22603VIC
Certificate IV in Cyber Security

Version 1.1 September 2023

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

Accredited for the period: 1 January 2023 to 31 December 2027

VICTORIA State Government | Jobs, Skills, Industry and Regions

Version History:		Date
Version 1.1	Department of Education and Training (DET) details and contact information updated with Department of Jobs, Skills Industries and Regions (DJSIR) details in Section A	September 2023

Table of contents

Section A: Applicant and course classification information 1
1. Person in respect of whom the course is being accredited 1
2. Address 1
3. Type of submission 1
4. Copyright acknowledgement 1
5. Licensing and franchise 2
6. Course accrediting body 2
7. AVETMISS information 2
8. Period of accreditation 3
Section B: Course information 5
1 Nomenclature 4
1.1 Name of the qualification 4
1.2 Nominal duration of the course 4
2 Vocational or educational outcomes of the course 4
2.1 Outome(s) of the course 4
2.2 Course description 4
3 Development of the course 4
3.1 Industry, education, legislative, enterprise or community needs 5
3.2 Review for re-accreditation 7
4 Course outcomes 10
4.1 Qualification level 10
4.2 Foundation skills 11
4.3 Recognition given to the course 11
4.4 Licensing/regulatory requirements 11
5 Course rules 11
5.1 Course structure 11
5.2 Entry requirements 14
6 Assessment 14
6.1 Assessment strategy 14
6.2 Assessor competencies 15
7 Delivery 15
7.1 Delivery modes 15
7.2 Resources 16
8 Pathways and articulation 16
9 Ongoing monitoring and evaluation 17

Table 1 Summary of the Foundation Skills for the Certificate IV in Cyber Security 17
Section C—Units of competency 20

Section A: Applicant and course classification information

1. Person in respect of whom the course is being accredited	Copyright of this material is reserved to the Crown in the right of the State of Victoria on behalf of the Department of Jobs, Skills, Industries and Regions (DJSIR) Victoria. © State of Victoria (DJSIR) 2022
2. Address	*Deputy CEO* *Victorian Skills Authority* *Department of Jobs, Skills, Industries and Regions (DJSIR)* *GPO Box 4509* *MELBOURNE VIC 3001* ***Organisational contact*** *Manager, Training and Learning Products Unit* *Engagement Branch* *Victorian Skills Authority* *Department of Jobs, Skills, Industries and Regions (DJSIR)* *Email:* course.enquiry@djsir.vic.gov.au **Day-to-day contact:** Curriculum Maintenance Manager - Engineering Industries, Box Hill Institute Private Bag 2014 Box Hill, Victoria 3128 Email: cmmei@boxhill.edu.au
3. Type of submission	This submission is for re-accreditation of: **22334VIC Certificate IV in Cyber Security.**
4. Copyright acknowledgement	The following units of competency: BSBINS401 – Analyse and present research information BSBWHS309 – Contribute effectively to WHS communication and consultation processes have been imported from: **BSB – Business Services Training Package** administered by the Commonwealth of Australia. © Commonwealth of Australia The following units of competency: ICTCLD301 - Evaluate characteristics of cloud computing solutions and services ICTCLD401 - Configure cloud services ICTICT426 – Identify and evaluate emerging technologies and practices ICTICT443 – Work collaboratively in the ICT industry

	ICTNWK435 – Create secure virtual private networks ICTNWK422 – Install and manage servers ICTNWK537 – Implement secure encryption technologies ICTNWK538 – Install and maintain valid authentication processes ICTNWK544 – Design and implement a security perimeter for ICT networks ICTNWK546 – Manage network security ICTPRG434 – Automate processes ICTPRG435 – Write script for software applications ICTSAS440 – Monitor and administer security of ICT systems ICTSAS526 – Review and update disaster recovery and contingency plans have been imported from: **ICT - Information and Communication 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 (DJSIR) 2022. This work is licensed under a Creative Commons Attribution 4.0 International licence (see *Creative Commons* for more information). You are free to use, copy and distribute to anyone in its original form if you attribute the State of Victoria (DJSIR) as the author and you licence any derivative work you make available under the same licence. Requests for other use should be addresses to: Executive Director Higher Education and Workforce Skills and Employment Department of Jobs, Skills, Industries and Regions (DJSIR) Email: course.enquiry@djsir.vic.gov.au Copies of this publication can be downloaded free of charge from the Victorian government website.
6. Course accrediting body	Victorian Registration and Qualifications Authority (VRQA)
7. AVETMISS information	***ANZSCO code:***

	Australian and New Zealand Standard Classification of Occupations 313199 ICT Support Technicians ***ASCED Code*** *Field of Education* 0299 Other Information Technology ***National course code*** 22603VIC
8. Period of accreditation	1 January 2023 to 31 December 2027

Section B: Course information

1 Nomenclature	
1.1 Name of the qualification	*Standard 4.1 and 5.8 AQTF 2021 Standards for Accredited Courses* Certificate IV in Cyber Security
1.2 Nominal duration of the course	655 – 970 hours
2 Vocational or educational outcomes of the course	
2.1 Outome(s) of the course	*Standard 5.1 AQTF 2021 Standards for Accredited Courses* The vocational/industry outcomes of the course are the ability to: • respond to and monitor cyber security events in an organisation • use a range of tools and procedures to mitigate cyber security threats • protect an organisation from insider security breaches • develop systems to minimise network vulnerabilities and risks • recognise implications using cloud based services • work effectively as a member of a cyber security team.
2.2 Course description	*Standard 5.1 AQTF 2021 Standards for Accredited Courses* The Certificate IV in Cyber Security is a technician level course. It provides participants with knowledge and a range of technical skills to enable them to seek employment as a cyber security technician in a range of organisations and government bodies.
3 Development of the course	

3.1 Industry, education, legislative, enterprise or community needs	*Standards 4.1, 5.1, 5.2, 5.3 and 5.4 AQTF 2021 Standards for Accredited Courses* The Austrailian Cyber Security Centre (ACSC) Annual Cyber Threat Report 2020-2021 - Executive Summary (in part) states: “Over the 2020–21 financial year, the ACSC received over 67,500 cybercrime reports, an increase of nearly 13 per cent from the previous financial year. The increase in volume of cybercrime reporting equates to one report of a cyber attack every 8 minutes compared to one every 10 minutes last financial year. A higher proportion of cyber security incidents this financial year was categorised by the ACSC as ‘substantial’ in impact. This change is due in part to an increased reporting of attacks by cybercriminals on larger organisations and the observed impact of these attacks on the victims, including several cases of data theft and/or services rendered offline. The increasing frequency of cybercriminal activity is compounded by the increased complexity and sophistication of their operations. The accessibility of cybercrime services – such as ransomware-as-a-service (RaaS) – via the dark web increasingly opens the market to a growing number of malicious actors without significant technical expertise and without significant financial investment. No sector of the Australian economy was immune from the impacts of cybercrime and other malicious cyber activity. Government agencies at all levels, large organisations, critical infrastructure providers, small to medium enterprises, families and individuals were all targeted over the reporting period – predominantly by criminals or state actors”. As a consequence of the increase in incidents of cyber interference as indicated in the ACSC 20/21 annual report, the demand for cyber security services is ongoing. The Certificate IV in Cyber Security was initially developed to address the cyber security skill shortage in Victoria. However, the course has also been taken up by RTOs in other States and the ACT. The increasing sophistication of cyber threats and the broadening landscape that requires security oversight such as mobile devices, cloud based services and the Internet of Things has also expanded the need for people with the knowledge and skills to identify, analyse, manage and prevent cyber interference and attacks. Enrolment figures from 2019 to 2022 provided by the Department of Education and Training (DET) for Victoria are: 2019 = 1580 2020 = 2954 2021 = 3404

2022 = 1994 (as at 03/22)

Currently, thirteen (13) public RTOs and two (2) private RTOs have the current course on their scope of registration. The course is also delivered in ACT, NSW, QLD, SA & WA.

As part of the reaccreditation process the current course content has been comprehensively reviewed and updated under the guidance of a well-qualified Course Steering Committee (CSC) consisting of the following persons:

Name:	Organisation:
Grant McKechnie (Chairperson)	Chief Information Security Officer, Endeavour Group
Jamie Rossato (Deputy Chairperson)	Information Security Director Lion Pty Limited
Malcolm Shore	Offensive Security Team Offensive Security (NZ)
Matt Carling	National Cybersecurity Advisor Cisco Systems Inc.
Damien Manuel	Chief Executive Officer Australian Information Security Association (AISA)
Joe D'Amico	Manager – Digital Skills and Concepts Chisholm Institute
Dominic Schipano	National Executive Officer Communications and Information Technology Training Ltd (CITT)
Deepak Gami	Senior Manager - Security Assurance NBN - Security Group
Jan Newmarch	Adjunct Professor, University of Canberra
Beth Worrall	Social Value program Director, Public Sector Microsoft Australia
Stephen Besford	Cyber Security Course Adviser (Technical content editor - course units)

In attendance:

George Adda (Project manager)	Supervising Executive Officer, CMM – Engineering Industries

	Box Hill Institute
Steven Bryant (Minutes)	Project Specialist CMM – Engineering Industries Box Hill Institute
Trevor Lange (Accreditation adviser/writer)	Snr. Project Officer, CMM – Engineering Industries Box Hill Institute
Jo Cave	Head of Cyber and Digital Transformation Programs Victoria University Polytechnic
Geethani Nair	Director, Digital Skills & Concepts

This course:

- does not duplicate, by title or coverage, the outcomes of an endorsed training package qualification or skill set
- is not a subset of a single training package qualification that could be recognised through one or more statements of attainment or a skill set
- does not include units of competency additional to those in a training package qualification that could be recognised through statements of attainment in addition to the qualification
- does not comprise units that duplicate units of competency of a training package qualification.

3.2 Review for re-accreditation

Standards 5.1, 5.2, 5.3 and 5.4 AQTF 2021 Standards for Accredited Courses

For the purpose of reaccreditation each enterprise unit in this course has been reviewed by a subject matter expert (SME) to ensure its' currency. In addition, four new enterprise units have been added to the course - three to the elective bank and one unit: VU23223 *Apply cyber security legislation, privacy and ethical practises* in the core component replacing unit ICTICT418.

RTO feedback indicated a preference for greater flexibility in unit choice but retaining the total number of units. This was achieved by reducing the core component from 10 to 8 units and increasing the required number of electives from 6 to 8 units.

The course 22603VIC Certificate IV in Cyber Security supersedes and is deemed not equivalent to 22334VIC Certificate IV in Cyber Security due the changes made to the core component of the course.

