engaging external contractors
- Escalating procedures
- Working effectively in a stressful environment
- Making clear concise decisions
- Communicating effectively to different working groups
- Contributing to organisation's policies and procedures
- Evaluating new technologies
- Evaluating of policies, standards and procedures effectiveness for continuous improvement

Required knowledge:

- Ethics & communication
- Coordinating/managing an incident
- Group collaboration & decision making
- Presentation skills for decision making groups
- Function and role of the monitoring equipment and software
- Sources of data threats
- Data gathering processes
- Communication styles
- Organisational members roles and responsibilities
- When and who to communicate incidents
- Escalation strategies
- Risk assessment of incidents
- Policies, standards and procedures effectiveness for continuous improvement
- Incident response procedures
- Tools and techniques used in the organisation to deal with incidents
- Required incident response documentation skills

Range Statement

The Range Statement relates to the unit of competency as a whole. It allows for different work environments and situations that may affect performance. Bold / italicised wording in the Performance Criteria is detailed below

Published incident response strategies *includes but not limited to:*	• Australian Signals Directorate (ASD) Strategies to mitigate cyber security incidents https://www.asd.gov.au/infosec/mitigationstrategies.html • European Union Agency for Network and Information Security (ENISA) https://www.enisa.europa.eu • BSI Grundschutz Catalogue (https://www.bsi.bund.de/EN/Topics/ITGrundschutz/ITGrundschutzCatalogues/itgrundschutzcatalogues_node.html
Incident response team (IRT) members *includes but not limited to:*	• Incident response team (IRT) members • IRT Team leader • External consultants
Relevant organisational groups *includes but not limited to:*	• IRT • Information Technology Services (ITS) • Human Resources (HR) • Management
Data sources *includes but not limited to:*	• Data logs • Data log analysis software warnings • Alerts • Database errors
Triage *includes but not limited to:*	• Perform risk assessment • Identify resources required to manage risk • Identify personnel • Communicate observed event
Mitigation strategies that quarantine the incident *includes but not limited to:*	• Blocking Ports • Limiting/blocking user access • Limiting/blocking data services
Appropriate personnel *includes but not limited to:*	• IRT member • IRT manager • External consultants • Relevant managers • Business stakeholders

EVIDENCE GUIDE

The evidence guide provides advice on assessment and must be read in conjunction with the Performance Criteria, Required Skills and Knowledge, the Range Statement and the Assessment section in Section B of the accreditation submission.

Critical aspects for assessment and evidence required to assess competency in this unit

To be considered competent in this unit assessors must be satisfied the candidate can demonstrate the achievement of all of the elements of the competency to the level defined by the associated performance criteria

Specifically they must be able to:

- make adequate preparations to respond to a cyber security incident;
- identify a cyber security incident when it occurs;
- make an appropriate response to the incident;
- monitor the effectiveness of the response strategies that deal with the incident;
- evaluate the incident for any long term effects;
- prepare relevant documentation regarding the incident;
- provide advice on the update of the organisation's incident response plan and the procurement of any additional security equipment.

Context of and specific resources for assessment

Evidence should show competency working in a realistic environment and a variety of conditions. The candidate will have access to all tools, equipment, materials and documentation required. The candidate will be permitted to refer to any relevant workplace procedures, product and manufacturing specifications, codes, standards, manuals and reference materials.

This unit may be assessed on the job, off the job or a combination of both. Where assessment occurs off the job, an appropriate simulation must be used where the range of conditions reflects realistic workplace situations. The competencies covered by this unit would be demonstrated by an individual working as part of a team. The assessment environment should not disadvantage the candidate.

Method of assessment

Evidence can be gathered in a variety of ways including:

- observation of processes and procedures
- oral and/or written questioning on required knowledge and skills
- testimony from supervisors, colleagues, clients and/or other appropriate persons
- inspection of the final product or outcome
- portfolio of documented evidence.

Where performance is not directly observed and/or is required to be demonstrated over a period of time and/or in a number of locations, any evidence should be authenticated by colleagues, supervisors, clients or other appropriate persons.

VU22242 - Assess and secure cloud services

Unit Descriptor

This unit introduces learners to the principles and operation of the cloud model and cloud services. It provides the knowledge and skills to categorise and select cloud services for an organisation as well as the ability to examine the security issues relating to cloud data and services.

The unit also introduces the current industry practices that support an organisation to secure its' cloud based data and application services

No licensing or certification requirements apply to this unit at the time of accreditation.

Employability Skills

This unit contains employability skills.

Application of the Unit

This unit is applicable to individuals working as cyber security paraprofessionals who amongst other security responsibilities oversees' the organisation's cloud based data and cloud services

Prerequisite Unit/s

Nil

ELEMENT Elements describe the essential outcomes of a unit of competency.	**PERFORMANCE CRITERIA** Performance criteria describe the required performance needed to demonstrate achievement of the element – they identify the standard for the element. Where bold/italicised text is used, further information or explanation is detailed in the required skills and knowledge and/or the range statement. Assessment of performance is to be consistent with the evidence guide.
1. Categorise cloud service and deployment models	1.1 ***Cloud service models*** are identified
	1.2 ***Cloud deployment models*** are classified
	1.3 ***Cloud infrastructure*** is defined
	1.4 In consultation with key personnel a risk assessment for cloud based data services is performed
2. Develop a risk management plan for cloud based data storage and services	2.1 Security risks and consequences in accordance with the***, Australian legislative requirements and relevant standards*** for cloud based data and services are identified
	2.2 Acceptable and unacceptable risks for cloud based data storage and services are clearly distinguished and confirmed
	2.3 High priority risks of cloud based data storage and services are emphasised and specified to ensure the development of appropriate controls
	2.4 Existing controls to determine the impact on risk occurrence are evaluated and required modifications identified
	2.5 Risk management plan for cloud based data storage and services for the organisation are documented

3. Implement legal and compliance issues of cloud data and services	3.1	Australian legislative requirements and relevant standards relating to cloud based services for the organisation are identified and evaluated
	3.2	Insurance of cloud data and services are recommended to the ***appropriate organisational bodies***
4. Evaluate, select and implement cloud based services for the organisation	4.1	Cloud service providers for the organisation are evaluated and selected
	4.2	Cloud services to access the organisation’s data are selected and deployed
	4.3	Deployment of cloud micro-services and containers utilised by an organisation are articulated
5. Develop strategies to protect cloud services	5.1	***Key personnel*** tasked to deal with user account management are identified
	5.2	Strategies to secure cloud services are developed for the organisation
	5.3	Back up strategies are developed for the organisation
	5.4	Disaster recovery (DR) strategies are developed for the organisation
	5.5	Strategies for cryptographic key management of cloud services are developed
6. Monitor the effectiveness of strategies developed to protect cloud based data and services for the organisation	6.1	Auditing and monitoring cloud based services and data tools are evaluated, selected and deployed
	6.2	Tools used to audit and monitor cloud based services are evaluated and selected
	6.3	Effectiveness of the selected tools to monitor cloud based data services are evaluated and any recommendations are documented
	6.4	Changes to the strategies and tools used to monitor the cloud services and data are presented to appropriate organisational bodies

REQUIRED SKILLS AND KNOWLEDGE

This describes the essential skills and knowledge and their level required for this unit.

Required skills:

- Articulating relevant issues encountered in the work environment
- Reading and accurately interpret documents and reports
- Determining changes required to work practices to implement new policies and procedures
- Assembling, participating in and coordinating a work team
- Problem solving within a team environment
- Evaluating the performance of a work team
- Contributing to the process of enhancing team performance
- Establishing project risk assessment
- Gathering, testing and allocating project resources
- Preparing technical documentation
- Making presentation to clients
- Interpreting data output from software packages
- Working as part of a team
- Securing cloud services
- Auditing and monitoring cloud services
- Assessing cloud based risk
- Using tools to access cloud based data and employing strategies to secure data
- Evaluating new technologies relating to cloud data and services
- Classifying data and corresponding information security risks

Required knowledge:

- Cloud based storage architectures (IaaS, PaaS, SaaS, CaaS, MaaS, XaaS)
- Cloud deployment models (public cloud, private cloud, single hosted cloud, multi hosted cloud)
- Cloud based risk assessment
- Cloud infrastructure (storage, network and computing)
- Cloud management and monitoring
- Micro-services and containers (docker) in the cloud
- Backup and data recovery (DR) aspects of cloud services
- Government certification, accreditation and compliance implications of cloud services
- Data privacy issues of cloud services
- Options of cryptographic key management when using cloud services
- Risk assessment of cloud based data and services
- Data vulnerabilities of cloud based data storage
- Tools used to access cloud data and their limitations
- Service management principles to deal with cloud based data
- Strategies for protecting data in transit and at rest
- Secure backup strategies
- Legal and regulatory implications associated with using cloud based data storage (e.g. Records retention requirements)
- Data sovereignty risks associated with cloud storage
- Data protection dependencies (e.g. Effective key management processes)

Range Statement

The Range Statement relates to the unit of competency as a whole. It allows for different work environments and situations that may affect performance. Bold / italicised wording in the Performance Criteria is detailed below

Cloud service models *includes but not limited to:*

- Infrastructure as a Service (IaaS)
- Platform as a Service (PaaS)
- Software as a Service (SaaS)
- Monitoring as a Service (MaaS
- Communication as a Service (CaaS)
- Anything as a Service (XaaS)

Cloud deployment models *includes but not limited to:*

- Public Cloud
- Private cloud
- Single hosted cloud
- Multihosted cloud

Cloud infrastructure *includes but not limited to:*

- On demand services
- Products
- Virtual servers
- Virtual PC's
- Virtual switches
- Storage clusters
- Networking

Australian legislative requirements and relevant standards *includes but not limited to:*

- Privacy Act 1988 (Cth) and its Australian Privacy Principles
- Australian Cybercrime Act 2001
- Australian Spam Act 2003
- Telecommunications (Interception & Access) Act 1979
- Australian Centre for Cyber Security - Australian Cyber Strategy, Law and Policies

Appropriate organisational bodies *includes but not limited to:*

- Information Technology Services (ITS)
- Human Resources (HR)
- Management

Key personnel *includes but not limited to:*

- Cyber security paraprofessional
- Cyber security manager
- External consultants
- Relevant managers
- Auditors
- Business stakeholders

EVIDENCE GUIDE

The evidence guide provides advice on assessment and must be read in conjunction with the Performance Criteria, Required Skills and Knowledge, the Range Statement and the Assessment section in Section B of the accreditation submission.

Critical aspects for assessment and evidence required to assess competency in this unit

To be considered competent in this unit, assessors must be satisfied the candidate can demonstrate the achievement of all of the elements of the competency to the level defined by the associated performance criteria.

Specifically they must be able to:

- Categorise cloud service and deployment models;
- Implement legal and compliance issues of cloud data and services;
- Select cloud based services for the organisation;
- Develop strategies to protect cloud services and monitor their effectiveness.

Context of and specific resources for assessment

Evidence should show competency working in a realistic environment and a variety of conditions. The candidate will have access to all tools, equipment, materials and documentation required. The candidate will be permitted to refer to any relevant workplace procedures, product and manufacturing specifications, codes, standards, manuals and reference materials.

This unit may be assessed on the job, off the job or a combination of both. Where assessment occurs off the job, an appropriate simulation must be used where the range of conditions reflects realistic workplace situations. The competencies covered by this unit would be demonstrated by an individual working alone or as part of a team. The assessment environment should not disadvantage the candidate.

Method of assessment

Evidence can be gathered in a variety of ways including:

- observation of processes and procedures
- oral and/or written questioning on required knowledge and skills
- testimony from supervisors, colleagues, clients and/or other appropriate persons
- inspection of the final product or outcome
- portfolio of documented evidence.

Where performance is not directly observed and/or is required to be demonstrated over a period of time and/or in a number of locations, any evidence should be authenticated by colleagues, supervisors, clients or other appropriate persons.

VU22247 - Acquire digital forensic data from workstations

Unit Descriptor	This unit provides the knowledge and skills to enable participants to select tools and apply techniques to gather and validate digital forensic data from workstations by physical or virtual means or through email or web applications The unit is not intended to prepare the practitioner to gather evidence for legal purposes. No licensing or certification requirements apply to this unit at the time of accreditation.
Employability Skills	This unit contains employability skills.
Application of the Unit	This unit is applicable to individuals working as cyber security paraprofessionals and as part of a team that responds to cyber security incidents
Prerequisite Unit/s	Nil

ELEMENT	**PERFORMANCE CRITERIA**	
Elements describe the essential outcomes of a unit of competency.	Performance criteria describe the required performance needed to demonstrate achievement of the element – they identify the standard for the element. Where bold/italicised text is used, further information or explanation is detailed in the required skills and knowledge and/or the range statement. Assessment of performance is to be consistent with the evidence guide.	
1. Examine relevant privacy laws pertaining to digital forensics	1.1	Difference between acquiring digital data and digital forensics is clarified
	1.2	Processes of forensic science and investigation are identified
	1.3	***Current Australian privacy laws and digital forensic legislation*** are collated and evaluated
	1.4	If required, changes to the organisation's digital forensic policies and practices are implemented
2 Define data to be recovered and evaluate and select digital forensic tools	2.1	***Forensic data to be recovered from the workstation*** is defined
	2.2	***Triage principles for acquiring and securing data*** for the organisation are developed
	2.3	***Tools for digital forensics*** are identified, evaluated and selected
3. Acquire defined forensic data from storage media	3.1	Structure and operation of the Windows file structures is articulated
	3.2	Structure and operation of the MAC operating system (OS) file structure is articulated
	3.3	Structure and operation of the Unix file structure is articulated
	3.4	Forensic data provided by the windows registry structure and

		content is identified and evaluated
	3.5	Data from ***disk drives*** is acquired
	3.6	Universal Serial Bus (USB) and bring your own device (BYOD) connection and disconnection times are determined
	3.7	Disk file open and file closure times are determined
4. Acquire defined email forensic data	4.1	Structure and operation of an email packet is reviewed
	4.2	***Different types of email formats*** are examined
	4.3	***Common forensic email tools*** are identified, evaluated and selected
	4.4	Email senders geographic locations are determined
5. Acquire defined web forensic data	5.1	Existing ***web browser structures*** and operation are reviewed
	5.2	***Common browser forensic tools*** are identified, evaluated and selected
	5.3	Tools and techniques to examine web forensic data are identified, evaluated and selected
	5.4	***Web forensic data*** for a particular browser is collated
6. Review defined recovered data	6.1	Defined data from storage media, email and the web is collated
	6.2	Acquired data is reviewed and checked for readability and completeness
	6.3	Report on the acquired data is compiled and discussed with appropriate personnel
7. Identify further data forensic tools and training	7.1	Advanced data collection forensic tools are identified and classified
	7.2	Forensic training and certifications are identified and completed

REQUIRED SKILLS AND KNOWLEDGE

This describes the essential skills and knowledge and their level required for this unit.

Required skills:

- Articulating relevant issues encountered in the work environment
- Reading and accurately interpreting documents and reports
- Operating a personal computer
- Assembling, participating in and coordinating a work team
- Problem solving within a team environment
- Evaluating the performance of a work team
- Contributing to the process of enhancing team performance
- Installing and using software packages
- Preparing technical documentation
- Making presentation to clients
- Communicating and engaging external contractors
- Escalation procedures
- Working calmly in a stressful environment
- Making clear decisions
- Communicating effectively to different working groups
- Operating system tools to gather forensic data
- Using tools to acquire disk forensic data
- Using tools to acquire email forensic data
- Using tools to acquire web forensic data
- Communicating and report writing for forensics

Required knowledge:

- Ethics and Digital forensics
- Digital forensic legislation
- Introduction to forensic science and investigation
- Hardware and operating system administration
- File system structures
  - Windows
  - Unix/Linux
  - MAC OS
- Digital forensic tools and techniques for
  - Storage files
  - Email
  - Web
- Methodological problem solving

Range Statement

The Range Statement relates to the unit of competency as a whole. It allows for different work environments and situations that may affect performance. Bold / italicised wording in the Performance Criteria is detailed below

Current Australian privacy laws and digital forensic legislation *includes but not limited to:*	• Australian Government Privacy Act 1988 • Victorian privacy and protection act 2014 • A Concise Guide to Various Australian Laws Related to Privacy and Cybersecurity Domains SANs Institute Reading room
forensic data to be recovered from the workstation *includes but not limited to:*	• Data from storage media • Email data • Web based data
Triage principles for acquiring and securing data *includes but not limited to:*	• Live triage processes • Post-mortem process
Tools for digital forensics *includes but not limited to:*	• EnCase • FTK (Access Data Forensic Toolkit) • X-Ways • iLook • SMART • WinHex • HELIX • md5sum • DriveSpy • FTK Imager • BlackBug • WinHex • WindowsSCOPE • Regripper and regripper plug-ins • TZWork • Tools.WFT (Windows forensic Toolchest) • Linux Evidence Collection Tool (LECT)
Disk drives *includes but not limited to:*	• Standard platted based drives • Solid State (SSD)
Different types of email formats *includes but not limited to:*	• Microsoft Outlook • Web-Based mail • Microsoft Exchange and Office 365
Common forensic email tools *includes but not limited to:*	• Nuix • MailXaminer • Add4Mail • eMailTrackerPro • Paraben E-Mail Examine

Web browser structures *includes but not limited to:*	• Internet Explorer • Firefox • Chrome • Microsoft Edge
Common browser forensic tools *includes but not limited to:*	• Nirsoft Tools • Woanware ChromeForensics • SQLite Manager • Hindsight
Web forensic data *includes but not limited to:*	• File locations • History files • Cache index timestamps • Download History

EVIDENCE GUIDE

The evidence guide provides advice on assessment and must be read in conjunction with the Performance Criteria, Required Skills and Knowledge, the Range Statement and the Assessment section in Section B of the accreditation submission.

Critical aspects for assessment and evidence required to assess competency in this unit	To be considered competent in this unit assessors must be satisfied the candidate can demonstrate the achievement of all of the elements of the competency to the level defined by the associated performance criteria Specifically they must be able to: • Evaluate and select digital forensic tools for the organisation • Using digital forensic tools, acquire defined forensic data from storage media • Using digital forensic tools to acquire email forensic data • Using digital forensic tools, acquire defined web forensic data
Context of and specific resources for assessment	Evidence should show competency working in a realistic environment and a variety of conditions. The candidate will have access to all tools, equipment, materials and documentation required. The candidate will be permitted to refer to any relevant workplace procedures, product and manufacturing specifications, codes, standards, manuals and reference materials. This unit may be assessed on the job, off the job or a combination of both. Where assessment occurs off the job, an appropriate simulation must be used where the range of conditions reflects realistic workplace situations. The competencies covered by this unit would be demonstrated by an individual working alone or as part of a team. The assessment environment should not disadvantage the candidate.
Method of assessment	Evidence can be gathered in a variety of ways including: - observation of processes and procedures - oral and/or written questioning on required knowledge and skills - testimony from supervisors, colleagues, clients and/or other appropriate persons - inspection of the final product or outcome - portfolio of documented evidence. Where performance is not directly observed and/or is required to be demonstrated over a period of time and/or in a number of locations, any evidence should be authenticated by colleagues, supervisors, clients or other appropriate persons.

VU22248 - Acquire digital forensic data from mobile devices

Unit Descriptor	This unit provides the knowledge and skills to enable participants to select tools and apply techniques to gather and validate digital forensic data from mobile devices The unit is not intended to prepare the practitioner to gather evidence for legal purposes. No licensing or certification requirements apply to this unit at the time of accreditation.
Employability Skills	This unit contains employability skills.
Application of the Unit	This unit is applicable to individuals working as cyber security paraprofessionals and as part of a team that respond to cyber security incidents
Prerequisite Unit/s	Nil

ELEMENT		**PERFORMANCE CRITERIA**
Elements describe the essential outcomes of a unit of competency.		Performance criteria describe the required performance needed to demonstrate achievement of the element – they identify the standard for the element. Where bold/italicised text is used, further information or explanation is detailed in the required skills and knowledge and/or the range statement. Assessment of performance is to be consistent with the evidence guide.
1. Determine relevant privacy laws, procedures and processes pertaining to mobile digital forensics	1.1	Difference between acquiring digital data and digital forensics is clarified
	1.2	Process of forensic science and investigation is identified
	1.3	***Current Australian privacy laws and mobile digital forensic legislation*** is collated and evaluated
	1.4	If required, changes to the organisation's mobile digital forensic policies and practices are implemented
	1.5	***Current mobile forensic procedures and processes*** are investigated
	1.6	***Layered models of mobile forensic data acquisition*** are defined and evaluated
2 Determine smartphone fundamentals and select mobile digital forensic tools	2.1	***Smartphone fundamentals*** are defined and articulated
	2.2	Components of, and foundational operation of the of the digital cellular network are investigated
	2.3	***Mobile forensic data tools*** are identified and evaluated
3. Define smartphone architecture and file structure	3.1	Structure and operation of the Android, file structure are clarified
	3.2	Structure and operation of the Apple iOS (macOS) file structure is articulated

	3.3	Structure and operation of the Nokia Symbian file structure is articulated
	3.4	Structure and operation of the Windows Phone file structure is articulated
4. Acquire mobile forensic data	4.1	Software drivers, cables and tools to synchronise phone data with a workstation from a phone are evaluated and selected
	4.2	***Key data to be acquired from a mobile device*** is identified
	4.3	Mobile forensic data tool to acquire key data for the phone is selected
	4.4	Mobile forensic data tool selected is installed and commissioned
	4.5	Users are familiarised with the tool selected to acquire the mobile device data
	4.6	Data from the mobile device is acquired
5. Review defined recovered data	5.1	Acquired data from the mobile device is collated
	5.2	Acquired data is checked for readability and completeness
	5.3	Report on the acquired data is compiled and discussed with appropriate personnel
6. Investigate the function and operation of further tools and techniques for mobile devices	6.1	Joint Test Action Group (JTAG) methods and tools to acquire and analyse data from mobile devices are identified
	6.2	Data encryption use in mobile devices is researched
	6.3	Cloud based mobile forensic tools are evaluated and selected
	6.4	Tools and techniques to examine mobile forensic data on Universal Integrated Circuit Card (UICC) devices are evaluated and selected
	6.5	Hardware tools used to acquire erased data files for mobile devices are researched
7. Identify further mobile data forensic tools and training	7.1	Developments in mobile data collection forensic tools are identified and classified
	7.2	Mobile forensic training and certification is planned and conducted

REQUIRED SKILLS AND KNOWLEDGE

This describes the essential skills and knowledge and their level required for this unit.

Required skills:

- Reading and interpreting technical documents, papers, vendor product specifications, reports and research papers
- Operating a personal computer
- Installing and using software packages
- Preparing technical documentation
- Working calmly in a stressful environment
- Making clear decisions
- Communicating effectively to different working groups
- Using tools to acquire mobile device forensic data
- Using digital forensic tools and techniques
- Communicating and report writing for forensics

Required knowledge:

- Ethics and Digital forensics
- Mobile digital forensic legislation
- Introduction to forensic science and investigation
- Hardware and operating system administration
- Mobile device file system structures
  - Mac Operating System (macOS)
  - Android
  - Symbian
  - Windows phone
- Digital forensic tools and techniques
- Tools to acquire mobile device forensic data
- Methodological problem solving

Range Statement

The Range Statement relates to the unit of competency as a whole. It allows for different work environments and situations that may affect performance. Bold / italicised wording in the Performance Criteria is detailed below

Current Australian privacy laws and digital forensic legislation *includes but not limited to:*

- Australian Government Privacy Act 1988
- Victorian privacy and protection act 2014
- A Concise Guide to Various Australian Laws Related to Privacy and Cybersecurity Domains SANs Institute Reading room

Current mobile forensic procedures and processes *includes but not limited to:*

- NIST Guidelines on Mobile Device Forensics, Developing Process for Mobile Device Forensics by Det. Cynthia A. Murphy)
- SWGDE Best Practices for Mobile Phone Forensics

Layered models of mobile forensic data acquisition *includes but not limited to:*

- User level (Information provided by the smartphone screen)
- Logical extraction (Information from an associated data repository eg itunes)
- Hex dumping and JTAG
- Chip off (Data acquired by removal of memory chips)

Smartphone fundamentals *includes but not limited to:*

- Phone architecture
- Memory systems
- Phone Identification (Universal Integrated Circuit Card (UICC) and components)
- Application structure

Mobile forensic data tools *includes but not limited to:*

- Guidance Software EnCase Forensic
- Cellebrite UFED Pro Series
- Logicube CellDEK
- Oxygen Forensic Suite
- XRY/XACT
- Paraben device seizure

Key data to be acquired from a mobile device *includes but not limited to:*

- International Mobile Equipment Identity (IMEI) phone number identification
- Carrier identification
- IP Address
- MAC address
- Call logs – dialed and received
- Text message recovery
- Deleted SMS
- Calendar
- Memos
- Date and time details
- Photos
- Passwords

EVIDENCE GUIDE

The evidence guide provides advice on assessment and must be read in conjunction with the Performance Criteria, Required Skills and Knowledge, the Range Statement and the Assessment section in Section B of the accreditation submission.

Critical aspects for assessment and evidence required to assess competency in this unit

To be considered competent in this unit, assessors must be satisfied the candidate can demonstrate the achievement of all of the elements of the competency to the level defined by the associated performance criteria.

Specifically they must be able to:

- Determine relevant privacy laws, procedures and processes pertaining to mobile digital forensics
- Select mobile digital forensic tools
- Acquire mobile forensic data
- Investigate the function and operation of further tools and techniques for mobile devices
- Identify further mobile data forensic tools and training

Context of and specific resources for assessment

Evidence should show competency working in a realistic environment and a variety of conditions. The candidate will have access to all tools, equipment, materials and documentation required. The candidate will be permitted to refer to any relevant workplace procedures, product and manufacturing specifications, codes, standards, manuals and reference materials.

This unit may be assessed on the job, off the job or a combination of both. Where assessment occurs off the job, an appropriate simulation must be used where the range of conditions reflects realistic workplace situations. The competencies covered by this unit would be demonstrated by an individual working alone or as part of a team. The assessment environment should not disadvantage the candidate.

Method of assessment

Evidence can be gathered in a variety of ways including:

- observation of processes and procedures
- oral and/or written questioning on required knowledge and skills
- testimony from supervisors, colleagues, clients and/or other appropriate persons
- inspection of the final product or outcome
- portfolio of documented evidence.

Where performance is not directly observed and/or is required to be demonstrated over a period of time and/or in a number of locations, any evidence should be authenticated by colleagues, supervisors, clients or other appropriate persons.

VU22255 - Evaluate threats and vulnerabilities for Internet of Things (IoT) devices

Unit Descriptor	This unit provides the knowledge and skills to examine the function and operation of IoT devices and to identify what threats and vulnerabilities exit when using them. The unit also includes strategies to minimise the threats. No licensing or certification requirements apply to this unit at the time of accreditation.
Employability Skills	This unit contains employability skills.
Application of the Unit	This unit is applicable to individuals working as cyber security paraprofessionals who will utilise IoT devices
Prerequisite Unit/s	Nil

ELEMENT Elements describe the essential outcomes of a unit of competency.	**PERFORMANCE CRITERIA** Performance criteria describe the required performance needed to demonstrate achievement of the element – they identify the standard for the element. Where bold/italicised text is used, further information or explanation is detailed in the required skills and knowledge and/or the range statement. Assessment of performance is to be consistent with the evidence guide.
1. Identify IoT device function and operation	1.1 Impact and use of IoT devices is defined 1.2 IoT devices are classified 1.3 Function and architecture of ***typical IoT devices*** is described 1.4 Operation of an example IoT device is described and demonstrated
2. Identify current threats and vulnerabilities for IoT devices	2.1 Complexity of security issues for IoT devices is investigated 2.2 ***Key strategies and guidance to mitigate IoT cyber security risks*** are identified and evaluated
3. Select relevant security frameworks or IoT incident mitigation strategies	3.1 Appropriate strategies and guidance to mitigate IoT cyber security risks are selected in consultation with ***key personnel*** 3.2 ***Mitigating strategies for application Layer vulnerabilities*** are researched 3.3 ***Emerging mitigating strategies for routing Layer vulnerabilities*** are researched
4. Implement relevant security frameworks or	4.1 Appropriate IoT security frameworks are implemented in consultation with key organisational personnel

IoT incident mitigation strategies	4.2	Training for staff to adopting the new or alter current working practices to improve the security culture is planned and implemented in consultation with key organisational personnel
	4.3	Mitigating strategies for application layer vulnerabilities are implemented
	4.4	Emerging mitigating strategies for routing layer vulnerabilities are implemented
5. Monitor the vulnerabilities of the IoT devices	5.1	Existing security infrastructure is configured to detect for IoT device vulnerabilities
	5.2	System messages and events to identify IoT malicious activity are evaluated
	5.3	Organisational policies and processes are followed upon the detection of IoT initiated incidents

REQUIRED SKILLS AND KNOWLEDGE

This describes the essential skills and knowledge and their level required for this unit.

Required skills:

- Articulating relevant issues encountered in the work environment
- Reading and accurately interpreting documents and reports
- Determining (as part of a team), changes required to work practices to implement new policies and procedures
- Assembling, participating in and coordinating a work team
- Problem solving within a team environment
- Evaluating the performance of a work team
- Contributing to the process of enhancing team performance
- Establishing project risk assessment
- Gathering, testing and allocating project resources
- Preparing technical documentation
- Making presentation to clients
- Performing calculations in binary and hexadecimal number systems
- Problem solving skills to implement provided scripts for a switch and a router
- Operating a personal computer
- Interpreting network diagrams
- Installing and using software packages
- Connecting cyber security equipment and networked devices
- Using basic Linux commands
- Utilising IoT devices
- Operating systems utilised in IoT devices
- Identifying appropriate IoT working frameworks
- Identifying current IoT security support documentation
- Identifying IoT security threats and vulnerabilities
- Mitigation strategies to secure IoT devices
- Evaluating policies, standards and procedure effectiveness (Continuous improvement)
- Evaluating new technologies

Required knowledge:

- Key IoT documents from the NIST Cybersecurity Framework
- Key documents from the ICS-CERT organisation relating to securing ICS infrastructure (https://ics-cert.us-cert.gov/)
- Key IoT documents from the European Union Agency for Network and Information Security (ENISA) https://www.enisa.europa.eu
- Key aspects of the IoT Alliance Australia: Internet of Things Security Guideline (https://static1.squarespace.com/static/573853ed1d07c093e27aefd2/t/58ab9bf8ebbd1a2b74e2aa2d/1487641596432/IoTAA+Security+Guideline+V1.0.pdf)
- IoT application development environment
- IoT device classification
- Risk assessment for IoT devices
- Differences between security frameworks, policies, standards, procedures, guidelines, and legislation

Range Statement

The Range Statement relates to the unit of competency as a whole. It allows for different work environments and situations that may affect performance. Bold / italicised wording in the Performance Criteria is detailed below

Typical IoT devices *includes but not limited to:*

- Rasberry Pi
- AWS IoT Button
- Arduino
- ARM
- Aruba
- Intel Quark SoC X1000
- Samsung SmarThings
- Google Nest devices
- Amazon Echo

Key strategies and guidance to mitigate IoT cyber security risks *includes but not limited to:*

- Strategies identified in the IoT Alliance Australia: Internet of Things Security Guideline document (https://static1.squarespace.com/static/573853ed1d07c093e27aefd2/t/58ab9bf8ebbd1a2b74e2aa2d/1487641596432/IoTAA+Security+Guideline+V1.0.pdf)
- Strategies identified by Department of Homeland Security (DHS) (Common Cybersecurity Vulnerabilities in Industrial Control Systems)
- Strategies identified by NIST (Guide to Industrial Control System (ICS) security)
- Strategies identified by the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) (Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies)
- Strategies identified by the IoT security foundation (http://iotsecurityfoundation.org/)

Key personnel *includes but not limited to:*

- Cyber security paraprofessional
- Team manager
- External consultants
- Relevant managers
- Business stakeholders

Mitigating strategies for application layer vulnerabilities *includes but not limited to:*

- Utilising the Constrained Application Protocol (CoAP)
- Utilising the Datagram Transport-Layer Security (DTLS) protocol
- Utilising the Message Queue Telemetry Transport (MQTT) protocol

Emerging mitigating strategies for routing layer vulnerabilities *includes but not limited to:*

- Using the 6LoWPAN Protocol
- Using IPv6 Routing protocol for Low power and lossy networks (RPL)

EVIDENCE GUIDE

The evidence guide provides advice on assessment and must be read in conjunction with the Performance Criteria, Required Skills and Knowledge, the Range Statement and the Assessment section in Section B of the accreditation submission.

Critical aspects for assessment and evidence required to assess competency in this unit

To be considered competent in this unit assessors must be satisfied the candidate can demonstrate the achievement of all of the elements of the competency to the level defined by the associated performance criteria

Specifically they must be able to:

- Identify IoT device function and operation;
- Identify current threats and vulnerabilities for IoT devices;
- Select and implement relevant security frameworks or IoT incident mitigation strategies;
- Monitor the vulnerabilities of the IoT devices.

Context of and specific resources for assessment

Evidence should show competency working in a realistic environment and a variety of conditions. The candidate will have access to all tools, equipment, materials and documentation required. The candidate will be permitted to refer to any relevant workplace procedures, product and manufacturing specifications, codes, standards, manuals and reference materials.

This unit may be assessed on the job, off the job or a combination of both. Where assessment occurs off the job, an appropriate simulation must be used where the range of conditions reflects realistic workplace situations. The competencies covered by this unit would be demonstrated by an individual working alone or as part of a team. The assessment environment should not disadvantage the candidate

Method of assessment

Evidence can be gathered in a variety of ways including:

- observation of processes and procedures
- oral and/or written questioning on required knowledge and skills
- testimony from supervisors, colleagues, clients and/or other appropriate persons
- inspection of the final product or outcome
- portfolio of documented evidence.

Where performance is not directly observed and/or is required to be demonstrated over a period of time and/or in a number of locations, any evidence should be authenticated by colleagues, supervisors, clients or other appropriate persons

VU22256 - Protect critical infrastructure for an organisation

Unit Descriptor

This unit provides the knowledge and skills to examine the key standard bodies and frameworks that offer constructive support for addressing threats and vulnerabilities of critical infrastructure.

The units also covers the development of mitigation strategies to protect an organisation's infrastructure as well as the implementation and monitoring of its' effectiveness.

No licensing or certification requirements apply to this unit at the time of accreditation.

Employability skills

This unit contains employability skills.

Application of the Unit

This unit is applicable to individuals working as cyber security paraprofessionals who will work to protect critical infrastructure from cyber security threats an vulnerabilities

Prerequisite

Nil

ELEMENT	**PERFORMANCE CRITERIA**
Elements describe the essential outcomes of a unit of competency.	Performance criteria describe the required performance needed to demonstrate achievement of the element – they identify the standard for the element. Where bold/italicised text is used, further information or explanation is detailed in the required skills and knowledge and/or the range statement. Assessment of performance is to be consistent with the evidence guide.
1. Collate security frameworks, cyber security risk mitigation strategies and other supportive documents for the organisation	1.1 Relationship between ***critical infrastructure*** and ***Industrial Control Systems (ICS)*** is defined 1.2 ***Key standards bodies and organisations*** that provide useful resources that address security issues in critical infrastructure or ICS are identified 1.3 ***Current working frameworks or practices*** that can support the improvement of critical infrastructure from cyber security attack are identified
2. Evaluate current critical infrastructure and associated vulnerabilities	2.1 Current critical infrastructure is identified and classified 2.2 Current vulnerabilities for critical infrastructure are identified 2.3 Current ICS deployment architectures are reviewed and evaluated 2.4 Risk assessment for critical infrastructure for the organisation is performed 2.5 Case study of the STUXnet virus is performed
3. Classify current cyber security vulnerabilities	3.1 Classification of current cyber security vulnerabilities for ICS's are identified

for critical infrastructure	3.2	Risk assessment of current ICS vulnerabilities is conducted
4. Select relevant cyber security frameworks and security critical infrastructure mitigation strategies	4.1	Resources that provide strategies to protect critical infrastructure are sourced
	4.2	Current organisational security policies to protect critical infrastructure are identified
	4.3	In consultation with ***key personnel*** current critical infrastructure protection policies are evaluated
	4.4	Appropriate strategies to enhance the protection of the critical infrastructure are adopt
	4.5	Training for staff to alter current working practices or adopt new practices to improve the security culture is planned and implemented
5. Monitor the effectiveness of the implementation of the cyber security frameworks and security critical infrastructure mitigation strategies	5.1	In consultation with key personnel, implemented changes to processes and procedures are measured for effectiveness against selected criteria
	5.2	Changes to organisational processes and procedures to deal with critical infrastructure incident responses are monitored for effectiveness

REQUIRED SKILLS AND KNOWLEDGE

This describes the essential skills and knowledge and their level required for this unit.