Transition Table				
22334VIC Certificate IV in Cyber Security		**22603VIC Certificate IV in Cyber Security**		**Relationship**
VU21988	Utilise basic network concepts and protocols required in cyber security	VU23213	Utilise basic network concepts and protocols required in cyber security	Equivalent
VU21989	Test concepts and procedures for cyber security	VU23215	Test concepts and procedures for cyber security	Equivalent
VU21990	Recognise the need for cyber security in an organisation	VU23217	Recognise the need for cyber security in an organisation	Equivalent
VU21991	Implement network security infrastructure for an organisation	VU23218	Implement network security infrastructure for an organisation	Equivalent
VU21992	Develop a cyber security industry project	VU23220	Develop and carry out a cyber security industry project	Equivalent
VU21993	Secure a networked personal computer	VU23214	Configure and secure networked end points	Equivalent
VU21994	Perform basic cyber security data analysis	VU23216	Perform basic cyber security data analysis	Equivalent
VU21995	Manage the security infrastructure for the organisation	VU23219	Manage the security infrastructure for an organisation	Equivalent
VU21996	Evaluate and test an incident response plan for an enterprise	VU23221	Evaluate and test an incident response plan for an enterprise	Equivalent
VU21997	Expose website security vulnerabilities	VU23222	Expose website security vulnerabilities	Equivalent
BSBWHS401	Implement and monitor WHS policies, procedures and programs to meet legislative requirements			Deleted
		BSBWHS309	Contribute effectively to WHS communication and	Newly imported unit

22334VIC Certificate IV in Cyber Security		22603VIC Certificate IV in Cyber Security		Relationship
			consultation processes	
BSBRES401	Analyse and present research information	BSBINS401	Analyse and present research information	Equivalent
ICTNWK401	Install and manage a server	ICTNWK422	Install and manage servers	Equivalent
ICTNWK416	Build security into virtual private networks	ICTNWK435	Create secure virtual private networks	Equivalent
ICTNWK502	Implement secure encryption technologies	ICTNWK537	Implement secure encryption technologies	Equivalent
ICTNWK503	Install and maintain valid authentication processes	ICTNWK538	Install and maintain valid authentication processes	Equivalent
ICTNWK509	Design and implement a security perimeter for ICT networks	ICTNWK544	Design and implement a security perimeter for ICT networks	Equivalent
ICTNWK511	Manage network security	ICTNWK546	Manage network security	Equivalent
ICTPRG405	Automate processes	ICTPRG434	Automate processes	Not equivalent
ICTPRG407	Write script for software applications	ICTPRG435	Write script for software applications	Equivalent
ICTSAS418	Monitor and administer security of an ICT system	ICTSAS440	Monitor and administer security of ICT systems	Equivalent
ICTSAS505	Review and update disaster recovery and contingency plans	ICTSAS526	Review and update disaster recovery and contingency plans	Equivalent
ICTICT418	Contribute to copyright, ethics and privacy in an ICT environment			Deleted
ICTNWK531	Configure an internet gateway			Deleted
ICTSAS409	Manage risk involving ICT systems and technology			Deleted

22334VIC Certificate IV in Cyber Security		22603VIC Certificate IV in Cyber Security		Relationship
RIICOM301D	Communicate information			Deleted
		ICTCLD301	Evaluate characteristics of cloud computing solutions and services	New imported unit
		ICTCLD 401	Configure cloud services	New imported unit
		ICTICT426	Identify and evaluate emerging technologies and practices	New imported unit
		ICTICT443	Work collaboratively in the ICT industry	New imported unit
		VU23223	Apply cyber security legislation, privacy and ethical practises	New unit
		VU23224	Identify the implications of cloud based security systems	New unit
		VU23225	Investigate Windows security features	New unit
		VU23226	Test concepts and procedures for cyber exploitation	New unit

4 Course outcomes

4.1 Qualification level

Standards 5.5 AQTF 2021 Standards for Accredited Courses

This course is aligned with Level 4 of the Australian Qualifications Framework (AQF) in that graduates will have:

- cognitive skills to identify and analyse risk of security attacks and recommend appropriate strategies to mitigate the attacks
- cognitive, technical and communication skills to implement and use a range of tools and procedures to mitigate cyber security threats in a

	wide variety of contexts • specialist technical skills to apply solutions to a defined range of unpredictable problems by methodically verifying compliance of all aspects associated with network security • broad knowledge base of relevant Australian standards, codes of practice and industry guidelines on network security • ability to evaluate information from a variety of sources and analyse the data gathered on the network security to assess compliance • ability to take responsibility for own outputs and contributions as part of a team to maintaining an organisation's cyber security system and incident response plan. The **Volume of Learning** for the Certificate IV in Cyber Security is typically 0.5 - 1 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 Foundation skills	*Standard 5.6 AQTF 2021 Standards for Accredited Courses* Refer Table 1 at the end of this section. Foundation skills applicable to the units are detailed in each unit of competency.
4.3 Recognition given to the course (if applicable)	*Standard 5.7 AQTF 2021 Standards for Accredited Courses* Nil
4.4 Licensing/regulatory requirements (if applicable)	*Standard 5.7 AQTF 2021 Standards for Accredited Courses* Not applicable
5 Course rules	
Standards 5.8 and 5.9 AQTF 2021 Standards for Accredited courses **5.1 Course structure** To achieve the qualification *22603VIC - Certificate IV in Cyber Security* the learner must successfully complete a total of sixteen (16) units comprising: – eight (8) core units – eight (8) elective units selected from the elective list below. Where the full course is not completed, a VET Statement of Attainment will be issued for each unit successfully completed.	

Unit of competency code	Field of Education code (six-digit)	Unit of competency title	Pre-requisite	Nominal hours
Core units:				
BSBWHS309		Contribute effectively to WHS communication and consultation processes	Nil	30
BSBINS401		Analyse and present research information	Nil	40
ICTICT443		Work collaboratively in the ICT industry	Nil	30
VU23223	029901	Apply cyber security legislation, privacy and ethical practices	Nil	30
VU23213	029901	Utilise basic network concepts and protocols required in cyber security	Nil	80
VU23215	029901	Test concepts and procedures for cyber security	Nil	60
VU23217	029901	Recognise the need for cyber security in an organisation	Nil	60
VU23220	029901	Develop and carry out a cyber security industry project	VU23213 VU23215	100
			Total core unit hours =	**430**
Elective units:				
VU23214	029901	Configure and secure networked end points	Nil	60
VU23216	029901	Perform basic cyber security data analysis	Nil	20
VU23218	029901	Implement network security infrastructure for an organisation	VU23213	80
VU23219	029901	Manage the security infrastructure for an organisation	Nil	80
VU23221	029901	Evaluate and test an incident response plan for an enterprise	Nil	40
VU23222	029901	Expose website security vulnerabilities	Nil	40

VU23224	029901	Identify the implications of cloud based security systems	Nil	40
ICTCLD301		Evaluate characteristics of cloud computing solutions and services	Nil	40
ICTCLD401		Configure cloud services	Nil	60
VU23225	029901	Investigate Windows security features	Nil	40
VU23226	029901	Test concepts and procedures for cyber exploitation	VU23215	60
ICTICT426		Identify and evaluate emerging technologies and practices	Nil	60
ICTNWK435		Create secure virtual private networks	Nil	20
ICTNWK422		Install and manage servers	Nil	40
ICTNWK537		Implement secure encryption technologies	Nil	20
ICTNWK538	029901	Install and maintain valid authentication processes	Nil	25
ICTNWK544	029901	Design and implement a security perimeter for ICT networks	Nil	60
ICTNWK546	029901	Manage network security	Nil	80
ICTPRG434	020103	Automate processes	Nil	40
ICTPRG435	020103	Write script for software applications	Nil	40
ICTSAS440	029901	Monitor and administer security of ICT systems	Nil	30
ICTSAS526	029999	Review and update disaster recovery and contingency plans	Nil	30
Range totals for elective units =				**225 - 540**
Totals nominal hour range for course (Core and Elective units) =				**655 - 970**

5.2 Entry requirements	*Standard 5.11 AQTF 2021 Standards for Accredited Courses* There are no essential entry requirements for the *22603VIC Certificate IV in Cyber Security*. Applicants are best equipped to achieve the course outcomes if they have as a minimum, language, literacy and numeracy skills that are equivalent to Level 3 of the Australian Core Skill Framework. Details can be found on website: *http://www.acsf.deewr.gov.au* Applicants with language, literacy and numeracy skills at levels lower than those recommended may require additional support to successfully undertake this course.
6 Assessment	
6.1 Assessment strategy	*Standard 5.12 AQTF 2021 Standards for Accredited Courses* All assessment, including Recognition of Prior Learning (RPL), must be compliant with the requirements of: • Standard 1 of the AQTF: Essential Conditions and Standards for Initial/Continuing Registration and Guidelines 4.1 and 4.2 of the VRQA Guidelines for VET Providers, *or* • the Standards for Registered Training Organisations 2015 (SRTOs), *or* • the relevant standards and Guidelines for RTOs 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; • assist assessors to interpret evidence consistently; • recognise prior learning. • be equitable to all groups of learners. Assessment methods may include: • oral and/or written questioning • inspection of final process outcomes • portfolio of documentary workplace evidence • practical demonstration of required physical tasks • investigative research and case study analysis. Questioning techniques should not require language and literacy skills beyond the level recommended for each unit of competency. 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. Assessment of imported units must reflect the Assessment Requirements for the relevant training package
6.2 Assessor competencies	*Standard 5.12 AQTF 2021 Standards for Accredited Courses* Assessment must be undertaken by a person or persons in accordance with: • Standard 1.4 of the AQTF: Essential Conditions and Standards for Initial/Continuing Registration and Guidelines 3 of the VRQA Guidelines for VET Providers, *or* • the Standards for Registered Training Organisations 2015 (SRTOs), *or* • the relevant standards and Guidelines for RTOs at the time of assessment. Units of competency imported from training packages must reflect the requirements for assessors specified in that training package.
7 Delivery	
7.1 Delivery modes	*Standard 5.12, 5.13 and 5.14 AQTF 2021 Standards for Accredited Courses* This course may be delivered either full-time or part-time or a combination of full-time and part-time.