Required skills:

- Articulating relevant issues encountered in the work environment
- Reading and accurately interpreting documents and reports
- Determine changes required to work practices to implement new policies and procedures
- Assembling, participating in and coordinating a work team
- Problem solving within a team environment
- Evaluating the performance of a work team
- Contributing to the process of enhancing team performance
- Establishing project risk assessment
- Gathering, testing and allocating project resources
- Preparing technical documentation
- Making presentation to clients
- Evaluation of policies, standards and procedures effectiveness (Continuous improvement)
- Evaluating new technologies
- Educating critical infrastructure technicians
- Identifying critical infrastructure vulnerabilities
- Implementing mitigation strategies for the enterprise

Required knowledge:

- Industrial Control System (ICS) architectures
- Critical infrastructure:
  - heating, ventilation and air conditioning (HVAC)
  - building management
  - lighting
  - security
- Key aspects of the National Institute of Standards and Technology (NIST) Cybersecurity Framework (https://www.nist.gov/cyberframework)
- Key strategies from the European Union Agency for Network and Information Security (ENISA) (https://www.enisa.europa.eu)
- Anatomy of a cyber attack (ie STUXNET virus
- Strategies to defend ICS's:
  - application whitelisting
  - configuration & patch management
  - reduce attack surface area
  - defendable environment
  - manage authentication
  - monitor and respond
  - implement secure remote access
- Key strategies from ISO/IEC 2700X
- Risk assessment
- Differences between security frameworks, policies, standards, procedures, guidelines, and legislation
- Critical infrastructure
- Mitigation strategies to security critical infrastructure
- Communicating styles to key decision making groups

Range Statement

The Range Statement relates to the unit of competency as a whole. It allows for different work environments and situations that may affect performance. Bold / italicised wording in the Performance Criteria is detailed below

Critical infrastructure *includes but not limited to:*

- Heating, Ventilation and Air Conditioning (HVAC)
- Building management systems
- Lighting
- Security systems
- IT equipment infrastructure

Industrial Control Systems (ICS) *includes but not limited to:*

- Supervisory Control and Data Acquisition (SCADA)
- Programmable Logic Controllers (PLCs)
- Microprocessor controlled devices (Uc)
- PC with Controller card
- Internet of Things (IoT) device

Key standards bodies and organisations *includes but not limited to:*

- International Organisation for Standardisation (ISO/IEC)
- The Industrial Control Systems Cyber Emergency Response Team (ICS-Cert)
- National Cyber Security and Communications Integration Centre (NCCIC)
- National Institute of Standards and Technology (NIST)
- European Union Agency for Network and Information Security (ENISA)

Current working frameworks or practices *includes but not limited to:*

- NIST framework for improving Critical Infrastructure cyber security (cybersecurity-framework-021214.pdf, https://www.nist.gov/cyberframework)
- International Organisation for Standardisation, Risk management – Principles and guidelines, ISO 31000:2009, 2009 (http://www.iso.org/iso/home/standards/iso31000.htm)
- International Organisation for Standardisation/International Electrotechnical Commission, Information technology – Security techniques – Information security risk management, ISO/IEC 27005:2011, 2011 (http://www.iso.org/iso/catalogue_detail?csnumber=56742)
- U.S. Department of Energy, Electricity Subsector Cybersecurity Risk Management Process, DOE/OE-0003, May 2012 (http://energy.gov/sites/prod/files/Cybersecurity%20Risk%20Management%20Process%20Guideline%20%20Final%20-%20May%202012.pdf)

Key personnel *includes but not limited to:*

- Cyber security paraprofessional
- Team manager
- External consultants
- Relevant managers
- Business stakeholders

EVIDENCE GUIDE

The evidence guide provides advice on assessment and must be read in conjunction with the Performance Criteria, Required Skills and Knowledge, the Range Statement and the Assessment section in Section B of the accreditation submission.

Critical aspects for assessment and evidence required to assess competency in this unit

To be considered competent in this unit assessors must be satisfied the candidate can demonstrate the achievement of all of the elements of the competency to the level defined by the associated performance criteria

Specifically they must be able to:

- Collate security frameworks, cyber security risk mitigation strategies and other supportive documents for the organisation;
- Evaluate and classify current critical infrastructure and associated vulnerabilities;
- Select relevant security frameworks, cyber security critical infrastructure mitigation strategies;
- Monitor the effectiveness of the organisation’s implementation of the security frameworks, legislation and cyber security critical infrastructure mitigation strategies;

Context of and specific resources for assessment

Evidence should show competency working in a realistic environment and a variety of conditions. The candidate will have access to all tools, equipment, materials and documentation required. The candidate will be permitted to refer to any relevant workplace procedures, product and manufacturing specifications, codes, standards, manuals and reference materials.

This unit may be assessed on the job, off the job or a combination of both. Where assessment occurs off the job, an appropriate simulation must be used where the range of conditions reflects realistic workplace situations. The competencies covered by this unit would be demonstrated by an individual working alone or as part of a team. The assessment environment should not disadvantage the candidate.

Method of assessment

Evidence can be gathered in a variety of ways including:

- observation of processes and procedures
- oral and/or written questioning on required knowledge and skills
- testimony from supervisors, colleagues, clients and/or other appropriate persons
- inspection of the final product or outcome
- portfolio of documented evidence.

Where performance is not directly observed and/or is required to be demonstrated over a period of time and/or in a number of locations, any evidence should be authenticated by colleagues, supervisors, clients or other appropriate persons.

VU22257 - Configure security devices for an organisation

Unit Descriptor	This unit seeks to build on previous skills in configuring security devices by providing knowledge and skills to configure and modify where required an organisation's existing security devices. After implementation the devices will be monitored and assesed for their effectiveness. New security devices and technologies will be researched, evaluated and implemented in order to improve the security performance of the organisation No licensing or certification requirements apply to this unit at the time of accreditation.
Employability Skills	This unit contains employability skills.
Application of the Unit	This unit is applicable to individuals intending to work as cyber security paraprofessionals responsible for the security infrastructure
Pre requisite Unit	Nil

ELEMENT Elements describe the essential outcomes of a unit of competency.		**PERFORMANCE CRITERIA** Performance criteria describe the required performance needed to demonstrate achievement of the element – they identify the standard for the element. Where bold/italicised text is used, further information or explanation is detailed in the required skills and knowledge and/or the range statement. Assessment of performance is to be consistent with the evidence guide.
1. Collate the current network security diagram, security infrastructure functional operation and security device documentation	1.1	Existing security infrastructure diagram for the organisation are sourced
	1.2	In consultation with ***appropriate personnel*** the function and operation of the existing network security infrastructure is evaluated
	1.3	***Network security devices, systems and tools*** are identified
2. Configure security devices according to the functional specification	2.1	Resources and documents to configure these network security devices are gathered
	2.2	***Security policy*** document is sourced
	2.3	Selection of network security devices, systems and tools are configured according to the functionality described in the network security policy
3. Verify operation of security devices	3.1	Baseline functionality of network security devices are determined or identified
	3.2	Utilising software or hardware tools, network security device operation and performances is monitored according to baseline functionality
	3.3	Effectiveness of the security device operation are evaluated with appropriate personnel
4. Investigate and implement new network security architectures and devices	4.1	New network security devices and technologies are researched
	4.2	New network security devices and technology is evaluated and selected

4.3 Higher level packet inspection technology is described then implemented on a network security device

4.4 Holistic approaches to traffic inspection technologies is described and implemented on a network security device

4.5 Concept of dynamic update technology for defending against new cyber-attacks is described then implemented on a network security device

4.6 New network security technology solution is implement for a ***small to medium size organisation***

4.7 ***Virtual network security technologies*** are investigated and compared

4.8 A virtual network security technology is selected

4.9 A virtual network security technology solution is configured and implemented for the organisation

REQUIRED SKILLS AND KNOWLEDGE

This describes the essential skills and knowledge and their level, required for this unit

Required skills:

- Articulate relevant issues encountered in the work environment
- Base level problem solving skills to implement provided scripts for a networking security device
- Read and accurately interpret documents and reports
- Operate a personal computer
- Interpreting network diagrams
- Assembling, participating in and coordinating a work team
- Problem solving within a team environment
- Evaluating the performance of a work team
- Contributing to the process of enhancing team performance
- Installing and using software packages
- Connecting cyber security equipment and networked devices
- Evaluating effectiveness of network security devices
- Preparing technical documentation
- Identifying and collating relevant documents
- Evaluating operation performance
- Making presentation to clients

Required knowledge:

- Testing methodologies
- Identifying and using networking devices
- Evaluating new firewall technologies
- Writing reports to justify equipment purchases
- Command Line Interface (CLI) to configure network security devices
- Handle and use network security devices
- Overview of network security devices that provide network security functionality like:
    - Access Control Lists (ACLs)
    - Firewalls including Zone based policy firewalls
    - Packet filtering
    - Inspection rules
    - Intrusion detection Systems (IDS)
    - Intrusion Prevention Systems (IPS)
    - Virtual Private Networks (VPNs)
    - Network Access Control (NAC)
    - Web Application Firewalls (WAF)
    - Honeypots
    - Packet Shapers
    - Proxies
    - Reverse Proxies
- Network security device deployment
- Patch and vulnerability management of network devices
- Testing of network security devices
- New network security technologies
- Access lists

Range Statement

The Range Statement relates to the unit of competency as a whole. It allows for different work environments and situations that may affect performance

Appropriate personnel *includes but not limited to:*	• Cyber security paraprofessional • Cyber security manager • External consultants • Relevant managers • Business stakeholders
Network security devices, systems and tools *includes but not limited to:*	• Access lists (ACL's) • Firewalls including Zone based policy firewalls • Packet filtering • Inspection rules • Intrusion detection Systems (IDS) • Intrusion Prevention Systems (IPS) • Virtual Private Networks (VPNs) • Network Access Control (NAC) • Web Application Firewalls (WAF) • Honeypots • Packet Shapers • Proxies • Reverse Proxies
Security policy *includes but not limited to:*	• Breech consequences • Policy enforcement • User Access • Security profiles • Passwords • E-mail use • Internet use • Anti-Virus requirements • Back-up and recovery processes • Intrusion detection processes and procedures • Remote Access
Small to medium size organisation *includes but not limited to:*	• Single internet connection • Three VLANs • Five servers • Single demilitarized zone (DMZ) Firewall
Virtual network security technologies *includes but not limited to:*	• Palo Alto virtual solution • Cisco virtual solution • VMWare virtual solution • HP Tipping Point framework

EVIDENCE GUIDE

The evidence guide provides advice on assessment and must be read in conjunction with the Performance Criteria, Required Skills and Knowledge, the Range Statement and the Assessment section in Section B of the accreditation submission.

Critical aspects for assessment and evidence required to assess competency in this unit

To be considered competent in this unit assessors must be satisfied the candidate can demonstrate the achievement of all of the elements of the competency to the level defined by the associated performance criteria

Specifically they must be able to:

- Collate the current network security diagram, security infrastructure functional operation and security device documentation;
- Configure and verify security devices according to the functional specification;
- Investigate and implement new network security architectures and devices.

Context of and specific resources for assessment

Evidence should show competency working in a realistic environment and a variety of conditions. The candidate will have access to all tools, equipment, materials and documentation required. The candidate will be permitted to refer to any relevant workplace procedures, product and manufacturing specifications, codes, standards, manuals and reference materials.

This unit may be assessed on the job, off the job or a combination of both. Where assessment occurs off the job, an appropriate simulation must be used where the range of conditions reflects realistic workplace situations. The competencies covered by this unit would be demonstrated by an individual working alone or as part of a team. The assessment environment should not disadvantage the candidate.

Method of assessment

Evidence can be gathered in a variety of ways including:

- observation of processes and procedures
- oral and/or written questioning on required knowledge and skills
- testimony from supervisors, colleagues, clients and/or other appropriate persons
- inspection of the final product or outcome
- portfolio of documented evidence.

Where performance is not directly observed and/or is required to be demonstrated over a period of time and/or in a number of locations, any evidence should be authenticated by colleagues, supervisors, clients or other appropriate persons.

VU22258 - Design and implement a virtualised cyber security infrastructure for an organisation

Unit Descriptor

This unit provides the knowledge and skills required to design, implement and monitor a fundamental virtualised cyber security infrastructure for an organisation. The unit includes designing an infrastructure to suit key specifications, the utilisation of testing procedures in the development stage, implementation process, monitoring functionality following implementation and continuous improvement processes

No licensing or certification requirements apply to this unit at the time of accreditation.

Employability skills

This unit contains employability skills.

Application of the Unit

This unit is applicable to a practitioner working as part of a team responsible for the design, implementation and monitoring of a virtualised cyber security infrastructure for the organisation

Prerequisite

ICTNWK525 Configure an enterprise virtual computing environment

ELEMENT	**PERFORMANCE CRITERIA**
Elements describe the essential outcomes of a unit of competency.	Performance criteria describe the required performance needed to demonstrate achievement of the element – they identify the standard for the element. Where bold/italicised text is used, further information or explanation is detailed in the required skills and knowledge and/or the range statement. Assessment of performance is to be consistent with the evidence guide.
1. Compile key specifications for the security infrastructure design	1.1 Functional requirements of the cyber security infrastructure are compiled
	1.2 Virtualised security infrastructure design brief is developed
	1.3 Virtualised machine devices required to build the design are identified and gathered
	1.4 ***Testing tools for virtualised machines*** are identified and gathered
2. Design the virtualised security infrastructure	2.1 Virtualised security infrastructure design is evaluated for its effectiveness
	2.2 Feedback is provided to the system designer with modifications made as required to the system design
	2.3 Cyber security practitioners familiarize themselves with the ***software design environment***
	2.4 Virtualised security infrastructure is designed by utilising sound processes
	2.5 Internally connected virtual machines are secured and protected
	2.6 Externally connected virtual machines are secured and protected

3. Test the virtualised design for its functional operation according to design specifications	3.1	***Appropriate test procedures*** for the organisation are followed
	3.2	Virtualised security infrastructure is tested utilising appropriate tools
	3.3	Functional operation of the cyber security infrastructure is evaluated
	3.4	***Vulnerabilities of virtualised systems*** are identified and reported to appropriate personnel.
	3.5	Strategies to “harden” the virtualised security infrastructure design are developed in consultation with ***appropriate personnel***
4. Implement the virtualised cyber security system	4.1	Resources for the security infrastructure deployment are identified and sourced
	4.2	Resources are implemented and configured
	4.3	Virtualised security infrastructure is deployed
5. Monitor the performance of the virtualised cyber security system	5.1	***Tools to monitor the performance*** of the security infrastructure are chosen
	5.2	Tools to monitor the performance of the system are configured and deployed
	5.3	File outputs or alerts for system performance are monitored
	5.4	Monitored data is evaluated and if appropriate, modification to the system is performed

REQUIRED SKILLS AND KNOWLEDGE

This describes the essential skills and knowledge and their level required for this unit.

Required skills:

- Articulating relevant issues encountered in the work environment
- Performing calculations in binary and hexadecimal number systems
- Reading and accurately interpreting documents and reports
- Operating a personal computer
- Interpreting network diagrams
- Assembling, participating in and coordinating a work team
- Problem solving within a team environment
- Evaluating the performance of a work team
- Contributing to the process of enhancing team performance
- Developing a project implementation plan including realistic timelines and allocation of tasks for team members
- Establishing project risk assessment
- Gathering, testing and allocating project resources
- Penetration testing concepts and procedures for required for a cyber security infrastructure
- Installing and using software packages
- Using basic Linux commands
- Interpreting and writing scripts
- Preparing technical documentation
- Making presentation to clients
- Identify vulnerabilities
- Report vulnerabilities to appropriate personnel
- Securing internally connected virtual machines

Required knowledge:

- Virtualised security devices such as:
  - routers
  - switches
  - firewalls
  - virtual network interface card
  - and end points
- Virtualised development environment
- Cyber security infrastructure design
- Connecting virtual images
- Network penetration testing tools
- Virtualised system testing tools
- Vulnerabilities of virtualised systems (shared hosting and/or shared memory pages)
- Externally connected virtual machines

Range Statement

The Range Statement relates to the unit of competency as a whole. It allows for different work environments and situations that may affect performance. Bold / italicised wording in the Performance Criteria is detailed below

Testing tools for virtualised machines *includes but not limited to:*

- Hyper-V
- VMware vSphere
- Citrix XenServer
- Parallels
- VMware Fusion
- VMware Workstation
- KVM
- Qemu
- Xen
- VIrtualBox

Software design environment *includes but not limited to:*

- Hyper-V
- VMware vSphere
- Citrix XenServer
- Parallels
- VMware Fusion
- VMware Workstation
- OpenStack
- CloudStackVIrtualBox

Appropriate test procedures *includes but not limited to:*

- Exhaustive testing of the system off line that would not affect the existing networking infrastructure
- Turnkey (implement solution all at once) or in stages

Vulnerabilities of virtualised systems *includes but not limited to:*

- Securing resources (eg Databases or other stored media)
- Hosts that access this media (ie shared hosting)
- Internally connected Virtual Machines
- Externally connected Virtual Machines

Appropriate personnel *includes but not limited to:*

- Colleagues
- line managers
- external consultants
- virtualised security infrastructure designer

Tools to monitor the performance *includes but not limited to:*

- PRTG Network Monitor
- vRealize Operations Manager
- vRealize Network Insight
- Pandora FMS
- Nagios
- Zabbix

EVIDENCE GUIDE

The evidence guide provides advice on assessment and must be read in conjunction with the Performance Criteria, Required Skills and Knowledge, the Range Statement and the Assessment section in Section B of the accreditation submission.

Critical aspects for assessment and evidence required to assess competency in this unit

To be considered competent in this unit assessors must be satisfied the candidate can demonstrate the achievement of all of the elements of the competency to the level defined by the associated performance criteria

Specifically they must be able to:

- Develop the virtualised security infrastructure brief, identify and collate appropriate virtual machines;
- Design the virtualised security infrastructure;
- Test the system design and evaluate it for its effectiveness
- Implement the virtualised security infrastructure;
- Implement monitoring tools for the infrastructure;
- Evaluate the infrastructure performance, and, modify the system if required;

Context of and specific resources for assessment

Evidence should show competency working in a realistic environment and a variety of conditions. The candidate will have access to all tools, equipment, materials and documentation required. The candidate will be permitted to refer to any relevant workplace procedures, product and manufacturing specifications, codes, standards, manuals and reference materials.

This unit may be assessed on the job, off the job or a combination of both. Where assessment occurs off the job, an appropriate simulation must be used where the range of conditions reflects realistic workplace situations. The competencies covered by this unit would be demonstrated by an individual working alone or as part of a team. The assessment environment should not disadvantage the candidate.

Method of assessment

Evidence can be gathered in a variety of ways including:

- observation of processes and procedures
- oral and/or written questioning on required knowledge and skills
- testimony from supervisors, colleagues, clients and/or other appropriate persons
- inspection of the final product or outcome
- portfolio of documented evidence.

Where performance is not directly observed and/or is required to be demonstrated over a period of time and/or in a number of locations, any evidence should be authenticated by colleagues, supervisors, clients or other appropriate persons.

VU22253 - Undertake penetration testing of the security infrastructure for an organisation

Unit Descriptor

This unit provides the knowledge and skills required to use a series of tools to test the vulnerabilities of the security infrastructure for an organisation. The unit includes the compiling of information on the existing security infrastructure design, evaluating and selecting testing tools and preforming vulnerability scanning and penetration testing. It also includes developing a report which assesses the weaknesses and includes mitigation strategies that can be implemented to 'harden' the organisation's cyber security infrastructure

No licensing or certification requirements apply to this unit at the time of accreditation.

Employability Skills

This unit contains employability skills.

Application of the Unit

This unit is applicable to individuals working as cyber security paraprofessionals who will test the organisation's security infrastructure for vulnerabilities

Prerequisite Unit/s

Nil

ELEMENT Elements describe the essential outcomes of a unit of competency.	**PERFORMANCE CRITERIA** Performance criteria describe the required performance needed to demonstrate achievement of the element – they identify the standard for the element. Where bold/italicised text is used, further information or explanation is detailed in the required skills and knowledge and/or the range statement. Assessment of performance is to be consistent with the evidence guide.
1. Compile the information on the security infrastructure	1.1 Information regarding the organisation's security infrastructure is sourced
	1.2 Information on the function and operation on each item of the security infrastructure is collated
	1.3 Security infrastructure design is evaluated
2. Evaluate and select testing tools to test the security infrastructure	2.1 ***Tools used to perform penetration testing (PEN)*** on the organisation's security infrastructure are sourced and evaluated
	2.2 Tools to perform penetration testing are selected
	2.3 Testing environment is setup and configured
3. Develop penetration testing skills	3.1 Familiarity with the function and configuration of the tools within the PEN testing environment is developed
	3.2 Skills in using the PEN testing tools for detecting vulnerabilities in security infrastructure are developed
4. Perform vulnerability scanning on the security infrastructure	4.1 Differences between PEN testing and vulnerability scanning are articulated
	4.2 Baseline for the organisation's security infrastructure vulnerabilities is created
	4.3 Tool to perform vulnerability scans is evaluated and selected

	4.4 Regular procedure of vulnerability scans for the organisation is proposed
	4.5 Results of the vulnerability scan are interpreted with ***appropriate personnel***
5. Perform penetration testing on the security infrastructure	5.1 Processes and extent of the PEN testing procedure are examined and evaluated
	5.2 Process used to test for vulnerabilities of the organisation’s security infrastructure is developed
	5.3 Advantages and disadvantages of PEN testing is articulated
	5.4 Vulnerabilities of the organisation’s security infrastructure is tested with selected tools and methodologies
6. Develop and present the penetration test report	6.1 Results of the PEN test for the security infrastructure are assessed
	6.2 Risk assessment of vulnerabilities is performed
	6.3 ***Penetration testing report*** for the security infrastructure is developed
	6.4 Penetration testing report is presented to appropriate personnel
7. Research new security technology developments	7.1 ***Useful information on cyber security infrastructure testing developments*** is sourced and reviewed
	7.2 New tools to determine vulnerabilities in security infrastructure are researched

REQUIRED SKILLS AND KNOWLEDGE

This describes the essential skills and knowledge and their level required for this unit.

Required skills:

- Articulating relevant issues encountered in the work environment
- Reading and accurately interpreting documents and reports
- Operating a personal computer
- Interpreting network diagrams
- Assembling, participating in and coordinating a work team
- Problem solving within a team environment
- Evaluating the performance of a work team
- Contributing to the process of enhancing team performance
- Gathering, testing and allocating project resources
- Penetration testing concepts and procedures required for a cyber security infrastructure
- Installing and using software packages
- Using basic Linux commands
- Interpret and writing scripts
- Preparing technical documentation
- Making presentation to clients
- Interpreting network vulnerability scanning tool results
- Managing network vulnerability scanning tool results
- Using PEN testing tools to test the security infrastructure
- Identify vulnerabilities
- Reporting vulnerabilities to appropriate personnel

Required knowledge:

- Physical and virtual cyber security infrastructure
- Network security penetration testing
- Types of testing
- Dangers of testing
- Project communication and time management
- Network vulnerability scanning tools
- Network penetration testing
- Vulnerabilities of virtualised systems (shared hosting)

Range Statement

The Range Statement relates to the unit of competency as a whole. It allows for different work environments and situations that may affect performance. Bold / italicised wording in the Performance Criteria is detailed below

Tools used to perform penetration testing (PEN) *includes but not limited to:*

- Network vulnerability scanning tools
- Software design environments
  - Hyper-V
  - VMware vSphere
  - Citrix XenServer
  - Parallels
  - VMware Fusion
  - VMware Workstation
  - OpenStack
  - CloudStackVIrtualBox
  - etc)
- Kali Linux environment
- Metasploit

Appropriate personnel *includes but not limited to:*

- PEN tester
- PEN tester manager
- External consultants
- Relevant managers
- Business stakeholders

Penetration testing report *includes but not limited to:*

- Executive summary
- Discussion of the root cause/s
- Technical issues
- Risk assessment
- Reproduction steps
- Remediation steps

Useful information on cyber security infrastructure testing developments *includes but not limited to:*

- Trade magazines
- Related articles
- Vendor data
- Books
- Newsletters
- Blogs

EVIDENCE GUIDE

The evidence guide provides advice on assessment and must be read in conjunction with the Performance Criteria, Required Skills and Knowledge, the Range Statement and the Assessment section in Section B of the accreditation submission.

Critical aspects for assessment and evidence required to assess competency in this unit

To be considered competent in this unit assessors must be satisfied the candidate can demonstrate the achievement of all of the elements of the competency to the level defined by the associated performance criteria

Specifically they must be able to:

- Compile the security infrastructure and evaluate its' weaknesses;
- Select and configure PEN testing tools and the testing environment;
- Perform PEN tests on the security infrastructure;
- Developing and presenting the penetration test report;
- Research new developments in PEN testing procedures and equipment.

Context of and specific resources for assessment

Evidence should show competency working in a realistic environment and a variety of conditions. The candidate will have access to all tools, equipment, materials and documentation required. The candidate will be permitted to refer to any relevant workplace procedures, product and manufacturing specifications, codes, standards, manuals and reference materials.

This unit may be assessed on the job, off the job or a combination of both. Where assessment occurs off the job, an appropriate simulation must be used where the range of conditions reflects realistic workplace situations. The competencies covered by this unit would be demonstrated by an individual working alone or as part of a team. The assessment environment should not disadvantage the candidate.

Method of assessment

Evidence can be gathered in a variety of ways including:

- observation of processes and procedures;
- oral and/or written questioning on required knowledge and skills;
- testimony from supervisors, colleagues, clients and/or other appropriate persons;
- inspection of the final product or outcome;
- portfolio of documented evidence;

Where performance is not directly observed and/or is required to be demonstrated over a period of time and/or in a number of locations, any evidence should be authenticated by colleagues, supervisors, clients or other appropriate persons

VU22251 - Gather, analyse and interpret threat data

Unit Descriptor	This unit provides the knowledge and skills to demonstrate the function and operation of hardware and software tools used to detect cyber incidents. The unit includes the selection and use of tools to analyse logged data, detection of malicious data streams as well as analysis of the results and evaluation of the selected tools in their effectiveness in detecting data patterns. No licensing or certification requirements apply to this unit at the time of accreditation.
Employability skills	This unit contains employability skills.
Application of the Unit	This unit applies to a paraprofessional working as part of a team which response to cyber security incidents.
Prerequisite Unit/s	Nil

ELEMENT Elements describe the essential outcomes of a unit of competency	**PERFORMANCE CRITERIA** Performance criteria describe the required performance needed to demonstrate achievement of the element – they identify the standard for the element. Where bold/italicised text is used, further information or explanation is detailed in the required skills and knowledge and/or the range statement. Assessment of performance is to be consistent with the evidence guide.
1. Identify the function and operation of hardware and software tools deployed to detect cyber incidents	1.1 Function and role of hardware devices used to detect incidents for the organisation are evaluated 1.2 Function and role of software used to detect incidents for the organisation is evaluated 1.3 ***Data sources*** to gather incident information are identified 1.4 Function and role of events, logs and data sources used to detect incidents for the organisation are evaluated
2. Select and use tools that analyse logged data	2.1 ***Tools that support the interpretation of logged data*** are evaluated 2.2 Features of the ***logged data tool environment*** are identified and evaluated 2.3 Appropriate tool to analyse logged data is selected
3. Develop skills in analysing data	3.1 Data source to perform analysis is selected 3.2 Knowledge of normal data sets is developed 3.3 Techniques and procedures to identify irregular events are developed 3.4 Effectiveness of the strategy to detect irregular events is evaluated and modified if required

4. Demonstrate the use of the tools used to analyse logged data	4.1	Most appropriate tool to analyse logged data stream is selected from the working environment
	4.2	Skills using tools to detect data stream anomalies are developed
	4.3	Tools used to detect data stream anomalies are demonstrated
	4.4	Overview of the methodology to integrate python scripts to the logged data analysis tool in order to detect data patterns are demonstrated
5. Develop continuous improvement strategies to detect anomalous events for the organisation	5.1	Effectiveness of the tools used to detect data patterns is evaluated
	5.2	Strategies to detect data patterns are evaluated and modified if required

REQUIRED SKILLS AND KNOWLEDGE

This describes the essential skills and knowledge and their level required for this unit.

Required skills:

- Interpreting anomalies
- Articulating relevant issues encountered in the work environment
- Reading and accurately interpreting documents and reports
- Operating a personal computer
- Assembling, participating in and coordinating a work team
- Problem solving within a team environment
- Evaluating the performance of a work team
- Establishing project risk assessment
- Gathering, testing and allocating project resources
- Installing and using software packages
- Preparing technical documentation
- Making presentation to clients
- Communicating and engaging external contractors
- Interpreting and analysing data

Required knowledge:

- Python scripts
- Collaboration techniques
- Methods to solve problems
- Documentation techniques
- Identifiying data sources
- Gathering data
- Select data sources
- Tools that supports data analysis of log files (eg splunk)

Range Statement

The Range Statement relates to the unit of competency as a whole. It allows for different work environments and situations that may affect performance. Bold / italicised wording in the Performance Criteria is detailed below

***Data sources** includes but not limited to::*

- Alerts
- Logs
- reported events
- Files and directories
- Network events
- Operating system event log data

***Tools that support the interpretation of logged data** includes but not limited to:*

- Splunk
- ELK/Logtash
- Sumo Logic
- HP ArcSight Logger
- NetWrix
- Tibco
- XpoLog

***Logged data tool environment** includes but not limited to:*

- Analysing system performance
- Troubleshoot failure
- Monitoring business metrics
- Search and investigate
- Create dashboards
- Store and retrieve data
- Identify data patterns
- Set alarms
- Select data sources

EVIDENCE GUIDE

The evidence guide provides advice on assessment and must be read in conjunction with the Performance Criteria, Required Skills and Knowledge, the Range Statement and the Assessment section in Section B of the accreditation submission.

Critical aspects for assessment and evidence required to assess competency in this unit

To be considered competent in this unit assessors must be satisfied the candidate can demonstrate the achievement of all of the elements of the competency to the level defined by the associated performance criteria

Specifically they must be able to:

- Identify the function and operation of the hardware and software of the incident response environment;
- Familiarise and demonstrate the operation of the tools that analyse logged data;
- Evaluate the effectiveness of detecting data patterns.

Context of and specific resources for assessment

Evidence should show competency working in a realistic environment and a variety of conditions. The candidate will have access to all tools, equipment, materials and documentation required. The candidate will be permitted to refer to any relevant workplace procedures, product and manufacturing specifications, codes, standards, manuals and reference materials.

This unit may be assessed on the job, off the job or a combination of both. Where assessment occurs off the job, an appropriate simulation must be used where the range of conditions reflects realistic workplace situations. The competencies covered by this unit would be demonstrated by an individual working alone or as part of a team. The assessment environment should not disadvantage the candidate.

Method of assessment

Evidence can be gathered in a variety of ways including:

- observation of processes and procedures
- oral and/or written questioning on required knowledge and skills; testimony from supervisors, colleagues, clients and/or other appropriate persons
- inspection of the final product or outcome
- portfolio of documented evidence.

Where performance is not directly observed and/or is required to be demonstrated over a period of time and/or in a number of locations, any evidence should be authenticated by colleagues, supervisors, clients or other appropriate persons.

VU22254 - Undertake advanced penetration testing for web site vulnerabilities

Unit Descriptor

This unit provides the knowledge and skills to expand the testing capability for web vulnerabilities. The unit includes skills in using advance features of current toolsets in order identify weaknesses in the security of an organisation's website. It also includes the development of a penetration (PEN) test report which will identify the root cause of the issues and includes mitigation strategies for the identified web site weaknesses.

This unit utilises the current security framework Open Web Application Security Project (OWASP) security methodology and open source tools provide a sound foundation to develop these skills

No licensing or certification requirements apply to this unit at the time of accreditation.

Employability Skills

This unit contains employability skills.

Application of the Unit

This unit is applicable to persons working as cyber security paraprofessionals capable of using advanced testing tools to determine vulnerabilities in an organisation's web site

Prerequisite Unit/s

Nil

ELEMENT	**PERFORMANCE CRITERIA**
Elements describe the essential outcomes of a unit of competency.	Performance criteria describe the required performance needed to demonstrate achievement of the element – they identify the standard for the element. Where bold/italicised text is used, further information or explanation is detailed in the required skills and knowledge and/or the range statement. Assessment of performance is to be consistent with the evidence guide.
1. Comprehend the web application development process	1.1 ***Web application development process*** is elaborated 1.2 ***Web application development environment*** and associated test phases are determined 1.3 Web architecture concepts is reviewed 1.4 Examples of ***web frameworks*** are reviewed 1.5 Introduction to Secure Development Lifecycle (SDLC) and the importance of integrating it with security during all phases of development is established
2. Utilise tools and technology for testing web site content	2.1 ***Tools used to determine the technology stack used in web applications and web servers*** are utilised 2.2 Custom wordlists for spidering are created 2.3 Value of user-agent strings used in testing tools are evaluated 2.4 ***Identifying the technology stack of a web application utilising current resources*** are investigated

3. Examine the advanced features of a current proxy testing tool suite	3.1	Revision of a current proxy tool suite is demonstrated
	3.2	Dangers of live scanning are articulated
	3.3	Utilising ***extended features of a current proxy testing tool,*** vulnerabilities of the organisation’s web site are explored
4. Select a testing framework for web sites	4.1	***Web site testing frameworks*** are evaluated
	4.2	Web site testing framework are selected
	4.3	Features of the web site testing framework are reviewed
	4.4	Individual vulnerabilities within a testing framework are elaborated
5. Perform vulnerability scanning	5.1	Difference between automated testing and manual testing is compared
	5.2	Use of an ***automated web application scanner*** to test an application is demonstrated
	5.3	Results from the automated scanner report are interpreted
	5.4	Use of manual testing of a web application is discussed
6. Identify common web application vulnerabilities	6.1	***Common web application vulnerabilities*** are reviewed
	6.2	Remediation strategies to mitigate the defined web application vulnerabilities are formulated
	6.3	Vulnerabilities for software rework are reported to the developer
7. Exploit web application vulnerabilities	7.1	Testing tools and manual methods used to exploit web application vulnerabilities are selected
	7.2	Advantages and disadvantages of web application testing tools are evaluated
	7.3	Use of testing tool operation to exploit web site vulnerabilities is demonstrated
8. Develop and present the penetration testing report	8.1	***Penetration testing report*** is developed and presented to appropriate personnel
	8.2	Penetration testing report is evaluated and strategies are developed to mitigate web site vulnerabilities
9. Research new web site application developments	9.1	New research topics in vulnerabilities for web site applications are researched
	9.2	Skills in using penetration testing tools to detect vulnerabilities in web sites are developed

REQUIRED SKILLS AND KNOWLEDGE

This describes the essential skills and knowledge and their level required for this unit.