	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 unit therefore, some integration of delivery may be appropriate.
7.2 *Resources*	*Standard 5.12, 5.13 and 5.14 AQTF 2021 Standards for Accredited Courses* Workplace and/or training facilities and equipment including: • access to computer hardware and software • access to the internet • access to exploitation testing and enumeration tools • access to virtual lab environment including Virtual Windows machines and Security Information Event Management (SIEM) tool • access to different cloud based environments • access to logging, alerting and monitoring tool • access to relevant texts and sample organisational cyber security policies and procedures Training must be undertaken by a person or persons in accordance with: • Standard 1.4 of the AQTF: Essential Conditions and Standards for Initial/Continuing Registration and Guideline 3 of the VRQA Guidelines for VET Providers, *or* • the Standards for Registered Training Organisations 2015 (SRTOs), *or* • the relevant standards and Guidelines for RTOs at the time of assessment. Units of competency imported from training packages must reflect the requirements for resources/trainers specified in that training package.
8 Pathways and articulation	
	Standard 5.10 AQTF 2021 Standards for Accredited Courses There are no formal arrangements for articulation to other accredited courses or higher education qualifications. However, graduates of this course meet the entry

	requirements for entry into Advanced Diploma of Cyber Security Applicants for this course will also gain a credit/s for any common training package unit/s successfully completed from previous training. Likewise, graduates who successfully complete any training package unit/s in this course will be able to gain credit into other qualifications containing these units in future studies." When arranging articulation providers should refer to the: *AQF Second Edition 2013 Pathways Policy*
9 Ongoing monitoring and evaluation	
	Standard 5.15 AQTF 2021 Standards for Accredited Courses *22603VIC - Certificate IV in Cyber Security* will be monitored and maintained by the Curriculum Maintenance Manager (CMM) - Engineering Industries. A review will take place midway through the course accreditation period or earlier if required. The review will be informed by feedback from: • course participants and graduates • teaching staff • industry representatives. Course maintenance procedures may also indicate this course should be expired if a suitable qualification becomes available through the development, review or continuous improvement process of a training package qualification. The Victorian Registration and Qualifications Authority (VRQA) will be notified of any significant changes to the course resulting from course monitoring and evaluation processes.

Table 1

Summary of the Foundation Skills for the Certificate IV in Cyber Security

This table contains those language, literacy, numeracy and employment skills that are essential to performance. These skills should be interpreted in conjunction with the detailed requirements of each unit of competency contained in this course. The outcomes described here are broad industry requirements.

Reading skills to:	• read and interpret relevant regulations, signs, labels and other relevant workplace documents associated with cyber security
Writing skills to:	• write reports as part of the inspection and testing requirements and investigations in

	network security • prepare written instructions for others
Oral communication skills to:	• negotiate complex cyber related issues with team members • speak clearly and directly on complex matters, when sharing data, requirements or other information relevant to inspection and testing outcomes in network security
Numeracy skills to:	• perform calculations in binary and hexadecimal number systems • perform basic mathematical calculations when implementing network security infrastructure for an organisation
Learning skills to:	• listen to, or read, interpret and implement technical complex cyber security processes and procedures • adapt own competence in response to change • update own knowledge and skills required for network security
Problem-solving skills to:	• monitor and anticipate problems that may occur including risks and take appropriate action • respond to network security risks in a range of complex and diverse situations • resolve client concerns in relation to cyber security issues • monitor and anticipate problems that may occur in the course of cyber security vulnerability inspection and testing activities
Initiative and enterprise skills to:	• modify activities dependent on different situations • respond appropriately to changes in equipment, standard operation procedures and the working environment • take appropriate actions in a diverse range of cyber security incidents
Teamwork skills to:	• provide leadership during activities as appropriate • collaborate with others • work with diverse range of people with in a

	team environment.
Planning and organising skills to:	• implement emergency plans, systems and procedures • implement procedures for maintaining compliance with relevant work requirements • collect and interpret information needed when undertaking inspection and testing of the network security • organise and plan own activities • manage time priorities
Self-management skills to:	• interpret and apply relevant enterprise procedures • establish and follow own work plans and schedules • evaluate and monitor own work performance
Technology skills to :	• use testing equipment and systems as required • use computers and printers to prepare reports • implement and monitor the application of security software
Digital literacy skills to:	• undertake independent research in a range of technical cyber related issues • find, evaluate, and communicate information on various digital platforms • produce text, images, audio and designs using technology to communicate information to others

Section C - Units of competency

Enterprise units:

VU23213	Utilise basic network concepts and protocols required in cyber security
VU23214	Configure and secure networked end points
VU23215	Test concepts and procedures for cyber security
VU23216	Perform basic cyber security data analysis
VU23217	Recognise the need for cyber security in an organisation
VU23218	Implement network security infrastructure for an organisation
VU23219	Manage the security infrastructure for an organisation
VU23220	Develop and carry out a cyber security industry project
VU23221	Evaluate and test an incident response plan for an enterprise
VU23222	Expose website security vulnerabilities
VU23223	Apply cyber security legislation, privacy and ethical practises
VU23224	Identify the implications of cloud based security systems
VU23225	Investigate Windows security features
VU23226	Test concepts and procedures for cyber exploitation

Endorsed Training package units:

These unit can be download from the National Register of VET *http://training .gov.au*

BSBINS401	Analyse and present research information
BSBWHS309	Contribute effectively to WHS communication and consultation processes
ICTCLD301	Evaluate characteristics of cloud computing solutions and services
ICTCLD401	Configure cloud services
ICTICT426	Identify and evaluate emerging technologies and practices
ICTICT443	Work collaboratively in the ICT industry
ICTNWK422	Install and manage servers
ICTNWK435	Create secure virtual private networks
ICTNWK537	Implement secure encryption technologies
ICTNWK538	Install and maintain valid authentication processes
ICTNWK544	Design and implement a security perimeter for ICT networks
ICTNWK546	Manage network security
ICTPRG434	Automate processes

ICTPRG435	Write script for software applications
ICTSAS440	Monitor and administer security of ICT systems
ICTSAS526	Review and update disaster recovery and contingency plans

UNIT CODE		**VU23213**	
UNIT TITLE		**Utilise basic network concepts and protocols required in cyber security**	
APPLICATION		This unit describes the performance outcomes, skills and knowledge required to comprehend how data travels around the internet. It includes the function and operation of protocols such as Open System Interconnection (OSI) and Transmission Control Protocol/Internet Protocol (TCP/IP) suite and devices that facilitate data transfer. The exposure to these protocols is at an introductory level in this unit. The unit applies to individuals working as cyber security technicians and supports their ability to detect breaches in security infrastructure No licensing or certification requirements apply to this unit at the time of accreditation	
PRE-REQUISITE UNIT(S)		N/A	
ELEMENTS		**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. Assessment of performance is to be consistent with the evidence guide.	
1	Outline key network security concepts	1.1	Network vulnerabilities that affect cyber security in a data network are defined
		1.2	Differences between network security and cyber security are clarified
		1.3	OSI and TCP/IP models of data communication are defined
		1.4	Organisation/enterprises' security policy is sourced reviewed
		1.5	Business implications of cyber security breaches are identified
2	Define key features of the TCP/IP suite of protocols	2.1	Binary number system and hexadecimal number systems are defined
		2.2	Conversions between number systems are demonstrated
		2.3	IPv4 and IPv6 (internet protocol versions 4 & 6) addressing schemes are identified

		2.4	Differences and commonalities between the OSI and TCP/IP models are described and demonstrated
		2.5	Key protocols of the TCP/IP suite are identified and demonstrated
		2.6	TCP/IP Network Interface Layer standards are identified
		2.7	TCP/IP Internet Layer standards and protocols are defined and demonstrated
		2.8	TCP/IP Transport Layer Standards and protocols are defined and demonstrated
		2.9	TCP/IP Application Layer standards and protocols are identified and demonstrated with particular emphasis on how TLS and HTTPS can provide security for network communications
3	Define services, standards and protocols that facilitate security and the functional operation of a network	3.1	Server Message Block (SMB) in the local area network are defined and demonstrated
		3.2	Use of Quick (QUIC) User Datagram Protocol (UDP) to establish more secure HTTP traffic is investigated
		3.3	Narrowband Internet of Things (NB-IoT) and Long Range IoT (LoRa-IoT) standards for IoT devices are investigated
4	Implement and demonstrate the function and operation of key networking devices	4.1	Physical and logical network representations of a local area network are implemented
		4.2	Function and operation of network switches and network routers are described and implemented
		4.3	Function and operation of a firewall is identified
		4.4	Function and operation of a wireless access point (WAP) and a wireless enabled end point is described and implemented
		4.5	End to end network troubleshooting methodologies and commands are demonstrated
5	Implement the components of a network security laboratory and testing environment	5.1	Software tools for the testing environment are identified and implemented
		5.2	Use of virtualisation is described and demonstrated in the testing environment
		5.3	Interconnectivity of the virtualised tools is described and demonstrated

		5.4	Use of the testing environment is demonstrated
6	Present current examples of cyber network attacks and resources	6.1	Example of a Distributed Denial of Service (DDoS) attack is presented
		6.2	Example of a current ransomware breach is presented
		6.3	Example of Local Area Network (LAN) Address Resolution Poisoning (ARP) is presented
		6.4	Useful resources that increase industry's awareness of cyber security awareness are identified

RANGE OF CONDITIONS

Optional Field

N/A

FOUNDATION SKILLS

This section describes language, literacy, numeracy and employment skills that are essential to performance and are not explicitly expressed in the performance criteria of this unit of competency.