Required skills:

- Articulating relevant issues encountered in the work environment
- Performing calculations in binary and hexadecimal number systems
- Reading and accurately interpreting documents and reports
- Operating a personal computer
- Interpreting network diagrams
- Assembling, participating in and coordinating a work team
- Problem solving within a team environment
- Evaluating the performance of a work team
- Contributing to the process of enhancing team performance
- Developing a project implementation plan including realistic timelines and allocation of tasks for team members
- Establishing project risk assessment
- Gathering, testing and allocating project resources
- Using Penetration testing concepts and procedures for testing a cyber security infrastructure
- Installing and using software packages
- Using basic Linux commands
- Interpret and writing scripts
- Preparing technical documentation
- Making presentation to clients

Required knowledge:

- Web application development practices (e.g. waterfall, agile)
- Web application development environment
- Web architectures
- Web frameworks
- Secure development lifecycle
- Web application enumeration tools (Nikto, dirb, wfuzz, cadaver, wp-scan skipfish etc)
- Custom wordlists for spidering
- User agent string values
- Web application technology stack
- Web application proxy tools eg (burp)
- Spider and scanning tools (eg burp spider)
- Penetration testing frameworks (eg OWASP)
- Common web site vulnerabilities such as:
    - Injection weaknesses
    - Broken Authentication and Session Management weakness
    - Cross Site Scripting (XSS) weaknesses
    - Insecure Direct Object References weaknesses
    - Identify Security Misconfiguration weaknesses
    - Identify Sensitive Data Exposure weaknesses
    - Missing function level access control weaknesses
    - Identify Cross Site Request Forgery (CSRF) weaknesses
    - Using known vulnerable components weaknesses
    - Invalidate redirects and forwards weaknesses

Range Statement

The Range Statement relates to the unit of competency as a whole. It allows for different work environments and situations that may affect performance. Bold / italicised wording in the Performance Criteria is detailed below

Web application development process *includes but not limited to:*	• Waterfall • agile methodology etc
Web application development environment *includes but not limited to:*	• Pre-Production • Production • Unit-Testing • Functional testing • User-Acceptance
Web frameworks *includes but not limited to:*	• Spring • JSF • Ruby on rails • Zend • Symfony • Dot.NET
Tools used to determine the technology stack used in web applications and web servers *includes but not limited to:*	• Nikto • Dirb • Wfuzz • Cadaver • Wp-scan • skipfish
Identifying the technology stack of a web application utilising current resources *includes but not limited to:*	• Favicons • Error messages • Online research
Extended features of a current proxy testing tool *includes but not limited to:*	• Burp web application proxy tools • Burp spider and scanning tools • Burp intruder • Burp cross-site request forgery (CSRF) • Burp sequences • Burp plugins
Web site testing frameworks *includes but not limited to:*	• Open Web Application Security Project (OWASP)
Automated web application scanner *includes but not limited to:*	• Vega • Arachni • Zed attack Proxy (ZAP) • W3af

***Common web application vulnerabilities** includes but not limited to:*

As defined by the OWASP Framework:

- Identify and exploit advanced injection (SQLi) weaknesses
- Identify and exploit broken authentication and session management weakness
- Identify and exploit Cross Site Scripting (XSS) weaknesses
- Identify and exploit insecure direct object reference weaknesses
- Identify and exploit Identify security misconfiguration weaknesses
- Identify and exploit sensitive data exposure weaknesses
- Identify and exploit access control weaknesses
- Identify and exploit Cross Site Request Forgery (CSRF) weaknesses
- Identify and exploit vulnerable components
- Identify and exploit unvalidated redirects and forwards
- Identify and exploit file upload weaknesses
- Identify and exploit data serlalisation weaknesses

***Penetration testing report** includes but not limited to:*

- Executive summary
- Discussion of the root cause/s
- Technical issues
- Risk assessment
- Reproduction steps
- Remediation steps

EVIDENCE GUIDE

The evidence guide provides advice on assessment and must be read in conjunction with the Performance Criteria, Required Skills and Knowledge, the Range Statement and the Assessment section in Section B of the accreditation submission.

Critical aspects for assessment and evidence required to assess competency in this unit

To be considered competent in this unit assessors must be satisfied the candidate can demonstrate the achievement of all of the elements of the competency to the level defined by the associated performance criteria

Specifically they must be able to:

- interpret the web application development process;
- use tools and technology to determine web site content;
- utilise a testing framework for web sites in order to determine web application vulnerabilities;
- develop and present a penetration testing report;
- research new web site application developments.

Context of and specific resources for assessment

Evidence should show competency working in a realistic environment and a variety of conditions. The candidate will have access to all tools, equipment, materials and documentation required. The candidate will be permitted to refer to any relevant workplace procedures, product and manufacturing specifications, codes, standards, manuals and reference materials.

This unit may be assessed on the job, off the job or a combination of both. Where assessment occurs off the job, an appropriate simulation must be used where the range of conditions reflects realistic workplace situations. The competencies covered by this unit would be demonstrated by an individual working alone or as part of a team. The assessment environment should not disadvantage the candidate.

Method of assessment

Evidence can be gathered in a variety of ways including:

- observation of processes and procedures
- oral and/or written questioning on required knowledge and skills
- testimony from supervisors, colleagues, clients and/or other appropriate persons
- inspection of the final product or outcome
- portfolio of documented evidence.

Where performance is not directly observed and/or is required to be demonstrated over a period of time and/or in a number of locations, any evidence should be authenticated by colleagues, supervisors, clients or other appropriate persons.

VU22243 - Develop software skills for the cyber security practitioner

Unit Descriptor

The unit provides the knowledge and skills to examine concepts and operation of an executable (exe) file and an assembler instruction set, principles of the software development process and software vulnerabilities. The unit also develops skills in writing and reading scripts, utilising software troubleshooting techniques and finally, examining the principles of writing secure code.

Employability skills

This unit contains employability skills.

Application of the Unit

This unit is applicable to cyber security practitioners who are required to write and work with software scripts in a cyber security environment. This unit builds on existing foundational software skills required by a cyber security practitioner.

Prerequisite

Nil

ELEMENT		**PERFORMANCE CRITERIA**
Elements describe the essential outcomes of a unit of competency.		Performance criteria describe the required performance needed to demonstrate achievement of the element – they identify the standard for the element. Where bold/italicised text is used, further information or explanation is detailed in the required skills and knowledge and/or the range statement. Assessment of performance is to be consistent with the evidence guide.
1. Identify the interplay of hardware and software of a computer when executing a program	1.1	***Microprocessor architectures*** are identified and classified
	1.2	Overview of an ***assembler instruction set*** is investigated
	1.3	Structure and role of assembly language is defined
	1.4	Structure of an exe file is examined
	1.5	Function and operation of a compiler/linker is defined
	1.6	Process and structure of executing code in virtual machines is defined
	1.7	Processes to reverse engineer code are defined
2. Determine the operation of tools and components utilised in the software design process	2.1	***Various methods to create programs*** are identified
	2.1	Process of malware infecting executable code is identified
	2.3	***Frameworks used to identify a common cyber security software attack*** are examined
3. Write and interpret software scripts	3.1	***Common strategies used to write secure scripts*** are identifed
	3.2	Process of compiling a ***modern scripting language*** to bytecode is developed
	3.3	Code that accepts run time parameters is written
	3.4	Software scripts are interpreted
4. Apply software testing tools and techniques	4.1	Processes and practices of ***modern software testing methodologies*** are evaluated
	4.2	Software troubleshooting methodologies for scripts are developed

5. Identify principles and practices of developing secure code	5.1 ***Operating system tools to secure code*** are examined and deployed
	5.2 Methods to protect and secure code are investigated and deployed

REQUIRED SKILLS AND KNOWLEDGE

This describes the essential skills and knowledge and their level required for this unit.

Required skills:

- Articulating relevant issues encountered in the work environment
- Performing calculations in binary and hexadecimal number systems
- Reading and accurately interpreting documents and reports
- Operating a personal computer
- Applying problem solving methodologies
- Installing and using software packages
- Interpreting and writing scripts
- Preparing technical documentation
- Communicating with colleagues and line managers
- Writing software scripts
- Interpreting software scripts

Required knowledge:

- Fundamentals of computer architecture
- Microprocessor instruction sets
- Registers and stacks
- Fundamentals of assembler programming
- Concepts and operation of bytecode
- Compilers, interpreters and linkers
- Process of compiling a program
- Tools and environments utilised to write programs
- Structure and operation of an exe file
- Methods used to infect exe files
- Software testing methodologies
- Software troubleshooting techniques
- Operating system tools to protect code
- Methods of code execution in virtual images
- Introduction to the procedures to reverse engineer code

Range Statement

The Range Statement relates to the unit of competency as a whole. It allows for different work environments and situations that may affect performance. Bold / italicised wording in the Performance Criteria is detailed below

Microprocessor architectures *includes but not limited to:*

- Memory structures
- Registers
- Stacks
- Pointers
- Core processing units
- Sub processors:
    - Memory Management unit (MMU)
    - Floating point units (FPU)

Assembler instruction set *includes but not limited to:*

- Registers
- Stacks
- Pointers (Index registers
- Instruction groupings:
    - Arithmetic
    - Logic
    - Data transfer
    - Control
    - Floating point

Various methods to create programs *includes but not limited to:*

- Software development environments
- Interpreters
- Scripts
- Bytecode compilers

Frameworks used to identify a common cyber security software attack *includes but not limited to:*

- Open Web Application Security Project (OWASP) framework reports:
    - Buffer overflow
    - SQL injection

Common strategies used to write secure scripts *includes but not limited to:*

- Protecting usernames and passwords
- Encryption strategies
- Saving sensitive file data

Modern scripting language *includes but not limited to:*

- Python
- Java script
- PHP

Modern software testing methodologies *includes but not limited to:*

- Top down design bottom up testing
- Systematic testing strategies
- Writing test sets for code testing
- Inserting code breakpoints
- Invoking single stepping code tools
- White box testing
- Black box testing
- Red box testing

***Operating system tools to secure code** includes but not limited to:*	• EMET (Enhanced Mitigation Experience Toolkit) for windows • Antivirus tools • Windows defender • Nortons Antivirus • Symantec

EVIDENCE GUIDE

The evidence guide provides advice on assessment and must be read in conjunction with the Performance Criteria, Required Skills and Knowledge, the Range Statement and the Assessment section in Section B of the accreditation submission.

Critical aspects for assessment and evidence required to assess competency in this unit

To be considered competent in this unit assessors must be satisfied the candidate can demonstrate the achievement of all of the elements of the competency to the level defined by the associated performance criteria

Specifically they must be able to:

- Demonstrate how code executes at machine level on a computer;
- Utilise tools used in software design;
- Write test and troubleshoot software scripts;
- Interpret scripts;
- Apply tools and practices used to develop secure code

Context of and specific resources for assessment

Evidence should show competency working in a realistic environment and a variety of conditions. The candidate will have access to all tools, equipment, materials and documentation required. The candidate will be permitted to refer to any relevant workplace procedures, product and manufacturing specifications, codes, standards, manuals and reference materials.

This unit may be assessed on the job, off the job or a combination of both. Where assessment occurs off the job, an appropriate simulation must be used where the range of conditions reflects realistic workplace situations. The competencies covered by this unit would be demonstrated by an individual working alone or as part of a team. The assessment environment should not disadvantage the candidate.

Method of assessment

Evidence can be gathered in a variety of ways including:

- observation of processes and procedures
- oral and/or written questioning on required knowledge and skills
- testimony from supervisors, colleagues, clients and/or other appropriate persons
- inspection of the final product or outcome
- portfolio of documented evidence.

Where performance is not directly observed and/or is required to be demonstrated over a period of time and/or in a number of locations, any evidence should be authenticated by colleagues, supervisors, clients or other appropriate persons.

VU22244 - Implement best practices for identity management

Unit Descriptor

This unit provides the knowledge and skills to apply strategies to deal with issues associated with fraudulent identity and to deploy best practices for identity and access management for an organisation

Employability skills

This unit contains employability skills.

Application of the Unit

This unit is applicable to a cyber security or IT paraprofessional who is responsible for configuring, setting up, monitoring and decommissioning users in an organisation

Prerequisite

Nil

ELEMENT Elements describe the essential outcomes of a unit of competency.	**PERFORMANCE CRITERIA** Performance criteria describe the required performance needed to demonstrate achievement of the element – they identify the standard for the element. Where bold/italicised text is used, further information or explanation is detailed in the required skills and knowledge and/or the range statement. Assessment of performance is to be consistent with the evidence guide.
1. Explore the function and operation of key identity and access management features and operation	1.1 ***Identity theft and identity fraud methods*** are evaluated
	1.2 Function and operation of ***common authentication services*** are compared
	1.3 Key Australian legislation regarding identity theft and identity fraud is identified
	1.4 Function and operation of ***Identification, Authentication and Authorization access control services*** are evaluated
	1.5 ***Emerging identification technologies*** are identified and evaluated
	1.6 Differences between identity federation and Single Sign On (SSO) are defined
	1.7 ***Password policies*** for the organisation are defined
2. Implement best practices for user account management	2.1 ***Key personnel*** tasked to deal with user account management are identified
	2.2 Mitigating strategies that deal with multiple or shared accounts are evaluated and implemented
	2.3 Current operating system ***account policy enforcement*** is reviewed and implemented
	2.4 Current operating system group based privileges are reviewed and implemented
	2.5 Current operating system user assigned privileges are reviewed and implemented

	2.6	Current monitoring access and identity controls are reviewed and implemented
3. Identify, configure and monitor identity management for the organisation	3.1	***Working principles for identity management*** are examined
	3.2	Process to configure identity management for various ***operating systems*** is investigated
	3.3	Identity management for an operating system is implemented
	3.4	Testing strategies for identity management vulnerabilities are developed
	3.5	Testing strategies to the identity management system of the operating system to determine its' vulnerabilities are applied
	3.6	Identity management processes are evaluated with key personnel and if required, are modified to improve security
4. Identify, configure and monitor access management for the organisation	4.1	***Working principles for access management*** are examined
	4.2	Access management for an operating system is investigated and implemented
	4.3	Testing strategies for access management vulnerabilities are developed
	4.4	Testing strategies on the access management system for an operating system to determine its' vulnerabilities are applied
	4.5	Access management processes are evaluated with key personnel and modify if required for improved security

REQUIRED SKILLS AND KNOWLEDGE

This describes the essential skills and knowledge and their level required for this unit

Required skills:

- Articulating relevant issues encountered in the work environment
- Reading and accurately interpreting documents and reports
- Determine changes required to work practices to implement new policies and procedures
- Assembling, participating in and coordinating a work team
- Problem solving within a team environment
- Contributing to the process of enhancing team performance
- Establishing project risk assessment
- Gathering, testing and allocating project resources
- Preparing technical documentation
- Configuring features of an operating system
- Evaluating new technologies
- Configuring users with Windows Server
- Configuring users with MAC OS X Lion or Sierra
- Configuring users with Linux
- Implementing mitigation strategies for the organisation
- Applying communication styles for key decision making groups
- Evaluating the effectiveness of policies, standards and procedures (Continuous improvement)

Required knowledge:

- The identity lifecycle:
  - provisioning
  - revalidation
  - deprovisioning
- Identity theft
- Key Australian legislation regarding identity theft and identity fraud
- Authentication and Authorisation Access
- New trends in determining identity
- Identity federation
- Identity fraud
- Identity management
- Risk assessment

Range Statement

The Range Statement relates to the unit of competency as a whole. It allows for different work environments and situations that may affect performance. Bold / italicised wording in the Performance Criteria is detailed below

Identity theft and identity fraud methods. includes but not limited to:

- Identity theft:
  - Stolen electronic records
  - Searching dumped files
  - Misuse of authority
  - Stolen personal records, physical or electronic
  - Impersonation
  - etc
- Identity fraud:
  - Phishing
  - Pharming
  - Skimming

Common authentication services includes but not limited to:

- RADIUS
- TACACS+
- Kerberos
- LDAP
- Secure LDAP

Identification, Authentication and Authorization access control services includes but not limited to:

- Identification:
  - Username
  - Smart Card
- Authentication:
  - Tokens
  - Smart Card
  - CHAP
  - PAP
- Authorisation:
  - Least privilege
  - Rule-based access control
  - Time of day restrictions

Emerging identification technologies includes but not limited to:

- Biometric:
  - Facial recognition
  - Finger print
  - Hand geometry
  - Iris detection
  - Retinal pattern
  - Signature
  - Voice print
  - Thermograms

Password policies include but not limited to:

- Changing passwords
- Password strength
- Securing passwords

Key personnel includes but not limited to:	• Cyber security paraprofessional • Team manager • External consultants • Relevant managers • Business stakeholders
Account policy enforcement includes but not limited to:	• Credential enforcement • Group policy • Password complexity • Account expiry • Lockout
Working principles for identity management includes but not limited to:	• Provisioning, Revalidation and Deprovisioning • Identity Federation • Synchronisation • Consolidation
Operating systems includes but not limited to:	• Windows • Linux • MAC OS
Working principles for access management includes but not limited to:	• Authentication • Authorisation • Accounting

EVIDENCE GUIDE

The evidence guide provides advice on assessment and must be read in conjunction with the Performance Criteria, Required Skills and Knowledge, the Range Statement and the Assessment section in Section B of the accreditation submission.

Critical aspects for assessment and evidence required to assess competency in this unit

To be considered competent in this unit assessors must be satisfied the candidate can demonstrate the achievement of all of the elements of the competency to the level defined by the associated performance criteria

Specifically they must be able to:

- Implement best practices for user account management utilising an operating system;
- Identify, configure and monitor identity management for the organisation utilising current software tools and strategies;

Context of and specific resources for assessment

Evidence should show competency working in a realistic environment and a variety of conditions. The candidate will have access to all tools, equipment, materials and documentation required. The candidate will be permitted to refer to any relevant workplace procedures, product and manufacturing specifications, codes, standards, manuals and reference materials.

This unit may be assessed on the job, off the job or a combination of both. Where assessment occurs off the job, an appropriate simulation must be used where the range of conditions reflects realistic workplace situations. The competencies covered by this unit would be demonstrated by an individual working alone or as part of a team. The assessment environment should not disadvantage the candidate.

Method of assessment

Evidence can be gathered in a variety of ways including:

- observation of processes and procedures
- oral and/or written questioning on required knowledge and skills
- testimony from supervisors, colleagues, clients and/or other appropriate persons
- inspection of the final product or outcome
- portfolio of documented evidence.

Where performance is not directly observed and/or is required to be demonstrated over a period of time and/or in a number of locations, any evidence should be authenticated by colleagues, supervisors, clients or other appropriate persons.

VU22245 – Plan and implement a cyber security project

Unit Descriptor

This unit provides the knowledge and skills to plan and implement a cyber security project that either simulates a real cyber security environment or is an actual workplace project.

Learners are required to actively participate and contribute to the project team. They are required to receive tasks, communicate outcomes, design solutions, solve project problems and meet required deadlines to ensure effective and timely delivery of the project.