Skill	**Description**
Reading skills to:	interpret technical documents and reports
Oral communication skills to:	articulate issues arising from the operation of a network
Technology skills to:	operate a personal computer

UNIT MAPPING INFORMATION	Code and Title Current Version	Code and Title Previous Version	Comments
	VU23213 Utilise basic network concepts and protocols required in cyber security	VU21988 Utilise basic network concepts and protocols required in cyber security	Equivalent

Assessment Requirements

TITLE	Assessment Requirements for: **VU23213 - Utilise basic network concepts and protocols required in cyber security**
PERFORMANCE EVIDENCE	The learner must be able to demonstrate competency in all of the elements, performance criteria and foundation skills in this unit, including evidence of the ability to: • use a network environment to demonstrate the key features of the TCP/IP and OSI models and function as well as the interconnection and operation of key networking devices.
KNOWLEDGE EVIDENCE	The learner must be able to demonstrate essential knowledge required to effectively do the task outlined in elements and performance criteria of this unit, manage the task and manage contingencies in the context of the work role. This includes knowledge of: • Open System Interconnection (OSI) layered communication model • Media Access Layer (MAC) addresses • binary number system • hexadecimal number system • Transmission Control Protocol/Internet Protocol (TCP/IP) • User Datagram Protocol (UDP) • Address resolution Protocol (ARP) • Server Management Block (SMB) • Transport layer Security (TLS) • Hypertext Transfer Protocol Secure (HTTPS) • basics of Internet Protocal Version (IPV4) and Internet Protocol Version (IPV6) addressing • Narrowband IoT (NB – IoT) and Long Range IoT (LoRA) Internet of Things protocols • routers, switches, firewall fundamentals & wireless access points • end to end test commands e.g. Ping, Traceroute, netcat • Quick User Datagram Protocol (UDP) Internet Connections (QUIC) Operation • Denial-of-Service (DOS) & Distributed Denial-of-Service (DDOS) attack mechanisms • Address Resolution Poisoning (ARP) attack mechanism • fundamental ransomware attack mechanisms • virtual machine images and their construction

ASSESSMENT CONDITIONS	This unit can be assessed either in the workplace or in a simulated workplace environment. Where the assessment is conducted in a simulated workplace then the range of conditions must reflect a realistic workplace environment. **Resources:** • computer network system and devices • access to a network security laboratory and testing environment • organisation security documentation **Assessor requirements** Assessors of this unit must satisfy the requirements for assessors in applicable vocational education and training legislation, frameworks and/or standards

UNIT CODE		**VU23214**	
UNIT TITLE		**Configure and secure networked end points**	
APPLICATION		This unit describes the performance outcomes, skills and knowledge required to configure an operating system on a personal computer, adding security, setting user level passwords and privileges to limit and identify user access – all required to increase protection of the end point from cyber security attacks. The unit also provides an overview of internet of things (IoT) devices, an introduction to computer networking virtualisation and base level Linux commands. The unit applies to individuals working as cyber security technicians either alone or as part of a team. No licensing or certification requirements apply to this unit at the time of accreditation.	
PRE-REQUISITE UNIT(S)		N/A	
ELEMENTS		**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. Assessment of performance is to be consistent with the evidence guide.	
1	Identify the role of personal computers and other computing devices in cyber security	1.1	Computer system components are identified and how they work together is explained
		1.2	Role of security relevant peripherals is defined
		1.3	Common computer input output devices are identified
		1.4	Emerging Internet of Things (IOT) devices are identified and demonstrated
		1.5	Security concerns for the network due to the inherent lack of security of IoT devices is identified
2	Undertake preventative maintenance and base level troubleshooting procedures	2.1	Preventative maintenance procedures for a personal computer are described and demonstrated
		2.2	Base level troubleshooting procedures for the operation of a personal computer are demonstrated
3	Configure and use a computer operating system and relevant applications	3.1	Computer Operating System (OS) installation is performed
		3.2	Structure of the OS for a personal computer is examined and the function of the components are explained

		3.3	Security applications for a personal computer are installed and configured
		3.4	Routine system management tasks with appropriate operating system tools are demonstrated
		3.5	Common preventative maintenance techniques for operating systems are described and demonstrated
		3.6	Configuring access controls for a personal computer is described and implemented
		3.7	Setting passwords and allocating privileges for the operating system are described and implemented
4	Define principles of safe software upgrade security practises	4.1	Models of resource access for a computer system are identified
		4.2	Client/Server and Client/Client security issues are explained
		4.3	Strategies for updating software for a Client/Server to minimise security risks are investigated
5	Configure and use virtualised images	5.1	System requirements for installing the virtualisation software are reviewed
		5.2	Required services within the virtualised environment are installed
		5.3	System requirements to ensure virtual machines function are configured
		5.4	Remote client access to virtual machines is configured
6	Identify key concepts in networking personal computers	6.1	Key components of a computer network are identified
		6.2	Purpose and characteristics of networking standards are explained
		6.3	Changing the IP address in an operating system is performed
		6.4	Network connectivity between computers is configured and tested
7	Connect devices to networks	7.1	Setting the IP address in an operating system is performed
		7.2	Network connectivity between wired computers is configured and tested
		7.3	Connectivity to an Internet Service Provider (ISP) from a wired Local Area Network (LAN) is demonstrated

		7.4	Base level troubleshooting methods for wired networks are demonstrated
		7.5	Network connectivity using a Wireless LAN (WLAN) is demonstrated
		7.6	Connectivity to an ISP from the WLAN is demonstrated
		7.7	Base level troubleshooting methods for WLAN networks are explained and demonstrated
		7.8	Connectivity to an ISP from the WLAN is demonstrated
8	Demonstrate base level Linux commands	8.1	Linux Operating system installation on a personal computer is performed
		8.2	Structure and characteristics of the Linux operating system environment are defined
		8.3	Linux security applications are identified
		8.4	Basic system administration using Linux commands is performed
		8.5	Linux commands to enable the personal computer to communicate with other devices in a network are defined and implemented

RANGE OF CONDITIONS

Optional Field

N/A

FOUNDATION SKILLS

This section describes language, literacy, numeracy and employment skills that are essential to performance and are not explicitly expressed in the performance criteria of this unit of competency.

Skill	**Description**
Reading skills to:	comprehend computer technology reports

UNIT MAPPING INFORMATION	Code and Title Current Version	Code and Title Previous Version	Comments
	VU23214 Configure and secure a networked end points	VU21993 Secure a networked personal computer	Equivalent

Assessment Requirements

TITLE	Assessment Requirements for: **VU23214 – Configure and secure networked end points**
PERFORMANCE EVIDENCE	The learner must be able to demonstrate competency in all of the elements. performance criteria and foundation skills in this unit and provide evidence of the ability to: • install an operating system on a personal computer • configure the personal computer in order for it to connect with other network devices • set a user level password on a personal computer
KNOWLEDGE EVIDENCE	The learner must be able to demonstrate essential knowledge required to effectively do the task outlined in elements and performance criteria of this unit, manage the task and manage contingencies in the context of the work role. This includes knowledge of: • Hardware components of a personal computer • Personal computer (PC) peripherals • Internet of Things (IoT) devices • Windows operating system installation, structure and base level security configuration • Virtualisation concepts, structure and operation • Creating and configuring virtualised images • Linux operating system installation, structure and base level security configuration
ASSESSMENT CONDITIONS	This unit can be assessed either in the workplace or in a simulated workplace environment. Where the assessment is conducted in a simulated workplace then the range of condition must reflect a realistic workplace environment. **Resources:** • computer equipment • networking equipment • relevant computer software • relevant documentation **Assessor requirements** Assessors of this unit must satisfy the requirements for assessors in applicable vocational education and training legislation, frameworks and/or standards.

UNIT CODE		**VU23215**	
UNIT TITLE		**Test concepts and procedures for cyber security**	
APPLICATION		This unit describes the performance outcomes, skills and knowledge required to implement testing procedures for computer systems in an organisation. The unit examines common threats, ethical hacking principles, and an introduction to penetration testing, social engineering security issues, enumeration, port scanning, foot printing, traffic sniffers and wireless local area network (WLAN) vulnerabilities and also includes treatment of intrusions. It also requires the ability to apply layer testing framworks and tools as well as network testing and monitoring tools This unit is applies to individuals working as cyber security technicians either alone or as part of a team. No licensing or certification requirements apply to this unit at the time of accreditation.	
PRE-REQUISITE UNIT(S)		N/A	
ELEMENTS		**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. Assessment of performance is to be consistent with the evidence guide.	
1	Identify typical cyber security application layer testing methodologies and tools	1.1	Existing frameworks that identify common application layer vulnerabilities are investigated
		1.2	Common application layer security vulnerabilities are identified
		1.3	Current policies to minimise the identified application layer vulnerabilities are reviewed
2	Use networking security testing methodologies, tools and commands	2.1	End to end testing commands for network continuity are demonstrated
		2.2	Systematic troubleshooting procedures for network connectivity are demonstrated
		2.3	Use of networking monitoring tools are demonstrated
3	Implement the laboratory testing environment	3.1	Laboratory testing environment is configured
		3.2	Using end to end testing commands, the laboratory environment is tested for functionality
4		4.1	Current Trojans, Virus’s and Worms are identified

	Identify common threats and mitigation strategies	4.2	Methods of Denial of Service (DOS) and Distributed Denial of Service (DDOS) attacks and corresponding mitigation strategies are investigated
		4.3	Methods of Domain Name Server (DNS) attacks and corresponding mitigation strategies are identified
		4.4	Zero day vulnerabilities are identified
		4.5	Common vulnerabilities and exposures (CVEs) are defined
		4.6	Heuristics as a methodology for string analysis and their corresponding toolset are described
5	Demonstrate ethical hacking principles and procedures	5.1	Ethical hacking process and procedures are described
		5.2	Base level troubleshooting procedures are demonstrated
		5.3	Fundamentals of penetration testing are described
		5.4	Legal implications of hacking are explained
		5.5	Process of foot printing the computer systems of a company is examined
		5.6	Methodologies of enumeration to gather system usernames are described
		5.7	Tools to port scan a computer system are demonstrated
		5.8	Methodologies of system hacking are described then demonstrated
		5.9	Common sniffing tools are described and demonstrated
6	Identify security vulnerabilities of WLANs	6.1	WLAN physical vulnerabilities are identified
		6.2	WLAN software issues and vulnerabilities are determined
7	Demonstrate basic scripting for a cyber security environment	7.1	Introduction to scripting languages is demonstrated
		7.2	Scripts for testing tools are described and demonstrated
		7.3	Key system and third-party import libraries are described
		7.4	Scripting basic programming language is described and demonstrated

RANGE OF CONDITIONS

Optional Field

N/A

FOUNDATION SKILLS

This section describes language, literacy, numeracy and employment skills that are essential to performance and are not explicitly expressed in the performance criteria of this unit of competency.

Skill	Description
Problem solving skills to:	interpret results from software packages and configure lab testing environment
Writing skills to:	communicate test results effectively via reporting to enable remediation of identified issues

UNIT MAPPING INFORMATION

Code and Title Current Version	Code and Title Previous Version	Comments
VU23215 Test concepts and procedures for cyber security	VU21989 Test concepts and procedures for cyber security	Equivalent

Assessment Requirements

TITLE	Assessment Requirements for: **VU23215 - Test concepts and procedures for cyber security**
PERFORMANCE EVIDENCE	The learner must be able to demonstrate competency in all of the elements, performance criteria and foundation skills in this unit and must provide evidence of the ability to: • Undertake testing procedures on a system in order to demonstrate security vulnerabilities and identify appropriate mitigation strategies for two (2) scenarios.

KNOWLEDGE EVIDENCE	The learner must be able to demonstrate essential knowledge required to effectively do the task outlined in elements and performance criteria of this unit, manage the task and manage contingencies in the context of the work role. This includes knowledge of:
	• layer 3 test command:
	  ○ Ping
	  ○ Traceroute
	• ethical hacking procedures
	• common threats and mitigation strategies
	• penetration testing
	• foot printing
	• enumeration
	• port Scanning
	• system hacking
	• trojans, viruses and worms
	• sniffing tools
	• Denial-of-Service (DOS) & Distributed Denial-of-Service (DDOS) attack mechanisms
	• Domain Name System (DNS) attack methodologies
	• Wireless Local Area Network (WLAN) physical and software vulnerabilities
	• scripting languages such as Python

ASSESSMENT CONDITIONS	This unit can be assessed either in the workplace or in a simulated workplace environment. Where the assessment is conducted in a simulated workplace then the range of conditions must reflect a realistic workplace environment. **Resources:** • computer software • virtualisated testing environment e.g. Kali, Wireshark

	• relevant documentation including:
	  ○ codes
	  ○ standards
	  ○ manuals
	  ○ reference material
	Assessor requirements
	Assessors of this unit must satisfy the requirements for assessors in applicable vocational education and training legislation, frameworks and/or standards.

UNIT CODE		**VU23216**	
UNIT TITLE		**Perform basic cyber security data analysis**	
APPLICATION		This unit describes the performance outcomes, knowledge and skills required to detect and recognise discrepancies in data by performing analysis. The unit covers the collection of data on a scenario and performing basic analysis which includes the process of breaking down the scenario to a set of subtasks which are examined for their effectiveness. The unit also examines databases as a repository for data and the vulnerabilities that exist as well as software tools to support pattern recognition. This unit is applies to individuals working as cyber security technician either alone or as part of a team.. No licensing sor certification requirements apply to this unit at the time of accreditation.	
PRE-REQUISITE UNIT(S)		N/A	
ELEMENTS		**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. Assessment of performance is to be consistent with the evidence guide.	
1	Demonstrate the process of basic cyber security data analysis	1.1	Sources of data used to monitor a network are identified
		1.2	Information for a provided scenario from alerts, logs or reported events is collected
		1.3	Strategies to process this data is developed
		1.4	Data to be processed is broken down into subtasks and a range of strategies to analyse these subtasks are developed.
		1.5	Effectiveness of the subtasks implementation is evaluated and modified as required
2	Examine the use of data bases as a repository for data	2.1	Use of a data base to store personal information is described and demonstrated
		2.2	Structured Query Language (SQL) commands to access the data are identified and demonstrated
		2.3	Database security vulnerabilities are identified
		2.4	Strategies for mitigating database vulnerabilities are investigated

3	Identify discrepancies and anomalies in data sets	3.1	Detecting discrepancies in data is described and performed
		3.2	Pattern recognition is demonstrated
		3.3	Software tools to support the detection of anomalies and discrepancies are demonstrated
		3.4	Detecting anomalies in data is demonstrated
		3.5	Software tools to support the detection of anomalies and discrepancies are demonstrated
		3.6	Use of automation in data collection and analysis is explained

RANGE OF CONDITIONS

Sources of data provided in the Knowledge Evidence are examples only. Sources maybe replaced or added to.

FOUNDATION SKILLS

This section describes language, literacy, numeracy and employment skills that are essential to performance and are not explicitly expressed in the performance criteria of this unit of competency.

Skill	**Description**
Reading skills to:	comprehend documented material and procedures
Technology skills to:	use a laptop or workstation and install and use software packages

UNIT MAPPING INFORMATION	Code and Title Current Version	Code and Title Previous Version	Comments
	VU23216 Perform basic cyber security data analysis	VU21994 Perform basic cyber security data analysis	Equivalent

Assessment Requirements

TITLE	Assessment Requirements for: **VU23216 - Perform basic cyber security data analysis**
PERFORMANCE EVIDENCE	The learner must be able to demonstrate competency in all of the elements, performance criteria and foundation skills in this unit and provide evidence of their ability to: • Collect data and perform basic cyber security data analysis using software tools to detect anomalies and discrepancies.

KNOWLEDGE EVIDENCE	The learner must be able to demonstrate essential knowledge required to effectively do the task outlined in elements and performance criteria of this unit, manage the task and manage contingencies in the context of the work role. This includes knowledge of:
	• Sources of data. Examples are:
	  ○ firewalls
	  ○ Intrusion Detection Systems (IDS)
	  ○ Access Control Systems (ACS)
	  ○ System logs
	  ○ Netflow information
	  ○ Network Access Control (NAC) systems
	  ○ Security and Event Management systems (SIEM)
	• Database concepts
	• Inputting data to a database
	• Accessing data from a database
	• Database security vulnerabilities
	• Software tools to identify data patterns
	• Mitigation strategies to minimise database security vulnerabilities

ASSESSMENT CONDITIONS	This unit can be assessed either in the workplace or in a simulated workplace environment. Where the assessment is conducted in a simulated workplace then the range of conditions must reflect a realistic workplace environment.
	Resources:
	• computer hardware and software
	• access to data scenarios
	• relevant documentation including:
	  ○ workplace procedures
	  ○ codes/standards
	  ○ manuals and reference material
	Assessor requirements
	Assessors of this unit must satisfy the requirements for assessors in applicable vocational education and training legislation, frameworks and/or standards.

UNIT CODE		**VU23217**	
UNIT TITLE		**Recognise the need for cyber security in an organisation**	
APPLICATION		This unit describes the performance outcome, knowledge and skills required to recognise threats, risks and vulnerabilities to cyber security in an organisation. The threats to an organisation include networks, machines, applications, data, users and infrastructure. The unit addresses common cyber security attack mechanisms and an introduction to threat management as well as security issues surrounding Internet of Things (IoT) devices. The unit also includes the implementation of tools and systems an organisation can use for protection against cyber-attacks. This unit applies to individuals working as cyber security technicians either alone or as part of a team. No licensing or certification requirements apply to this unit at the time of accreditation.	
PRE-REQUISITE UNIT(S)		N/A	
ELEMENTS		**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. Assessment of performance is to be consistent with the evidence guide.	
1	Identify the need for cyber security for an organisation	1.1	Reasons to protect online identity and personal data are clarified
		1.2	Reasons to protect an organisation's data are explained
		1.3	Cyber security awareness practices for an organisation are identified
		1.4	Concept of cyber threat is defined
		1.5	Reasons for the need for cyber security professionals are explained
2	Investigate common and emerging cyber security attacks, and techniques	2.1	Difference between threat actors, threat vectors and threat goals are clarified
		2.2	Techniques used by attackers to infiltrate a system are described

		2.3	Characteristics and operation of a cyber-attack are explained
		2.4	Trends of cyber threats are examined
		2.5	Cyber attack methods on an organisation infrastructure are identified
		2.6	Examples of IoT devices are provided
		2.7	Security vulnerabilities for IoT devices are explained
3	Investigate methods to protect personal data and privacy	3.1	Techniques to protect personal devices from cyber threats are described and demonstrated
		3.2	User authentication techniques are identified and demonstrated
		3.3	Methods and tools to safeguard personal privacy are identified and demonstrated
4	Examine methods used to protect an organisation's data	4.1	Common infrastructure, equipment, and software used to protect an organisation from cyber security attacks are identified
		4.2	Cyber security terms such as botnets, malware, virus's, worms, Root Kits are clarified
		4.3	Mitigation strategies such as the cyber kill chain process, the MITRE Adversarial Tactics, Techniques and Common Knowledge (ATT&CK) in the context of cyber security protection and mitigation strategies are explained
		4.4	Policies, tools and systems for protecting an organisation from cyber-attacks are investigated
		4.5	Behaviour based approach to cyber security is investigated
		4.6	Incident response policies, processes and systems are reviewed
5	Investigate current Cyber Security Frameworks (CSF)	5.1	Fundamentals of the National Institute of Standards and Technology Cyber Security Framework (NIST CSF) are examined and explained
		5.2	Essential Eight strategies from the Australian Cyber Security Centre (ACSC) to mitigate Cyber Security incidents are identified
		5.3	Centre for Internet Security (CIS) controls identified for organisations to implement for Cyber Security protection are examined

RANGE OF CONDITIONS

Optional Field

N/A

FOUNDATION SKILLS

This section describes language, literacy, numeracy and employment skills that are essential to performance and are not explicitly expressed in the performance criteria of this unit of competency.

Skill	Description
Reading skills to	interpret and follow documented material and procedures
Technology skills to	use a PC or laptop computer and software tools

UNIT MAPPING INFORMATION

Code and Title Current Version	Code and Title Previous Version	Comments
VU23217 Recognise the need for cyber security in an organisation	VU21990 Recognise the need for cyber security in an organisation	Equivalent

Assessment Requirements

TITLE	Assessment Requirements for **VU23217 - Recognise the need for cyber security in an organisation**
PERFORMANCE EVIDENCE	The learner must be able to demonstrate competency in all of the elements, performance criteria and foundation skills in this unit and provide evidence of the ability to: • identify threats, risks and vulnerabilities to sensitive organisational data and recommend suitable methodologies to protect the data for two (2) scenarios.
KNOWLEDGE EVIDENCE	The learner must be able to demonstrate essential knowledge required to effectively do the task outlined in elements and performance criteria of this unit, manage the task and manage contingencies in the context of the work role. This includes knowledge of: • cyber security awareness work practises • sources of cyber security attacks • types of security vulnerabilities and malware • methods to protect your own data and privacy • methods of cyber security attacks • introduction to cyber security mitigation techniques and resources • methods and tools used to protect an organisation's data • fundamentals of National Institute of Standards and Technology Cyber Security Framework (NIST CSF) • Essential eight strategies from the Australian Cyber Security Centre (ACSC) to mitigate cyber security incidents • Centre for Internet Security (CIS) controls • Internet of Things (IoT) devices and their security vulnerabilities

ASSESSMENT CONDITIONS	This unit can be assessed either in the workplace or in a simulated workplace environment. Where the assessment is conducted in a simulated workplace then the range of conditions must reflect a realistic workplace environment.
	Resources:
	• computer equipment
	• networking equipment
	• computer software
	• relevant documentation including:
	  ○ workplace procedures
	  ○ codes/standards
	  ○ manuals and reference material
	Assessor requirements

	Assessors of this unit must satisfy the requirements for assessors in applicable vocational education and training legislation, frameworks and/or standards.