The project may include using a Cyber Security Operations Centre (CSOC) sandbox or equivalent laboratory environment. This environment allows the learner to demonstrate configuring and testing of firewalls, implementing Intrusion Detection System (IDS) and evaluating and identifying any traffic anomalies. The use of Red and Blue teaming exercises to identify security breaches and apply mitigation strategies to minimise further risk should be included as part of the project.

Employability skills

This unit contains employability skills.

Application of the Unit

This unit is applicable to cyber security or IT paraprofessionals working in an organisation and responsible to deliver a cyber security project.

Prerequisite

VU22240 - Communicate cyber security incidents within the organisation

VU22243 - Develop software skills for the cyber security practitioner

VU22244 - Implement best practice for identity management

ELEMENT Elements describe the essential outcomes of a unit of competency.	**PERFORMANCE CRITERIA** Performance criteria describe the required performance needed to demonstrate achievement of the element – they identify the standard for the element. Where bold/italicised text is used, further information or explanation is detailed in the required skills and knowledge and/or the range statement. Assessment of performance is to be consistent with the evidence guide.
1. Identify the strategic and operational needs of the project during the planning phase	1.1 Strategic and operational needs of the ***cyber security project*** during the planning phase is identified
	1.2 Cyber security project's strategic context and requirements are identified and considered
	1.3 Implications of the organisation's ***strategic and business plans***, and its' output requirements are identified and considered
	1.4 ***Client requirements*** and the impact of ***legislation and industry codes and standards*** are identified and explored
	1.5 ***Risk management analysis*** is conducted and a risk management plan is prepared and documented
2. Support the preparation of the project plan	2.1 ***Precise specifications and terms of reference*** for the cyber security project are defined and documented
	2.2 ***Physical and other resources*** required to support the cyber security project are defined, documented and secured
	2.3 ***Timelines, schedules and critical paths*** for the cyber security project, taking into consideration contingencies and planning for time slippages are developed and documented

	2.4	Project budget which takes into consideration the cost of the primary project, management of a range of sub tasks and contingencies is prepared
	2.5	Consultation strategies used to inform clients, contractors and other interested parties of the cyber security project's progress are defined and documented
3. Support the assembly of personnel for the project team	3.1	Required skills needed for the successful completion of the cyber security project are identified
	3.2	Required skills for the cyber security project are mapped against the available personnel
	3.3	Effective communication processes to coordinate work are implemented
	3.4	Clear reporting processes are identified and communicated
	3.5	Modifications and improvements to the cyber security project are suggested
4. Design the subtask for the project	4.1	The delegated task for the project is defined and recieved
	4.2	Action plan for each project subtask is prepared and where possible tested for functionality
	4.3	Outputs of the subtask are tested for interconnectivity and functionality
5. Gather resources and test the system design	5.1	Project resources are acquired according to organisational policy
	5.2	Vendor documentation for the equipment purchased is collated
	5.3	Operation and functionality of the acquired equipment to achieve the project outcomes is investigated
	5.4	Project subtasks are built, and where possible tested for functionality
6. Implement the project solution	6.1	Each subtask of the project is interconnected and tested for functionality
	6.2	Verification of end to end functionality of the project design is performed and changes are made if required to ensure the design brief is achieved
	6.3	Further testing and modification are undertaken to the system if required to ensure the design brief is achieved
7. Use project outcome to contribute to improved policies and processes	7.1	Opportunities for wider organisational learning including improvements to current policies and procedures are identified
	7.2	Opportunities for future and further developments following the project completion are identified and conveyed to senior management
	7.3	Strategic impact of the project is considered and feed into the organisation's ongoing strategic planning processes
	8.1	Cyber security project is completed in line with the requirements of the project plan

8. Finalise the project and facilitate handover	8.2	Project handover is undertaken in accordance with ***organisational procedures*** to staff responsible for ongoing implementation and maintenance
	8.3	Team members and relevant stakeholders are debriefed concerning the conduct of the project and outcomes achieved
	8.4	Report analysing the strengths and weaknesses of the project plan and the conduct of the project is prepared

REQUIRED SKILLS AND KNOWLEDGE

This describes the essential skills and knowledge and their level required for this unit.

Required skills:

- Designing and implementing a cyber security project
- Contributing to a planning processes
- Scheduling human resources
- Reporting and responding to contingencies
- Aligning project brief with organisational strategies and required outcomes
- Assessing project outcomes and providing recommendations that will refine and improve future projects
- Problem solving within a team environment
- Contributing to the process of enhancing team performance
- Gathering, testing and allocating project resources
- Preparing technical documentation
- Communicating with team members and other stakeholders
- Working independently and as a team member
- Interpreting vendor equipment documents
- Clear and decisive decision making
- Configuring cyber security equipment
- Analysing and interpreting information
- Testing methodologies
- Operating software testing packages
- Interconnecting virtual images
- Creating and configuring virtualised images
- Identifying and using networking devices

Required knowledge:

- Concepts of risk management planning processes and assessment
- Relevant current legislation, codes and standards
- Tools and models of project management
- Organisational structures, frameworks and functions, including:
    - enterprises
    - government bodies
    - industry associations
- Troubleshooting techniques
- Working in teams
- Design of cyber security infrastructure
- Operating systems (Windows or Linux)
- Virtualisation operation and structure
- Introductory red and blue teaming exercises

Range Statement

The Range Statement relates to the unit of competency as a whole. It allows for different work environments and situations that may affect performance. Bold / italicised wording in the Performance Criteria is detailed below

Cyber security project includes but not limited to:	• Detailed Security infrastructure • Cyber Security Operations Centre • Capture the flag event
Strategic and business plans includes but not limited to:	• Target Customers • Industry Analysis • Marketing Plan • Financial Projections • Mission statement • SWOT Analysis • Goals • Infrastructure development and upgrade • Growth predictions • KPI's
Client requirements includes but not limited to:	• Functionality • Scalability • Cost • User experience
Legislation and industry codes and standards includes but not limited to:	• Workplace OH&S • Cyber security legislation • Privacy laws • Workplace relations • Worker code of conduct • Relevant standards
Risk management analysis but not limited to:	• Identifying risk • Analysing risk • Responding to risk
Precise specifications and terms of reference includes but not limited to:	• Functionality • User experience • Management • Defining roles and expectations • Engaging external contractors • Non-disclosure requirements • Planned implementation • Service disruption • Delivery penalties
Physical and other resources includes but not limited to:	• Workspace • Equipment • Environment

Timelines, schedules and critical paths includes but not limited to:	• Selection and use of automated tools • Defining subtask interdependencies • Timelines • Handover • Commissioning • Methods development
Organisational procedures includes but not limited to:	• Invoicing/Payment • Project debriefing • Documentation • Project handover • Staff debriefing

EVIDENCE GUIDE

The evidence guide provides advice on assessment and must be read in conjunction with the Performance Criteria, Required Skills and Knowledge, the Range Statement and the Assessment section in Section B of the accreditation submission.

Critical aspects for assessment and evidence required to assess competency in this unit

To be considered competent in this unit assessors must be satisfied the candidate can demonstrate the achievement of all of the elements of the competency to the level defined by the associated performance criteria

Specifically they must be able to:

- plan, resource, implement and hand over a cyber security project;
- analyse and document the project achievements against the planned outcomes including the strengths and weaknesses of the planning, resourcing, implementation and management processes.

Context of and specific resources for assessment

Evidence should show competency working in a realistic environment and a variety of conditions. The candidate will have access to all tools, equipment, materials and documentation required. The candidate will be permitted to refer to any relevant workplace procedures, product and manufacturing specifications, codes, standards, manuals and reference materials.

This unit may be assessed on the job, off the job or a combination of both. Where assessment occurs off the job, an appropriate simulation must be used where the range of conditions reflects realistic workplace situations. The competencies covered by this unit would be demonstrated by an individual working alone or as part of a team. The assessment environment should not disadvantage the candidate.

Method of assessment

Evidence can be gathered in a variety of ways including:

- observation of processes and procedures
- oral and/or written questioning on required knowledge and skills
- testimony from supervisors, colleagues, clients and/or other appropriate persons
- inspection of the final product or outcome
- portfolio of documented evidence.

Where performance is not directly observed and/or is required to be demonstrated over a period of time and/or in a number of locations, any evidence should be authenticated by colleagues, supervisors, clients or other appropriate persons.

VU22252 - Implement cyber security operations

Unit Descriptor	The unit provides the knowledge and skills to implement and monitor a cyber security operation for an organisation. The unit addresses the key elements of implementation which include preparing the organisation for an incident, knowing how it could occur, and the processes and procedures to respond. The unit also includes the use of tools and processes to analyse data and detect intrusions. The unit applies procedures and processes developed by the National Institute of Standards and Technology (NIST) and it aligns with the Cisco Cyber Operations course
Employability skills	This unit contains employability skills.
Application of the Unit	This unit is applicable to cyber security or IT paraprofessionals who are responsible for implementing and monitoring cyber security operations for an organisation
Prerequisite	Nil

ELEMENT	**PERFORMANCE CRITERIA**	
Elements describe the essential outcomes of a unit of competency.	Performance criteria describe the required performance needed to demonstrate achievement of the element – they identify the standard for the element. Where bold/italicised text is used, further information or explanation is detailed in the required skills and knowledge and/or the range statement. Assessment of performance is to be consistent with the evidence guide.	
1. Define endpoint threat analysis and computer forensics	1.1	Common Vulnerability Scoring System CVSS 3.0 for risk assessment is defined
	1.2	***Cyber security features*** are classified for risk assessment
	1.3	***Windows file system components*** are defined
	1.4	***Linux file system components*** are defined
	1.5	***Evidence types*** are contrasted
	1.6	Altered and unaltered disk images are contrasted
	1.7	Role of assets and ***threat actors*** are defined
2. Analysing network intrusion events	2.1	Vulnerabilities in ***networking protocols*** are evaluated
	2.2	Elements from a NetFlow record of a security event are analysed
	2.3	***Network monitoring tools*** are identified, evaluated and selected
	2.4	***Key elements in an intrusion*** are identified
	2.5	Data from an event is acquired
	2.6	*Selected* ***intrusion elements*** from an event to ***common source technologies*** are mapped

	2.7	Intrusion detection flags such as False Positive, False Negative, True Positive and True Negative are defined
3. Prepare to deal with incident responses	3.1	Incident response plan from the National Institute of Standards and Technology (NIST) described in the NIST.SP800-61 r2 document is evaluated and implemented
	3.2	Organisation ***incident response plan*** is implemented
	3.3	Function and role of the Cyber Security Incident Response Team (CSIRT) is defined
	3.4	Elements for ***network profiling*** are defined
	3.5	Elements for ***server profiling*** are defined
	3.6	Acquired data is mapped to finance, health or credit card compliance frameworks
4. Compose processes for data and event analysis	4.1	***Steps and methods used to gather data*** are described and evaluated
	4.2	Domain Name Server (DNS) and HTTP logs are mapped to identify threat actors
	4.3	Threat intelligence data is collated from internal records and public trusted sites
	4.4	Organisational detection tools and methods are utilised to correlate generated alerts from multiple data sources
	4.5	***Alternative tools and techniques used for data analysis*** are utilised
5. Apply models and processes to incidents	5.1	***Diamond model of intrusion detection*** is described and evaluated
	5.2	Intrusion events are classified according to the diamond model of intrusion
	5.3	Incident response processes are applied to the event
	5.4	***Selected range of activities relating to incident handling*** are defined
	5.5	***Documents that support the organisation to collect forensic data for incident responses*** are identified, evaluated and adopted
	5.6	***Data evidence and collection forensic activities*** are defined according to organisational guidelines
	5.7	***Vocabulary for Event Recording and Incident Sharing (VERIS) schema categories*** are defined, evaluated and implemented
	5.8	VERIS schema categories are applied to the incident

REQUIRED SKILLS AND KNOWLEDGE

This describes the essential skills and knowledge and their level required for this unit.

Required skills:

- Articulating relevant issues encountered in the work environment
- Reading and accurately interpreting documents and reports
- Operating a personal computer
- Assembling, participating in and coordinating a work team
- Problem solving within a team environment
- Evaluating the performance of a work team
- Contributing to the process of enhancing team performance
- Establishing project risk assessment
- Gathering, testing and allocating project resources
- Installing and using software packages
- Preparing technical documentation
- Making presentation to clients
- Communicating and engaging external contractors
- Escalating procedures
- Working calmly in a stressful environment
- Clear decision making
- Communicating effectively to different working groups
- Coordinating/managing an incident
- Identifying sources of threat data
- Gathering data
- Evaluating and contributing to organisation's policies and procedures
- Evaluating new technologies

Required knowledge:

- Ethics and communication techniques
- Group collaboration and decision making
- Presentation skills to decision making group
- Function and role of the monitoring equipment and software
- Communication styles
- Roles and responsibilities within an organisation and to whom to communicate an incident
- Escalation strategies
- Risk assessment of incidents
- Incident response
- Tools and techniques used in the organisation to deal with incidents
- Documentation techniques

Range Statement

The Range Statement relates to the unit of competency as a whole. It allows for different work environments and situations that may affect performance. Bold / italicised wording in the Performance Criteria is detailed below

Cyber security features includes but not limited to:	• Attack Vector • Attack complexity • Privileges required • User interaction • Scope • Confidentiality • Integrity • Availability
Windows file system components includes but not limited to:	• FAT32 • NTFS • Alternative data streams • MACE • EFI • Free space • Timestamps on a file system
Linux file system components includes but not limited to:	• EX4 • Journaling • MBR • Swap file system • MAC
Evidence types includes but not limited to:	• Best evidence • Corroborative evidence • Indirect evidence
Threat actors includes but not limited to:	• Cyber Criminals, Organized and Otherwise • Hacktivists • State-Sponsored Attackers • State-Sponsored Attackers
Networking protocols includes but not limited to:	• Ethernet frame • IPv4 • IPv6 • TCP • UDP • ICMP • HTTP
Network monitoring tools includes but not limited to:	• Wireshark • Tcpdump • CA Netmaster • Microsoft network monitor

Key elements in an intrusion includes but not limited to:

- Source address
- Destination address
- Source port
- Destination port
- Protocols

Selected intrusion elements includes but not limited to:

- IP address (source and destination)
- Client and server port identity
- Process (file or registry)
- Hashes
- URI or URL

Common source technologies includes but not limited to:

- NetFlow
- IDS/IPS
- Firewall
- Network application control
- Antivirus

Incident response plan includes but not limited to:

- Mapping elements of analysis:
    - Preparation
    - Detection and analysis
    - Containment, eradication and recovery
    - Post-incident analysis
- Mapping organisational stakeholders:
    - Preparation
    - Detection and analysis
    - Containment, eradication and recovery
    - Post-incident analysis

Network profiling includes but not limited to:

- Total traffic throughput
- Session duration
- Ports used
- Address space utilized

Server profiling includes but not limited to:

- Listening ports
- Logged in users
- Running processes
- Running tasks
- Applications

Steps and methods used to gather data includes but not limited to:

- The process of data normalization
- 5-turple correlation structure and methods
- Retrospective analysis
- Identifying compromised networked hosts

Alternative tools and techniques used for data analysis includes but not limited to:

- Deterministic methods of data analysis
- Probabilistic methods of data analysis
- Heuristic methods of data analysis

Diamond model of classify intrusion events includes but not limited to:

- Reconnaissance
- Weponization
- Delivery
- Exploitation
- Installation
- Command and control
- Action on objectives

Selected range of activities relating to incident handling includes but not limited to:

- Scoping
- Containment
- Remediation
- Lesson-based hardening
- Reporting

Documents that support the organisation to collect forensic data for incident responses includes but not limited to:

- Guide to Integrating Forensic Techniques into Incident Response (NIST SP800-86)

Data evidence and collection forensic activities includes but not limited to:

- Evidence collection order
- Data integrity
- Data preservation
- Volatile data collection

Vocabulary for Event Recording and Incident Sharing (VERIS) schema categories includes but not limited to:

- Incident tracking
- Incident description
- Discovery and response
- Impact assessment

EVIDENCE GUIDE

The evidence guide provides advice on assessment and must be read in conjunction with the Performance Criteria, Required Skills and Knowledge, the Range Statement and the Assessment section in Section B of the accreditation submission.

Critical aspects for assessment and evidence required to assess competency in this unit

To be considered competent in this unit assessors must be satisfied the candidate can demonstrate the achievement of all of the elements of the competency to the level defined by the associated performance criteria

Specifically they must be able to:

- classify threats and demonstrate how threats occur;
- prepare the organisation to deal with incident responses;
- compose processes for data and event analysis;
- analyse data and detect intrusions;
- apply models and processes to incidents;

Context of and specific resources for assessment

Evidence should show competency working in a realistic environment and a variety of conditions. The candidate will have access to all tools, equipment, materials and documentation required. The candidate will be permitted to refer to any relevant workplace procedures, product and manufacturing specifications, codes, standards, manuals and reference materials.

This unit may be assessed on the job, off the job or a combination of both. Where assessment occurs off the job, an appropriate simulation must be used where the range of conditions reflects realistic workplace situations. The competencies covered by this unit would be demonstrated by an individual working alone or as part of a team. The assessment environment should not disadvantage the candidate.

Method of assessment

Evidence can be gathered in a variety of ways including:

- observation of processes and procedures
- oral and/or written questioning on required knowledge and skills
- testimony from supervisors, colleagues, clients and/or other appropriate persons
- inspection of the final product or outcome
- portfolio of documented evidence.

Where performance is not directly observed and/or is required to be demonstrated over a period of time and/or in a number of locations, any evidence should be authenticated by colleagues, supervisors, clients or other appropriate persons.

VU22246 - Evaluate an organisation’s compliance with relevant cyber security standards and Law

Unit Descriptor

This unit provides the knowledge and skills to enable a cyber security paraprofessional as part of a team, to identify relevant cyber standards and laws pertaining to the organisation, evaluate current working practices in light of these standards and laws and to plan and implement any required work practice changes

Employability skills

This unit contains employability skills.

Application of the Unit

This unit is applicable to a cyber security paraprofessional who as part of a team, is responsible for implementing and monitoring an organisation’s compliance to relevant Australian standards and law.