UNIT CODE		**VU23218**	
UNIT TITLE		**Implement network security infrastructure for an organisation**	
APPLICATION		This unit describes the performance outcomes skills and knowledge required to recognise the key features that make up the network security for an organisation. It required the ability to investigate threats and mitigation techniques, network security models, administration protection and user access methods, introduction to firewall setup and configuration, intrusion prevention and intrusion detection systems (IPS/IDS) and software used to protect an organisation. The unit also examine proxy server vulnerabilities, Wireless Local Area Network (WLAN), security vulnerabilities and the application of Virtual Private Networks (VPN's) and cryptography fundamentals. This unit applies to individuals working as cyber security technicians either alone or as part of a team. No licensing or certification requirements apply to this unit at the time of accreditation.	
PRE-REQUISITE UNIT		VU23213 - Utilise basic network concepts and protocols required in cyber security	
ELEMENTS		**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. Assessment of performance is to be consistent with the evidence guide.	
1	Examine the different models of security solutions for an organisation	1.1	Physical security system solutions for an organisation are described
		1.2	Hybrid security system solutions for an organisation are explained
		1.3	Cloud based security system solutions for an organisation are described
		1.4	Potential risks of network perimeter security devices for an organisation are identified
2	Investigate methods used to authenticate users to a network	2.1	Process and reasons for configuring secure administrative access to network devices are explained
		2.2	Authentication, Authorization and Accounting (AAA) procedures to access network devices are described
		2.3	AAA authentication from a local server is implemented

		2.4	Multifactor Authentication (MFA) processes to add security to an organisation's network access are examined
3	Investigate the operation and role of software tools to monitor traffic and security in an organisation	3.1	Examples of Network Access Control (NAC) features are described and demonstrated
		3.2	Function and role of End Point Protection (EPP), End point Detection and Response (EDR), Extended Detection and Response (XDR) and Data Loss Prevention (DLP) systems for end points is defined
		3.3	Features of network monitoring tools are identified and demonstrated
4	Prepare and implement a firewall	4.1	Features of basic and next generation firewalls are compared
		4.2	Methods of traffic flow control for firewalls are identified
		4.3	Function and operation of a firewall to mitigate network attacks is described and implemented
		4.4	Basic configuration of firewall security zones is demonstrated and implemented
		4.5	Basic packet filtering is demonstrated and implemented
5	Investigate intrusion prevention and intrusion detection systems (IPS/IDS)	5.1	Differences between intrusion prevention and intrusion detection systems are clarified
		5.2	Process of detecting malicious traffic using signatures is demonstrated
		5.3	Artificial Intelligence (AI) and Machine Learning (ML) methods and tools to detect malicious data streams are investigated
6	Examine proxy server vulnerability issues	6.1	Function and operation of a proxy server is explained
		6.2	Methods used to compromise the security of a proxy server are identified
		6.3	Mitigation strategies to protect a proxy server are defined
7	Investigate wireless security access and common vulnerabilities	7.1	Overview of the 802.11 Wireless Local Area Network (WLAN) Standard is provided
		7.2	Relationship between the Data Layer and the Physical layers for WLANs is defined

		7.3	WLAN architecture of a typical system is defined and demonstrated
		7.4	Authentication and Association methods for wireless clients are described and demonstrated
		7.5	Strengths and weaknesses of WLAN encryption techniques are identified
		7.6	Current tools to discover details about available WLANs are selected and utilised
		7.7	WLAN security checklist is developed
8	Demonstrate the fundamental operation of cryptographic systems	8.1	Overview of cryptography is provided
		8.2	Process of working with symmetric & asymmetric algorithms is defined
		8.3	Function and operation of encryption, hashes and digital signatures to secure a network is explained
		8.4	Data integrity and authentication utilising encryption algorithms are defined
		8.5	Data confidentiality utilizing encryption algorithms are summarised
		8.6	Process of public key encryption to ensure data confidentiality is demonstrated
		8.7	Cryptography standards and protocols are summarised
		8.8	Common use of protocols that utilise cryptography are demonstrated
9	Demonstrate the fundamentals of Virtual Private Networks (VPN's)	9.1	Advantages and operation of VPN's are explained
		9.2	Operation of tunnelling is described and demonstrated
		9.3	Operation of Internet Protocol Security (IPSec) VPN's is summarised
		9.4	Site to site IPSec VPN with pre shared key authentication is demonstrated
		9.5	Different software VPN software packages enabling remote access to an organisations network are compared
		9.6	VPN-Less alternatives for secure remote access to an organisations network are examined

RANGE OF CONDITIONS

End point security tools provided in the Knowledge Evidence are examples only. Individual tools maybe replaced or added to.

FOUNDATION SKILLS

This section describes language, literacy, numeracy and employment skills that are essential to performance and are not explicitly expressed in the performance criteria of this unit of competency.

Skill	**Description**
Numeracy skills to:	Perform basic mathematical calculations
Problem solving skills to:	plan and apply foundational troubleshooting of network security infrastructure
Technology skills to:	Use a personal computer

UNIT MAPPING INFORMATION

Code and Title Current Version	Code and Title Previous Version	Comments
VU23218 Implement network security infrastructure for an organisation	VU21991 Implement network security infrastructure for an organisation	Equivalent

Assessment Requirements

TITLE	Assessment Requirements for **VU23218 - Implement network security infrastructure for an organisation**
PERFORMANCE EVIDENCE	The learner must be able to demonstrate competency in all of the elements, performance criteria and foundation skills in this unit and provide evidence of the ability to: • recognise the key features that make up network security and apply strategies to secure the network infrastructure of an enterprise/organisation.
KNOWLEDGE EVIDENCE	The learner must be able to demonstrate essential knowledge required to effectively do the task outlined in elements and performance criteria of this unit, manage the task and manage contingencies in the context of the work role. This includes knowledge of: • Security models for an organisation • Authentication methods for users to connect securely to a network • End point security tools. Examples are: End Point Protection (EPP), End point Detection and Response (EDR), Extended Detection and Response (XDR) and Data Loss Prevention (DLP) • Configuring firewall zones • Intrusion Prevention and Intrusion Detection Systems (IPS/IDS) • Wireless Local Area Network (WLAN) operation and vulnerabilities • Proxy Server Security issues • Encryption, hashes and digital signature • Fundamentals of Virtual Private Networks (VPN's) • VPN-less methods to secure remote connect to a network
ASSESSMENT CONDITIONS	This unit can be assessed either in the workplace or in a simulated workplace environment. Where the assessment is conducted in a simulated workplace then the range of conditions must reflect a realistic workplace environment. **Resources:** • computer equipment • networking equipment • computer software • relevant documentation including: ○ manuals and reference materials **Assessor requirements** Assessors of this unit must satisfy the requirements for assessors in applicable vocational education and training legislation, frameworks and/or standards.

UNIT CODE		**VU23219**	
UNIT TITLE		**Manage the security infrastructure for an organisation**	
APPLICATION		This unit describes the performance outcomes, knowledge and skills required to manage the security infrastructure for an organisation. It includes assessing risk, implementing appropriate controls, monitoring their effectiveness and compiling reports for future audit purposes. It requires the ability to monitor and evaluate the physical security infrastructure of the organisation, and implement a security infrastructure maintenance program. This unit applies to individuals who work as cyber security technicians and who manage, monitor and evaluate the organisation's security infrastructure as part of a team. No licensing or certification requirements apply to this unit at the time of accreditation.	
PRE-REQUISITE UNIT(S)		N/A	
ELEMENTS		**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. Assessment of performance is to be consistent with the evidence guide.	
1	Identify the key features from information and security policies for an organisation	1.1	Information and security policy documents for the organisation are accessed and examined
		1.2	Implications of the organisation's employees work habits relating to its security policy are evaluated
		1.3	Implications of the organisation's configuration and change management capability are evaluated
		1.4	Levels of security clearances to access organisational data are identified
2	Determine risk category for the security infrastructure	2.1	Audit of existing tools and security infrastructure for the organisation is conducted
		2.2	Asset valuation for the organisation is determined
		2.3	Security infrastructure baseline is determined
		2.4	Risk assessment of the organisation assets is conducted and associated risks categorised
		2.5	Resources required by risk categories to minimise disruption to business operation is identified
3	Identify the physical security vulnerabilities	3.1	Physical structure of the organisation's security infrastructure is examined

	of the organisation's security infrastructure	3.2	Security infrastructure vulnerabilities are identified and documented
		3.3	Physical security infrastructure vulnerabilities are communicated to appropriate management personnel
4	Implement appropriate security system controls for managing the risk	4.1	Effective controls to manage risk are devised and implemented
		4.2	Policies and procedures to cover user access to the system are developed
		4.3	Security recovery plan is developed
		4.4	System controls to reduce risks in human interaction with the system are implemented
5	Monitor security infrastructure tools and procedures	5.1	Controls that manage risks are reviewed and monitored
		5.2	Vendor products that monitor risk rating criteria for an organisation are reviewed
6	Promote cyber security awareness in the organisation	6.1	Strategies to promote security policy awareness amongst the staff of the organisation are planned and implemented
		6.2	Security policy awareness strategies are evaluated for their effectiveness within the organisation and if required modified for increased impact
		6.3	Training to implement the organisation's security policy practices is planned and implemented
7	Implement cyber hygiene principles	7.1	Best practices in cyber hygiene are identified
		7.2	Cyber hygiene process is identified and implemented

RANGE OF CONDITIONS

Optional Field

N/A

FOUNDATION SKILLS

This section describes language, literacy, numeracy and employment skills that are essential to performance and are not explicitly expressed in the performance criteria of this unit of competency.

Skill	**Description**
Reading skills to:	interpret documented material and procedures
Writing skills to:	document incidents and complete reports
Planning and organising skills to:	deliver training to an organisations staff

UNIT MAPPING INFORMATION	Code and Title Current Version	Code and Title Previous Version	Comments
	VU23219 Manage the security infrastructure for an organisation	VU21995 Manage the security infrastructure for the organisation	Equivalent

Assessment Requirements

TITLE	Assessment Requirements **for VU23219 - Manage the security infrastructure for an organisation**
PERFORMANCE EVIDENCE	The learner must be able to demonstrate competency in all of the elements, performance criteria and foundation skills in this unit and provide evidence of their ability to: • plan and document a security infrastructure for an organisation which includes: assessing risks, implementing appropriate controls and monitoring of their effectiveness.
KNOWLEDGE EVIDENCE	The learner must be able to demonstrate essential knowledge required to effectively do the task outlined in elements and performance criteria of this unit, manage the task and manage contingencies in the context of the work role. This includes knowledge of: • cyber security risk management plans and policies • risk assessment of organisations assets and systems • risk assessment of organisations cyber security infrastructure • cyber security awareness strategies • best practices in cyber hygiene processes
ASSESSMENT CONDITIONS	This unit can be assessed either in the workplace or in a simulated workplace environment. Where the assessment is conducted in a simulated workplace then the range of conditions must reflect a realistic workplace environment. **Resources:** • access to an organisations security infrastructure, policy and procedures **Assessor requirements** Assessors of this unit must satisfy the requirements for assessors in applicable vocational education and training legislation, frameworks and/or standards.

UNIT CODE		**VU23220**	
UNIT TITLE		**Develop and carry out a cyber security industry project**	
APPLICATION		This unit describes the performance outcomes, skills and knowledge to develop and undertake a project that simulates a real cyber security industry environment. The project may include using a Cyber Security Operations Centre (CSOC) sandbox or equivalent laboratory environment. This environment allows the participant to demonstrate configuring and testing of firewalls, implementing Intrusion Detection/Prevention Systems (IDS/IPS) and evaluating and identifying any traffic anomalies. The use of Red & Blue teaming exercises to identify security breaches and apply mitigation strategies to minimise further risk are included as part of the project. This unit applies to individuals working as cyber security technicians within a team evironment. No licensing or certification requirements apply to this unit at the time of accreditation.	
PRE-REQUISITE UNITS		VU23213 - Utilise basic network concepts and protocols required in cyber security VU23215 - Test concepts and procedures for cyber security	
ELEMENTS		**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. Assessment of performance is to be consistent with the evidence guide.	
1	Establish project team	1.1	Team members for the project are selected
		1.2	Individual responsibilities for each team member are determined
		1.3	Team performance criteria are established
		1.4	Methodology of team performance measurement is defined
2	Determine context of business need or problem (project)	2.1	Scope and system boundaries of the business problem are determined together with the problem solving methodology
		2.2	Background information is gathered and development of questions appropriate to the business problem are prepared

		2.3	Objectives and expected outcomes to be achieved are identified and documented
		2.4	Key elements for project milestones are identified
		2.5	Work plan statement is developed
3	Support the project plan development	3.1	Process of identifying tasks and resources needed to complete the project plan is determined
		3.2	Schedule of project tasks including realistic timeframes and costs is prepared
		3.3	Specific responsibilities to project team members are allocated
		3.4	Process to manage risks and/or unexpected events that may impact upon the project objectives and/or timelines is developed
4	Evaluate the suitability of the gathered resources	4.1	Key components required from the project are identified
		4.2	Resources for the project are allocated
		4.3	Function and operation of selected resources allocated to team members are defined
5	Implement the project design	5.1	Suitable systematic processes to implement the project are selected
		5.2	Subtasks for the overall project are defined and allocated to team members
		5.3	Subtasks are developed
		5.4	A systematic testing procedure is defined
		5.5	As part of the project Red and Blue teaming exercises are planned and executed
		5.6	Verification of the functionality of the project in either part or full is performed
		5.7	Documentation for the process such as meeting minutes, reports, emails is generated
6	Support project completion and handover	6.1	An implementation plan with minimal end user's disruption is developed
		6.2	Technical documentation including project timeframes, scope, cost is drafted

		6.3	Technical documentation for approval by appropriate person/s is submitted
		6.4	Developed project risk strategy is evaluated
		6.5	Where required appropriate plan to train end users is presented
		6.6	Final project sign-off from sponsor and key stakeholders is obtained
		6.7	Project is closed and experience gained and lessons learnt are discussed and documented

RANGE OF CONDITIONS

Implementing tools listed in the Knowledge Evidence to detect data anomalies are examples only and may be replaced or added to.

FOUNDATION SKILLS

This section describes language, literacy, numeracy and employment skills that are essential to performance and are not explicitly expressed in the performance criteria of this unit of competency.

Skill	**Description**
Reading skills to:	interpret the problem brief and related documentation
Writing skills to:	prepare reports and related documentation
Oral communication skills to:	deliver presentations to clients and communicate and problem solve with team members
Technical skills to:	install and use software package

UNIT MAPPING INFORMATION

Code and Title Current Version	Code and Title Previous Version	Comments
VU23220 Develop and carry out a cyber security industry project	VU21992 Develop a cyber security industry project	Equivalent

Assessment Requirements

TITLE	Assessment Requirements for **VU23220 - Develop and carry out a cyber security industry project**
PERFORMANCE EVIDENCE	The learner must be able to demonstrate competency in all of the elements, performance criteria and foundation skills in this unit and provide evidence of: • participation in a team based cyber security project contributing to the development, execution and the evaluation of the project in a real or simulated industry environment.

KNOWLEDGE EVIDENCE	The learner must be able to demonstrate essential knowledge required to effectively do the task outlined in elements and performance criteria of this unit, manage the task and manage contingencies in the context of the work role. This includes knowledge of:
	• team work fundamentals
	• using project planning tools
	• creating and configuring and interconnecting virtualised devices
	• configuring basic features of firewalls
	• implementing tools to detect data anomalies. Examples are:
	  ○ Intrusion Detection/Prevention Systems (IDS/IPS) systems
	  ○ Security information and event management (SIEM) Tool
	  ○ End Point Protection (EPP)
	  ○ Wireshark
	• Models of Cyber Security for an organisation
	• Components of a Cyber Security Operation Centre (CSOC)
	• Red and Blue teaming exercises

ASSESSMENT CONDITIONS	This unit can be assessed either in the workplace or in a simulated workplace environment. Where the assessment is conducted in a simulated workplace then the range of conditions must reflect a realistic workplace environment. **Resources:** • access to a others to form a team • computer equipment • networking equipment • computer software/virtualised testing environment • relevant documentation **Assessor requirements**

	Assessors of this unit must satisfy the requirements for assessors in applicable vocational education and training legislation, frameworks and/or standards.

UNIT CODE		**VU23221**	
UNIT TITLE		**Evaluate and test an incident response plan for an enterprise**	
APPLICATION		This unit describes the performance outcomes knowledge and skills required to examine an organisation's existing incident response plan (IRP) and expand it as necessary to deal with incidents more thoroughly. The unit requires the ability to form a team, clarify roles, interpret an incident response plan (IRP), use red, blue and purple teams to test the IRP, implement an incident, evaluate the IRP for its effectiveness and if required make improvements. This unit applies to individuals working as cyber security technicians either alone or as part of a team. No licensing or certification requirements apply to this unit at the time of accreditation.	
PRE-REQUISITE UNIT(S)		N/A	
ELEMENTS		**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. Assessment of performance is to be consistent with the evidence guide.	
1	Form an incident response team	1.1	Members to form incident response team (IRT) are recruited
		1.2	IRT members roles and responsibilities are defined
		1.3	Communication strategies and reporting hierarchy for the IRT within the organisation are determined
		1.4	Business implications to the organisation of cyber incidents are articulated to the IRT
2	Define red, blue and purple team tasks	2.1	Fundamental red teaming activities for incident responses are created
		2.2	Fundamental blue teaming activities for incident responses are created
		2.3	Fundamental purple teaming activities are defined
3	Plan the implementation of the organisation's incident response plan (IRP)	3.1	Organisation's incident management plan is evaluated
		3.2	Services the IRT will provide are defined
		3.3	Response plans to a range of incidents are developed

		3.4	Reporting procedures for incident handling are developed
		3.5	Processes for collecting and protecting evidence during incident responses are developed
		3.6	Incident response exercises and red-teaming activities are created
		3.7	Incident response staffing and training requirements are specified
4	Implement the IRP for prescribed incidents	4.1	Red-teaming activities are executed for the range of incident responses
		4.2	Response to the incidents is reported
		4.3	Incident response evidence is collected, processed and preserved in accordance with the organisation's guidelines
		4.4	Strategy of blue-teaming activities to mitigate the incident responses are discussed and evaluated
		4.5	Incident management measures are collected, analysed and reported
5	Evaluate the IRP	5.1	Improvements learnt from the IRP activities are implemented
		5.2	Effectiveness of red teaming and incident response tests, training and exercises are examined and modified as required
		5.3	Communication between incident response team and organisations management are assessed for effectiveness and changes implemented if required

RANGE OF CONDITIONS

Tools used to test a network for vulnerabilities provided in the Knowledge Evidence are examples only. Individual tools maybe replaced or added to.

FOUNDATION SKILLS

This section describes language, literacy, numeracy and employment skills that are essential to performance and are not explicitly expressed in the performance criteria of this unit of competency.

Skill	**Description**
Reading skills to:	interpret and follow documented material and procedures
Numeracy skills to:	perform basic mathematical calculations
Problem solving skills to:	identify abnormal data

	Technology skills to:	install and demonstrate the application of software packages	
UNIT MAPPING INFORMATION	Code and Title Current Version	Code and Title Previous Version	Comments
	VU23221 Evaluate and test an incident response plan for an enterprise	VU21996 Evaluate and test an incident response plan for an enterprise	Equivalent

Assessment Requirements

TITLE	Assessment Requirements for **VU23221 - Evaluate and test an incident response plan for an enterprise**
PERFORMANCE EVIDENCE	The learner must be able to demonstrate competency in all of the elements, performance criteria and foundation skills in this unit and provide evidence of the ability to: • examine and test the effectiveness of an organisation's existing incident response plan (IRP) and modify it as necessary to deal with incidents more thoroughly.
KNOWLEDGE EVIDENCE	The learner must be able to demonstrate essential knowledge required to effectively do the task outlined in elements and performance criteria of this unit, manage the task and manage contingencies in the context of the work role. This includes knowledge of: • role and responsibilities of an incident response team (IRT) • content and function of an incident response plan (IRP) • basic level penetration testing of a simulated security system for an enterprise • tools used to test a network for vulnerabilities. Examples are: Kali, Linux, Metasploit • fundamental red, blue and purple teaming activities • continual quality improvements of the IRP plan
ASSESSMENT CONDITIONS	This unit can be assessed either in the workplace or in a simulated workplace environment. Where the assessment is conducted in a simulated workplace then the range of conditions must reflect a realistic workplace environment. **Resources:** • access to an IRP • computer hardware and software including testing tools • relevant documentation including: o workplace procedures o codes/standards o manuals and reference material **Assessor requirements:** Assessors of this unit must satisfy the requirements for assessors in applicable vocational education and training legislation, frameworks and/or standards.