Prerequisite

Nil

ELEMENT		**PERFORMANCE CRITERIA**
Elements describe the essential outcomes of a unit of competency.		Performance criteria describe the required performance needed to demonstrate achievement of the element – they identify the standard for the element. Where bold/italicised text is used, further information or explanation is detailed in the required skills and knowledge and/or the range statement. Assessment of performance is to be consistent with the evidence guide.
1. Identity the structure of the Australian legal system	1.1	Key ***legal terms*** are defined
	1.2	***Types of legal systems*** are investigated
	1.3	***Kinds of common law*** are identified
	1.4	Structure of the Australian federal system of government is defined
	1.5	Relationship between federal and state regulation is clarified
2. Defining Australian Cyber Law	2.1	***Model laws on electronic commerce*** are investigated
	2.2	***Conventions on the use of electronic communications*** are defined
	2.3	***Relevant international cybercrime conventions*** are investigated
	2.4	Repercussions of the international General Data Protection Regulation (GDPR) and its adoption in Australia is investigated
	2.5	***Key Acts defining Cyber Law in Australia*** are defined
3. Identify mandatory and discretionary cyber laws and practices	3.1	***Categories of information that the law affords protection*** as they pertain to cyber security for the organisation are identified
	3.2	***Legal resources pertaining to Cyber Law*** are identified
	3.3	***Relevant laws for particular industry sectors*** are identified and collated
	3.4	Difference between State and federal legislation for relevant laws pertaining to cyber security are identified

	3.5	Mandatory and discretionary outcomes of ***current Commonwealth Acts as they pertain to cyber security*** for the organisation are identified
	3.6	Mandatory and discretionary outcomes of ***current State based Acts as they pertain to cyber security*** for the organisation are identified
	3.7	***Codes*** pertinent to the organisation’s industry sector are identified
	3.8	***Frameworks*** pertinent to the organisation’s industry sector are identified
	3.9	***Voluntary codes and best practices for the industry sector*** aligned to the organisation are identified
4. Evaluate and select relevant Australian regulation and practices pertaining to security of the organisation	4.1	Methodology of utilising legal resources relevant to cyber law for the organisation is defined and demonstrated
	4.2	Mandatory regulations, standards, codes and frameworks pertaining to cyber security for the organisation are evaluated and selected
	4.3	Discretionary standards, codes and frameworks pertaining to cyber security for the organisation are evaluated and selected
	4.4	Voluntary codes and best practice for the industry sector aligned to the organisation are evaluated and selected
5. Implement relevant Australian regulation and practices pertaining to security of the organisation	5.1	Strategies to implement mandatory regulations, standards, codes and frameworks for the organisation are developed
	5.2	Strategies to implement discretionary standards, codes and frameworks for the organisation are developed
	5.3	Strategies to implement voluntary codes and best practice guidelines and organisational practices for the organisation are developed
	5.4	Organisational changes to appropriate groups within the organisation are articulated
6. Monitor the effectiveness of the organisation’s implementation regulation and practices	6.1	Criteria that measures the effectiveness of implemented changes to working practices required to implement the adopted organisational changes is created
	6.2	Utilising the developed list of criteria, the effectiveness of changes to the organisation’s working practices are measured and monitored
	6.3	Changes to the organisation’s working practices are documented and reported to appropriate organisational groups

REQUIRED SKILLS AND KNOWLEDGE

This describes the essential skills and knowledge and their level required for this unit

Required skills:

- Articulating relevant issues encountered in the work environment
- Reading and accurately interpreting documents and reports
- As part of a team determining changes required to work practices to implement new cyber security policies and procedures
- Participating and problem solving within a team environment
- Establishing project risk assessment
- Preparing technical documentation
- Facilitating the implementing organisational staff training programs
- Evaluating of policies, standards and procedures effectiveness (Continuous improvement)

Required knowledge:

- Australian federal system of Government
- Difference between federal and state regulation
- Accessing state and federal Acts (statutes) - using http://www.austlii.edu.au/
- Interpreting Cyber Law requirements for the organisation from state and federal acts
- Mandatory, Discretionary and Voluntary codes and best practices for the industry sector
- Key features of Federal Mandatory Acts pertaining to Cyber Security
  - ELECTRONIC TRANSACTIONS ACT 1999
  - CORPORATIONS ACT 2001
  - CRIMINAL CODE ACT 1995
  - PRIVACY ACT 1988
  - FREEDOM OF INFORMATION ACT 1982
  - TELECOMMUNICATIONS (INTERCEPTION AND ACCESS) ACT 1979
  - COMPETITION AND CONSUMER ACT 2010 (Can include SPAM Act 2003)
- Key features of State Mandatory Acts pertaining to Cyber Security
  - WRONGS ACT 1958
  - ELECTRONIC TRANSACTIONS (VICTORIA) ACT 2000
- Supporting work practices and standards (Discretionary adoption)
  - (National Institute of Standards and Technology) NIST Cybersecurity Framework
  - ISO 31000 Risk Management
  - ISO/IEC 38500:2015 Preview Information technology - Governance of IT for the organisation
  - ISO 15489 -1:2016 Preview Information and documentation - Records management - Part 1: Concepts and principles
  - ISO/IEC 27000 family - Information security management systems
  - BS 10008 - Evidential Weight and Legal Admissibility of Electronic Information
  - ISO/IEC 29100:2011 Preview Information technology - Security techniques - Privacy framework
  - Victorian Protective Data Security Framework (VPDSF)
- Key feature of Control Objectives for Information and Related Technologies (COBIT) as they pertain to Risk and IT governance
- Key feature of Information Technology Infrastructure Library (ITIL) as they pertain to risk and IT governance
- Legal implications of adopted standards and procedures
- Risk assessment
- Differences between security frameworks, policies, standards, procedures, guidelines, and legislation

Range Statement

The Range Statement relates to the unit of competency as a whole. It allows for different work environments and situations that may affect performance. Bold / italicised wording in the Performance Criteria is detailed below

Legal terms includes but not limited to:

- Act
- Law
- Regulation
- Statute
- Leglislation

Types of Legal systems includes but not limited to:

- Civil System
- Common System
- Customary
- Religious
- Mixed

Kinds of common law includes but not limited to:

- Civil Law (Tort)
- Criminal Law
- Administrative (Regulatory Law)

Model laws on electronic commerce includes but not limited to:

- The United Nations Commission on International Trade Law (UNCITRAL) Model Laws on Electronic Commerce

Conventions on the use of electronic communications includes but not limited to:

- UNCITRAL Convention on the Use of Electronic Communications

Relevant international Cybercrime convections includes but not limited to:

- Council of Europe's Convention on Cybercrime
- Budapest Convention on Cybercrime

Key Acts defining Cyber Law in Australia includes but not limited to:

- Commonwealth
    - ELECTRONIC TRANSACTIONS ACT 1999
- State (eg Victoria but all states have state based Acts)
    - ELECTRONIC TRANSACTIONS (VICTORIA) ACT 2000

Categories of information that the law affords protection includes but not limited to:

- privacy and personal information
- confidential information
- secret information
- intellectual property

Legal resources pertaining to Cyber Law includes but not limited to:

- Overview of state and federal Acts (statutes) see http://www.austlii.edu.au/

Relevant laws for particular industry sectors includes but not limited to:

- Banking and Finance
- Health
    - NATIONAL HEALTH ACT 1953
    - HEALTH RECORDS ACT 2001(VIC)
- Mining
- Internet service providers
- Telecommunications Providers
- Retailers
- Utilities

Current Commonwealth Acts as they pertain to cyber security includes but not limited to:

- CORPORATIONS ACT 2001
    - Discretionary
        - ISO 31000 Risk management
        - ISO/IEC 38500:2015 Preview
        - Information technology -- Governance of IT for the organisation
        - ISO 15489-1:2016 Preview
        - Information and documentation -- Records management -- Part 1: Concepts and principles
        - ISO/IEC 27000 family - Information security management systems
- CRIMINAL CODE ACT 1995
    - Discretionary
        - BS 10008 - Evidential Weight and Legal Admissibility of Electronic Information
- PRIVACY ACT 1988
    - Discretionary
        - ISO/IEC 29100:2011 Preview
        - Information technology - Security techniques - Privacy framework
- FREEDOM OF INFORMATION ACT 1982
- TELECOMMUNICATIONS (INTERCEPTION AND ACCESS) ACT 1979
- COMPETITION AND CONSUMER ACT 2010 (Can include SPAM Act 2003)

Current State based Acts as they pertain to cyber security includes but not limited to:

- (eg Victoria but each state has relevant Acts)
    - WRONGS ACT 1958
        - Discretionary
            - Victorian Protective Data Security Framework (VPDSF)

Codes includes but not limited to:

- Corporate governance
- Data governance
- Information security governance
- Responsible information governance
- Industry specific codes
    - Financial
    - Health
    - Mining

Frameworks includes but not limited to:	• Control Objectives for Information and Related Technologies (COBIT) • Information Technology Infrastructure Library (ITIL) • Prince 2
Voluntary codes and best practices for the industry sector includes but not limited to:	• North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Reliability standard version 7 • National Institute of Standards and Technology (NIST) Cyber security Framework for Critical Infrastructure • ISO/IEC 27002:2013 Information Technology – Security techniques code of practice • ISO/IEC TR 27019:2013 Information Technology - Security techniques information security management • NIST SP 800-82 Guide to Industrial control Systems (ICS) Security • Protective Security Policy Framework (PSPF) • Information Security Manual (ISM) Produced by the Australian Signals Directorate (ASD) • Prudential Practice Guide CPG 235 – Managing Data Risk • Prudential Practice Guide PPG 234 – Management of security risk in information and information technology • Australian Securities and Investment Corporation (ASIC) Report 429 • The Communication Alliance (iCodes). iCode C650:2014 voluntary code adopted by all Internet Service Providers (ISPs) in Australia)

EVIDENCE GUIDE

The evidence guide provides advice on assessment and must be read in conjunction with the Performance Criteria, Required Skills and Knowledge, the Range Statement and the Assessment section in Section B of the accreditation submission.

Critical aspects for assessment and evidence required to assess competency in this unit

To be considered competent in this unit assessors must be satisfied the candidate can demonstrate the achievement of all of the elements of the competency to the level defined by the associated performance criteria.

Specifically they must be able to:

- Clarify the structure of the Australian legal system;
- Demonstrate organisational compliance through the use of standards, frameworks, codes and best practice;
- Identify mandatory and discretionary cyber laws and practices;
- Evaluate, select and implement relevant Australian regulation and practices pertaining to security of the organisation;
- Monitor the effectiveness of the organisation's implementation regulation and practices;

Context of and specific resources for assessment

Evidence should show competency working in a realistic environment and a variety of conditions. The candidate will have access to all tools, equipment, materials and documentation required. The candidate will be permitted to refer to any relevant workplace procedures, product and manufacturing specifications, codes, standards, manuals and reference materials.

This unit may be assessed on the job, off the job or a combination of both. Where assessment occurs off the job, an appropriate simulation must be used where the range of conditions reflects realistic workplace situations. The competencies covered by this unit would be demonstrated by an individual working alone or as part of a team. The assessment environment should not disadvantage the candidate.

Method of assessment

Evidence can be gathered in a variety of ways including:

- observation of processes and procedures
- oral and/or written questioning on required knowledge and skills
- testimony from supervisors, colleagues, clients and/or other appropriate persons
- inspection of the final product or outcome
- portfolio of documented evidence.

Where performance is not directly observed and/or is required to be demonstrated over a period of time and/or in a number of locations, any evidence should be authenticated by colleagues, supervisors, clients or other appropriate persons.

VU22249 - Perform a security risk assessment for an organisation

Unit Descriptor

This unit provides skills and knowledge required to perform a risk assessment for the organisation; this assessment is most likely performed as part of a team. The unit covers; assessing current assets, identify current threats and vulnerabilities, identify a risk process and performing the assessment.

No licensing or certification requirements apply to this unit at the time of accreditation.

Employability Skills

This unit contains employability skills.

Application of the Unit

This unit will apply to cyber security paraprofessional working a team member in an organisation. As part of their role they are required to perform (or review) a risk assessment for the organisation.

Prerequisite Unit/s

Nil

ELEMENT Elements describe the essential outcomes of a unit of competency.	**PERFORMANCE CRITERIA** Performance criteria describe the required performance needed to demonstrate achievement of the element – they identify the standard for the element. Where bold/italicised text is used, further information or explanation is detailed in the required skills and knowledge and/or the range statement. Assessment of performance is to be consistent with the evidence guide.
1. Compile and evaluate risk management plan for the organisation	1.1 ***Methodologies for risk assessment*** are investigated
	1.2 Vulnerabilities and threats are identified
	1.3 Risk management plan for the organisation is sourced
	1.4 If a risk document doesn't exist, examine ***existing risk frameworks*** to determine templates that can be used to compile a risk management plan
	1.5 Risk management plan is developed with ***appropriate personnel***,
	1.6 ***Risk assessment process*** is defined
	1.7 ***Security recovery plan*** is developed
2. Compile risk categories for the security system	2.1 Information assets for the organisation are ranked and documented
	2.2 Risk analysis classification criteria is determined
	2.3 Using risk analysis processes within delegated authority and with appropriate personnel, analyse and qualify risks and threats
	2.4 Risk priorities for information assets are allocated
	2.5 Risk analysis outcomes for inclusion in the risk register and the risk management plan are documented
3. Implement appropriate security system	3.1 Effective ***controls to manage risk*** are devised documented and implemented

	controls for managing the risk	3.2	Emerging risks or threats are monitored with corrective measures planned documented and implemented in order to isolate the risk
4.	Monitor security system controls and processes	4.1	Controls that manage risks are reviewed and monitored for their continued effectiveness
		4.2	Regular risk review processes to maintain currency of risk plans are established
		4.3	Environment is regularly monitored to determine changed conditions
		4.4	If environment or a condition changes, implement and document appropriate changes to the risk controls and report changes to appropriate personnel
5.	Promote cybersecurity awareness in the organisation	5.1	Implications of the organisation’s security policy are defined and evaluated
		5.2	Strategies to promote security policy awareness in the organisation are planned and implemented
		5.3	Organisation’s security policy awareness strategies are evaluated for their effectiveness and if required, modified to increased their effectiveness

REQUIRED SKILLS AND KNOWLEDGE

This describes the essential skills and knowledge and their level, required for this unit

Required skills:

- Reading and interpreting cyber security related documentation such as organisation's risk management/assessment policies and procedures
- Working effectively as part of a team
- Identifying relevant risk assessment documents and procedures
- Assembling, participating in and coordinating a work team
- Problem solving within a team environment
- Evaluating the performance of a work team
- Contributing to the process of enhancing team performance
- Establishing risk assessment project
- Preparing technical documentation
- Making presentation to organisation's senior management and /or clients
- Performing risk assessment
- Working with others to identify relevant policy and procedures
- Working as part of a team to evaluate existing risk policy
- Implementing risk policy

Required knowledge:

- Methods of cyber security attacks
- Threats and vulnerabilities identity
- Risk assessment methodologies
- Tools and methods used to protect an organisation's data and privacy
- Cyber security risk management plans and policies
- Interpret risk assessment data, ISO 27001 standards for compliance
- Risk frameworks defined in ISO 31000
- Risk control selection, implementation and monitoring

Range Statement

The Range Statement relates to the unit of competency as a whole. It allows for different work environments and situations that may affect performance.

Methodologies for risk assessment includes but not limited to:

- Asset audit
- Pipeline model
- Attack trees
- Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE)
- Risk Management Guide for Information Technology Systems - National Institute of Standards and Technology (NIST)

Existing risk frameworks includes but not limited to:

- ISO 31000
- Samples of risk management templates for particular discipline

Appropriate personnel includes but not limited to:

- Cyber security paraprofessional employee
- Cyber security paraprofessional manager
- External consultants
- Relevant managers
- Business stakeholders

Risk assessment process includes but not limited to:

- Risk identification
- Risk analysis
- Risk assessment
- Risk evaluation
- Risk treatment
- Monitoring & review (of risks & control effectiveness)

Security recovery plan includes but not limited to:

- Disaster recovery plan
- Data backup strategies
- Data recovery
- Relocation

Controls to manage risk includes but not limited to:

- Isolate any incident effects
  - take system offline
  - block port
  - Implement backup strategy
- Evaluate and implement engineering controls to harden system from future incidents
- Administrative
  - Evaluate
  - Education
  - Training

EVIDENCE GUIDE

The evidence guide provides advice on assessment and must be read in conjunction with the Performance Criteria, Required Skills and Knowledge, the Range Statement and the Assessment section in Section B of the accreditation submission.

Critical aspects for assessment and evidence required to assess competency in this unit

To be considered competent in this unit assessors must be satisfied the candidate can demonstrate the achievement of all of the elements of the competency to the level defined by the associated performance criteria

Specifically they must be able to:

- Compile and evaluate a risk management plan for an organisation;
- Undertake cyber security risk assessment of an organisation's system;
- Implement appropriate security system controls for managing the risk;
- Monitor security system controls and processes;
- Promoting cybersecurity awareness in the organisation.

Context of and specific resources for assessment

Evidence should show competency working in a realistic environment and a variety of conditions. The candidate will have access to all tools, equipment, materials and documentation required. The candidate will be permitted to refer to any relevant workplace procedures, product and manufacturing specifications, codes, standards, manuals and reference materials.

This unit may be assessed on the job, off the job or a combination of both. Where assessment occurs off the job, an appropriate simulation must be used where the range of conditions reflects realistic workplace situations. The competencies covered by this unit would be demonstrated by an individual working alone or as part of a team. The assessment environment should not disadvantage the candidate.

Method of assessment

Evidence can be gathered in a variety of ways including:

- observation of processes and procedures
- oral and/or written questioning on required knowledge and skills
- testimony from supervisors, colleagues, clients and/or other appropriate persons
- inspection of the final product or outcome
- portfolio of documented evidence.

Where performance is not directly observed and/or is required to be demonstrated over a period of time and/or in a number of locations, any evidence should be authenticated by colleagues, supervisors, clients or other appropriate persons

VU22259 - Utilise design methodologies for security architecture

Unit Descriptor	The unit provides the knowledge and skills required by a cyber security paraprofessional to utilize tools and methodologies to design the security architecture for an organisation that addresses the business requirements, IT applications and end user expectations. The unit includes the implementation of a process for reviewing the existing security architecture and, conduct a security design audit and recommending improvements. No licensing or certification requirements apply to this unit at the time of accreditation.
Employability Skills	This unit contains employability skills.
Application of the Unit	This unit is applicable to individuals working as cyber security paraprofessionals responsible for the security infrastructure for the organisation
Pre requisite Unit/s	Nil

ELEMENT	**PERFORMANCE CRITERIA**	
Elements describe the essential outcomes of a unit of competency.	Performance criteria describe the required performance needed to demonstrate achievement of the element – they identify the standard for the element. Where bold/italicised text is used, further information or explanation is detailed in the required skills and knowledge and/or the range statement. Assessment of performance is to be consistent with the evidence guide.	
1. Evaluate current security architecture frameworks and methodologies	1.1	Existing ***security architecture frameworks and methodologies*** are identified and evaluated
	1.2	In consultation with ***appropriate personnel*** the outcomes of the standards and frameworks evaluation are examined for suitability and implementation
2. Collate network security design documentation	2.1	Existing network security logical diagram is reviewed and updated as required
	2.2	Existing network security physical diagram is reviewed and updated as required
3. Conduct a security assessment on the security devices and components	3.1	Network and perimeter security assessment is conducted
	3.2	Existing security infrastructure diagram for the organisation is sourced
	3.3	Network security tools to determine system vulnerabilities are evaluated and selected
	3.4	Template for security assessments including business impact is developed or sourced
	3.5	Risk and threat modelling for the organisation is developed
	3.6	Security metrics covering control objectives, warning thresholds and control thresholds is developed
4. Collate and review security policies for the organisation	4.1	Current ***security policy*** documents for the organisation are collated
	4.2	In consultation with appropriate personnel, security policies are reviewed and updated where appropriate

	4.3	***Change management process strategies*** to improve cyber security working practices within the organisation are developed
5. Evaluate methodologies for security architecture	5.1	In consultation with appropriate personnel a ***layered model of security architecture*** is evaluated and selected
	5.2	Issues around implementing a layered model of security architecture are prioritised
	5.3	***Different types of security technical designs*** are defined
	5.4	***Key development principles*** of a sound security architecture are investigated
	5.5	Process to address ***special security architecture challenges*** are investigated
6. Determine existing security architecture vulnerabilities	6.1	Tools and methodologies to enable security architecture vulnerabilities are collated, evaluated and selected
	6.2	An audit to detect vulnerabilities for the security architecture is performed
	6.3	In consultation with appropriate personnel, strategies to mitigate detected security architecture vulnerabilities are developed and deployed
7. Communicate design options for security architecture to the organisation	7.1	Engaging strategies for different ***stakeholder groups*** are developed
	7.2	***Communication strategies*** for different stakeholder groups are developed
	7.3	Reports to different stakeholder groups are written and presented utilising developed strategies
	7.3	***Tools to develop security architecture documentation*** are selected and sourced

REQUIRED SKILLS AND KNOWLEDGE

This describes the essential skills and knowledge and their level, required for this unit

Required skills:

- Articulating relevant issues encountered in the work environment
- Reading and accurately interpreting documents and reports
- Operating a personal computer
- Interpreting network diagrams
- Evaluating current security design frameworks
- Gathering relevant resources
- Interpreting key aspects from security design frameworks with relevance to the organisation
- Assembling, participating in and coordinating a work team
- Problem solving within a team environment
- Evaluating the performance of a work team
- Contributing to the process of enhancing team performance
- Installing and using software packages
- Connecting cyber security equipment and networked devices
- Preparing technical documentation
- Identifying and collating relevant documents
- Presenting security designs to various stakeholder groups
- Writing clear security architecture documentation
- Evaluating effectiveness of network security devices
- Coordinating different user groups
- Comprehending the different user groups perspectives of security architecture:
  - Business
  - Management
  - User
  - IT

Required knowledge:

- Security architecture designs to suit various stakeholder requirements
- Security architecture documentation
- Security network devices
- Business requirements of the organisation
- Communication strategies
- Security architecture frameworks and tools such as:
  - Sherwood Applied Business Security Architecture **(**SASBA)
  - Control Objectives for Information and Related Technologies (COBIT)
  - Information Technology Infrastructure Library (ITIL)
  - National Institute of Standards and Technology (NIST) Cybersecurity framework
  - Enterprise Architecture Framework - Zachman Institute for Framework Advancement
- SABSA Framework for security architecture design

Range Statement

The Range Statement relates to the unit of competency as a whole. It allows for different work environments and situations that may affect performance.

Security architecture frameworks and methodologies includes but not limited to:

- The open group architecture framework **(**TOGAF**)**
- Enterprise information security architecture (EISA)
- Sherwood applied business security architecture (SABSA)
- Information technology infrastructure library (ITIL)
- Control objectives for information and related technologies (COBIT)
- National Institute of Standards and Technology (NIST) Cybersecurity framework
- Enterprise Architecture Framework - Zachman Institute for Framework Advancement

Appropriate personnel includes but not limited to:

- Cyber security paraprofessional
- Cyber security manager
- External consultants
- Relevant managers
- Business stakeholders

Security policy includes but not limited to:

- Breech consequences
- Policy enforcement
- User Access
- Security profiles
- Passwords
- E-mail use
- Internet use
- Anti-Virus requirements
- Back-up and recovery processes
- Intrusion detection processes and procedures
- Remote Access

Change management process strategies includes but not limited to:

- Internal training
- Random work place audits
- Incentives for work place cyber security change practices
- Weekly staff security challenges

Layered model of security architecture includes but not limited to:

- Contextual (Business context)
- Conceptual (Security strategy)
- Logical (High level security design)
- Physical (Part of detailed design)
- Component (Part of detailed design)
- Operational design
- All the above are based on the SABSA

Different types of security technical designs includes but not limited to:

- Network security design
- Application security design
- Security monitoring design
- Identity and access management design

Key development principles includes but not limited to:

- Value driven
- Structure
- Traceable (from business objectives to detailed design)
- Metrics based

Special security architecture challenges includes but not limited to:

- Security which addresss critical infrastructure
- Security of Internet of Things (IoT) devices
- Security for bring your own devices (BYOD)
- Security of cloud based solutions

Stakeholder groups includes but not limited to:

- Executives
- Technical designers
- Users

Communication strategies includes but not limited to:

- Diagrammatic tools:
    - Unified Modeling Language (UML)
    - State machines
    - Swimlane diagrams
    - Entity relationship diagrams
- Communicating language and methods to:
    - Managers
    - Users
    - External consultants
    - Peers

Tools to develop security architecture documentation includes but not limited to:

- Archimate
- Visio
- Gliffy

EVIDENCE GUIDE

The evidence guide provides advice on assessment and must be read in conjunction with the Performance Criteria, Required Skills and Knowledge, the Range Statement and the Assessment section in Section B of the accreditation submission.

Critical aspects for assessment and evidence required to assess competency in this unit

To be considered competent in this unit assessors must be satisfied the candidate can demonstrate the achievement of all of the elements of the competency to the level defined by the associated performance criteria

Specifically they must be able to:

- Evaluate current security architecture frameworks and methodologies;
- Collate network security design documentation;
- Conduct a security assessment on the existing security devices and components;
- Utilise a design methodology for security architecture;
- Utilise tools and methodologies to determine security architecture vulnerabilities;
- Develop strategies to mitigate security architecture vulnerabilities;
- Communicate security architecture designs to the organisation.

Context of and specific resources for assessment

Evidence should show competency working in a realistic environment and a variety of conditions. The candidate will have access to all tools, equipment, materials and documentation required. The candidate will be permitted to refer to any relevant workplace procedures, product and manufacturing specifications, codes, standards, manuals and reference materials.

This unit may be assessed on the job, off the job or a combination of both. Where assessment occurs off the job, an appropriate simulation must be used where the range of conditions reflects realistic workplace situations. The competencies covered by this unit would be demonstrated by an individual working alone or as part of a team. The assessment environment should not disadvantage the candidate.

Method of assessment

Evidence can be gathered in a variety of ways including:

- observation of processes and procedures
- oral and/or written questioning on required knowledge and skills
- testimony from supervisors, colleagues, clients and/or other appropriate persons
- inspection of the final product or outcome
- portfolio of documented evidence.

Where performance is not directly observed and/or is required to be demonstrated over a period of time and/or in a number of locations, any evidence should be authenticated by colleagues, supervisors, clients or other appropriate persons.

Appendix 1 – Knowledge/Skills and Units of Competency Matrix

	BSBWOR502 Lead and manage team effectiveness	ICTNWK525 Configure an enterprise virtual computing environment	VU22240 Communicate cyber security incidents within the organisation	VU22241 Interpret and utilise key security frameworks, policies and procedures for the organisation	VU22242 Assess and secure cloud services	VU22243 Develop software skills for the cyber security practitioner	VU22244 Implement best practices for identity management	VU22245 Plan andImplement a cyber security project	VU22246 Evaluate an organisation’ s compliance with relevant cyber security standards and law
Knowledge	**Core Units**								
Basic understanding of threats and their implications			√	√	√	√	√	√	√
Team work techniques			√				√	√	√
Difference between threats and risks			√	√	√	√	√	√	√
Network features and functions					√		√	√	
Operating systems						√	√	√	
Risk assessment				√	√		√	√	
Security frameworks and standards				√				√	√
Cyber security law				√				√	√
Monitoring and responding to incidents			√					√	
Virtual security systems								√	
Algorithms and programming						√			
Fundamentals of computer hardware								√	
Authentication mechanisms						√	√	√	
Penetration testing								√	
Defence In-depth and Kill Chain security concepts					√		√	√	
Security frameworks and standards				√				√	√
Security capabilities and infrastructure					√	√	√	√	
Professional ethics	√	√	√	√	√	√	√	√	√
Skills	**Core Units**								
Working effectively in teams			√	√	√		√	√	√
Installing and using software packages						√		√	
Following professional ethics			√	√	√	√	√	√	√
Applying analytical skills								√	√
Displaying sound organisational skills			√	√	√			√	√
Displaying good interpersonal skills			√	√	√	√	√	√	√
Interpreting technical specifications			√	√	√	√	√	√	√
Solving problems in teams			√	√	√	√	√	√	√
Evaluating team performance			√	√	√	√	√	√	√
Displaying effective communication skills			√	√	√	√	√	√	√
Preparing technical documents			√	√	√		√	√	√

	BSBWOR502 Lead and manage team effectiveness	ICTNWK525 Configure an enterprise virtual computing environment	VU22240 Communicate cyber security incidents within the organisation	VU22241 Interpret and utilise key security frameworks, policies and procedures for the organisation	VU22242 Assess and secure cloud services	VU22243 Develop software skills for the cyber security practitioner	VU22244 Implement best practices for identity management	VU22245 Plan andImplement a cyber security project	VU22246 Evaluate an organisation’ s compliance with relevant cyber security standards and law
Making presentations to clients			√	√	√		√	√	√
Working independently			√	√	√	√	√	√	√

	VU22247 Acquire digital forensic data from workstations	VU22248 Acquire digital forensic data from mobile devices	VU22249 Perform a security risk assessment for an organisation	ICTNWK607 Design and implement wireless network security	ICTNWK531 Configure an internet gateway	ICTSAS505 Review and update disaster recovery and contingency plans	ICTNWK502Implement secure encryption technologies	ICTNWK503 Install and maintain valid authentication processes
Knowledge	**General Elective Stream**							
Basic understanding of threats and their implications	√	√	√	√	√	√		
Team work techniques			√		√	√		
Difference between threats and risks	√	√	√	√		√		
Network features and functions			√	√	√			
Operating systems	√	√	√	√				
Risk assessment	√	√	√	√		√		
Security frameworks and standards						√		
Cyber security law	√	√						
Monitoring and responding to incidents						√		
Virtual security systems								
Algorithms and programming							√	
Fundamentals of computer hardware	√	√						
Authentication mechanisms				√			√	√
Penetration testing								
Defence In-depth and Kill Chain security concepts						√		
Security frameworks and standards			√	√		√		
Security capabilities and infrastructure			√	√		√		
Professional ethics	√	√	√	√	√	√	√	√
Skills	**General Elective Stream**							
Working effectively in teams			√	√		√		
Installing and using software packages	√	√			√			
Following professional ethics	√	√	√	√	√	√	√	√
Applying analytical skills	√	√	√	√		√	√	
Displaying sound organisational skills	√	√	√	√	√	√	√	√
Displaying good interpersonal skills	√	√	√	√	√	√	√	√
Interpreting technical specifications	√	√	√	√	√	√	√	√
Solving problems in teams	√	√	√	√		√		
Evaluating team performance	√	√	√	√		√		
Displaying effective communication skills	√	√	√	√		√		

	VU22247 Acquire digital forensic data from workstations	VU22248 Acquire digital forensic data from mobile devices	VU22249 Perform a security risk assessment for an organisation	ICTNWK607 Design and implement wireless network security	ICTNWK531 Configure an internet gateway	ICTSAS505 Review and update disaster recovery and contingency plans	ICTNWK502Implement secure encryption technologies	ICTNWK503 Install and maintain valid authentication processes
Preparing technical documents	√	√	√	√	√	√		
Making presentations to clients	√	√	√	√		√		
Working independently	√	√	√	√	√		√	√

	VU22250 Respond to cyber security incidents	VU22251 Gather, analyse and interpreti threat data	VU22252 Implement cyber security operations	ICTSAS501 Develop, implement and evaluate an incident response plan	ICTNWK513 Manage system security
Knowledge	**Intrusion Analyst Stream**				
Basic understanding of threats and their implications	√	√	√	√	√
Team work techniques	√	√	√	√	√
Difference between threats and risks	√	√	√	√	
Network features and functions			√		√
Operating systems			√		
Risk assessment	√	√	√	√	√
Security frameworks and standards	√		√	√	√
Cyber security law	√				√
Monitoring and responding to incidents	√	√	√	√	√
Virtual security systems					
Algorithms and programming					
Fundamentals of computer hardware					√
Authentication mechanisms					√
Penetration testing	√		√		√
Defence In-depth and Kill Chain security concepts	√	√	√	√	√
Security frameworks and standards	√		√		√
Security capabilities and infrastructure	√		√	√	√
Professional ethics	√	√	√	√	√
Working effectively in teams	√	√	√	√	√

	VU22250 Respond to cyber security incidents	VU22251 Gather, analyse and interpreti threat data	VU22252 Implement cyber security operations	ICTSAS501 Develop, implement and evaluate an incident response plan	ICTNWK513 Manage system security
Installing and using software packages					√
Following professional ethics	√	√	√	√	√
Applying analytical skills	√	√	√	√	√
Displaying sound organisational skills	√	√	√	√	√
Displaying good interpersonal skills	√	√	√	√	√
Interpreting technical specifications	√	√	√	√	√
Solving problems in teams	√	√	√	√	√
Evaluating team performance	√	√	√	√	√
Displaying effective communication skills	√	√	√	√	√
Preparing technical documents	√	√	√	√	√
Making presentations to clients	√		√	√	√
Working independently	√	√	√	√	√

	VU22253 Undertake penetration testing of the security infrastructure for an organisation	VU22254 Undertake advanced penetration testing for web site vulnerabilities	VU22255 Evaluate threats and vulnerabilities of Internet of Things (IOT) devices
Knowledge	**Penetration Testing Stream**		
Basic understanding of threats and their implications	√	√	√
Team work techniques			
Difference between threats and risks	√	√	√
Network features and functions	√	√	√
Operating systems			
Risk assessment	√	√	√
Security frameworks and standards	√	√	√
Cyber security law			
Monitoring and responding to incidents	√	√	
Virtual security systems			

	VU22253 Undertake penetration testing of the security infrastructure for an organisation	VU22254 Undertake advanced penetration testing for web site vulnerabilities	VU22255 Evaluate threats and vulnerabilities of Internet of Things (IOT) devices
Algorithms and programming			
Fundamentals of computer hardware			√
Authentication mechanisms			
Penetration testing	√	√	√
Defence In-depth and Kill Chain security concepts	√	√	√
Security frameworks and standards	√	√	√
Security capabilities and infrastructure	√	√	√
Professional ethics	√	√	√
Skills	**Penetration Testing Stream**		
Working effectively in teams			
Installing and using software packages	√	√	√
Following professional ethics	√	√	√
Applying analytical skills	√	√	√
Displaying sound organisational skills	√	√	√
Displaying good interpersonal skills	√	√	√
Interpreting technical specifications	√	√	√
Solving problems in teams			
Evaluating team performance			
Displaying effective communication skills	√	√	√
Preparing technical documents	√	√	√
Making presentations to clients	√	√	√
Working independently	√	√	√

	VU22256 Protect critical infrastructure for an organisation	VU22257 Configure security devices for an organisation	VU22259 Utilise design methodologies for security architecture	ICTNWK509 Design and implement a security perimeter for ICT networks	ICTTEN811 Evaluate and apply network security
Knowledge	**Security Engineer Stream**				
Basic understanding of threats and their implications	√	√	√	√	√
Team work techniques	√		√	√	√
Difference between threats and risks	√	√	√	√	√
Network features and functions	√	√	√	√	√
Operating systems	√				
Risk assessment	√	√	√	√	√
Security frameworks and standards			√		
Cyber security law			√		
Monitoring and responding to incidents					
Virtual security systems					
Algorithms and programming					
Fundamentals of computer hardware	√			√	√
Authentication mechanisms					
Penetration testing					
Defence In-depth and Kill Chain security concepts	√	√	√	√	√
Security frameworks and standards					
Security capabilities and infrastructure	√	√	√	√	√
Professional ethics	√	√	√	√	√
Skills	**Security Engineer Stream**				
Working effectively in teams			√		√
Installing and using software packages					
Following professional ethics	√	√	√	√	√
Applying analytical skills					
Displaying sound organisational skills	√	√	√	√	√
Displaying good interpersonal skills	√	√	√	√	√
Interpreting technical specifications	√	√	√	√	√
Solving problems in teams			√		
Evaluating team performance			√		
Displaying effective communication skills	√	√	√	√	√
Preparing technical documents	√	√	√	√	√

	VU22256 Protect critical infrastructure for an organisation	VU22257 Configure security devices for an organisation	VU22259 Utilise design methodologies for security architecture	ICTNWK509 Design and implement a security perimeter for ICT networks	ICTTEN811 Evaluate and apply network security
Making presentations to clients	√	√	√	√	√
Working independently	√	√	√	√	√