UNIT CODE		**VU23222**	
UNIT TITLE		**Expose website security vulnerabilities**	
APPLICATION		This unit describes the performance outcomes knowledge and skills required to maintain the security of an organisation's website by utilising the outcomes of the Open Web Application Security Project (OWASP). It requires the ability to apply penetration testing tools to determine the vulnerabilities of a web site, assess the vulnerabilities and report to appropriate personnel. This unit applies to individuals working as cyber security technicians either alone or as part of a team. No licensing or certification requirements apply to this unit at the time of accreditation.	
PRE-REQUISITE UNIT(S)		N/A	
ELEMENTS		**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. Assessment of performance is to be consistent with the evidence guide.	
1	Explain the Hypertext Transfer Protocol (HTTP) and web server architectures	1.1	Web application server architecture is explained
		1.2	Structure and operation of the HTTP protocol is described
		1.3	Function and role of HTTP Headers is identified
		1.4	Typical HTTP Headers are examined
		1.5	Securing HTTP using headers is identified
		1.6	OWASP Secure Headers Project tools are examined
2	Identify web site content	2.1	Technology stack of a web application and web server are identified
		2.2	Web server scanner software and web content scanner software are demonstrated
		2.3	Spiderling for web applications and websites are described and demonstrated
3	Install web application proxy testing tools	3.1	Example of web application proxy testing tools are described and demonstrated
		3.2	Proxy testing tools for a proxy server are configured and installed

		3.3	Web application traffic is intercepted and logged with a web application testing tool suite
4	Use current frameworks that identify common software vulnerabilities	4.1	Existing frameworks that identify common software vulnerabilities are investigated
		4.2	Most common web security vulnerabilities are identified
		4.3	Methods to determine injection weaknesses (SQLite) for web applications are described and demonstrated
		4.4	Methods for basic Broken Authentication and Session Management weaknesses for web applications are described and demonstrated
		4.5	Methods for basic Cross Site Scripting (XSS) weaknesses for web applications are described and demonstrated
		4.6	Methods for Insecure Direct Object Reference (IDOR) weaknesses for web applications are described and demonstrated
5	Report web application vulnerabilities	5.1	Technical issues and assigning risk are identified
		5.2	Detailed reproduction steps are outlined
		5.3	Remediation steps are identified
		5.4	Penetration test report is written and presented to relevant technical persons
		5.5	Executive summary is prepared and provided to appropriate persons.

RANGE OF CONDITIONS

Current testing tools for website vulnerabilities provided in the Knowledge Evidence are examples only. Individual tools maybe replaced or added to.

FOUNDATION SKILLS

This section describes language, literacy, numeracy and employment skills that are essential to performance and are not explicitly expressed in the performance criteria of this unit of competency.

Skill	**Description**
Reading skills to:	comprehend technical procedures and documents
Writing skills to:	complete written reports on findings of website security vulnerabilities to appropriate persons
Oral communication skills to:	present findings to relevant technical persons

Technology skills to:	install and interpret software testing tools		
UNIT MAPPING INFORMATION	Code and Title Current Version	Code and Title Previous Version	Comments
	VU23222 Expose website security vulnerabilities	VU21997 Expose website security vulnerabilities	Equivalent

Assessment Requirements

TITLE	Assessment Requirements for **VU23222 - Expose website security vulnerabilities**
PERFORMANCE EVIDENCE	The learner must be able to demonstrate competency in all of the elements, performance criteria and foundation skills in this unit and provide evidence of their ability to • identify how OWASP outcomes can aid in securing an organisations web site • use tools to exploit web site vulnerabilities for two (2) scenarios

KNOWLEDGE EVIDENCE	The learner must be able to demonstrate essential knowledge required to effectively do the task outlined in elements and performance criteria of this unit, manage the task and manage contingencies in the context of the work role. This includes knowledge of:
	• Hypertext Transfer Protocol (HTTP) Structure & Headers & how to secure data
	• Open Web Application Security Project (OWASP) - Secure Headers Project
	• Website Vulnerabilities
	• Structured Query Language (SQL Injection (SQLite)
	• Cross Site Scripting (XSS)
	• Insecure Direct Object References (IDOR)
	• Browser Exploitation Framework (BeEF)
	• testing tools for website vulnerabilities: Examples are:
	  ○ Nikto
	  ○ Directory based (DIRB)
	  ○ Burp Suite
	  ○ Static Application Security testing (SAST)
	  ○ Dynamic Application Security Testing (DAST)
	• Open Web Application Security Project (OWASP) - Framework.

ASSESSMENT CONDITIONS	This unit can be assessed either in the workplace or in a simulated workplace environment. Where the assessment is conducted in a simulated workplace then the range of conditions must reflect a realistic workplace environment. **Resources:** • access to a web testing virtual environment • Open Web Application Security Project (OWASP) Secure Headers Project (*https://owasp.org/www-project-secure-headers/* • computer hardware and relevant software including penetration tools for testing an organisations website for vulnerabilities • relevant documentation including:

	○ workplace procedures ○ codes/standards ○ manuals and reference material **Assessor requirements** Assessors of this unit must satisfy the requirements for assessors in applicable vocational education and training legislation, frameworks and/or standards.

UNIT CODE		**VU23223**	
UNIT TITLE		**Apply cyber security legislation, privacy and ethical practises**	
APPLICATION		This unit describes the performance outcomes, skills and knowledge required to identify the current Australian cyber security legislation and to be cognisance of the interdependence between the key regulators. It requires the ability to apply the current cyber security privacy policies and procedures for an organisation The unit also includes the ethical practices required for employees to conduct themselves professionally both privately and when working for an organisation. The unit is applies to individuals working as cyber security technicians and supports their ability to work ethically and apply professional standards in their place of work. No licensing or certification requirements apply to this unit at the time of accreditation.	
PRE-REQUISITE UNIT(S)		N/A	
ELEMENTS		**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. Assessment of performance is to be consistent with the evidence guide.	
1	Review the cyber security legislative and regulatory landscape for Australian organisations	1.1	Current Federal, State & Territory, and sector specific cyber security legislation is identified
		1.2	International legislation that impacts Australian organisations is identified
		1.3	Interdependencies between various legislative instruments, key regulators and their impact to Australian organisations is investigated and clarified
		1.4	Current reforms in privacy, consumer and surveillance legislation are identified
2	Examine an organisations policies and procedures for compliance with relevant standards	2.1	An organisations policies and procedures are identified
		2.2	An organisations policies and procedures are reviewed for compliance in accordance with current standards
		2.3	Organisational practises of current policies and procedures are assessed

3	Review the ethical practises and procedures for an organisation	3.1	Ethical practises developed by employees in using red and blue teaming tools are identified
		3.2	Consequences of misuse of skills developed by employees in using red and blue teaming tools in public networks are explained
		3.3	Consequences of unauthorised access t devices are investigated
		3.4	Consequences of using file sharing services and tools to download and bypass copyright of various media or applications is explained
		3.5	An ethical code of practise for cyber security technicians working in an organisation is prepared and implemented

RANGE OF CONDITIONS

Range of references listed in the Knowledge Evidence are examples only. Individual references maybe replaced or added to.

Some FOUNDATION SKILLS

This section describes language, literacy, numeracy and employment skills that are essential to performance and are not explicitly expressed in the performance criteria of this unit of competency.

Skill	**Description**
Reading skills to:	comprehend legislative instruments or cyber security policy and procedures
Writing skills to:	present findings to relevant technical or management persons

UNIT MAPPING INFORMATION	New unit, no equivalent unit

Assessment Requirements

TITLE	Assessment Requirements for **VU23223 - Apply cyber security legislation, privacy and ethical practises**
PERFORMANCE EVIDENCE	The learner must be able to demonstrate competency in all of the elements, performance criteria and foundation skills in this unit and provide evidence of the ability to: Identify relevantcyber security • identify relevant cyber security legislation and regulations to meet two (2) organisations requirements.The two organisations must each be in a different industry sector • assess and prepare a written report on each organisations level of compliance or non-compliance with relevant privacy policies and procedures • identify a minimum of four (4) examples of unethical behaviour by ICT/cyber security technicians within an organisation or privately and explain the potential impact of each example.
KNOWLEDGE EVIDENCE	The learner must be able to demonstrate essential knowledge required to effectively do the task outlined in elements and performance criteria of this unit, manage the task and manage contingencies in the context of the work role. This includes knowledge of: • Commonwealth Legislation. Examples are: o Telecommunications (Interception & Access) Act 1979 o Criminal Code 1995 o Corporations Act 2001 (Cth) on their IT management systems (Australian Securities and Investments Commission (ASIC) Regulatory Guide 104: Licensing: Meeting the general obligations) o Privacy Act 1988 • Australian Regulators. Examples are: o Australian Prudential Regulation Authority **(**APRA) - CPS 234 (Prudential regulator) o Australian Securities and Investments Commission (ASIC) (Corporate Regulator) o Australian Competition and Consumer Commission (ACCC) (Consumer & consumer data rights) o Australian Energy Sector Cyber Security Framework (AESCSF) (Energy regulator) o Protective Service Manual (Australian Government rules for cybersecurity) • International Law and conventions. Examples are: o Budapest convention (Convention on Cyber Crime) o Australian Criminal Code Act 1995) o Payment Card Industry Data Security Standard (PCI DSS) (payment cards) • Global Standards. Examples are:

	○ ISO/IEC 27001 information security management systems ○ AS 27701: 2022 Security techniques – Extension to ISO/IEC 27001 • Organisation privacy policy • Ethics of red and blue team skills – (consequences of using these skills in a live network) • Unauthorised access to devices. Examples are: ○ Jail Breaking devices and the consequences ○ Hacking firmware and the consequences • File sharing services used to download. Examples are: ○ Torrents ○ UseNet - Non Zero Binary (NZB) ○ violating copyright of movies, games, PDF's, e-books, audio books • Cyber security ethical codes of practise
ASSESSMENT CONDITIONS	This unit can be assessed either in the workplace or in a simulated workplace environment. Where the assessment is conducted in a simulated workplace then the range of conditions must reflect a realistic workplace environment. **Resources:** • Access relevant documentation including: ○ workplace procedures (privacy and ethics policies) ○ cyber security legislation ○ relevant codes/standards **Assessor requirements** Assessors of this unit must satisfy the requirements for assessors in applicable vocational education and training legislation, frameworks and/or standards.

UNIT CODE		**VU23224**	
UNIT TITLE		**Identify the implications of cloud-based security services**	
APPLICATION		The unit describes the performance outcomes, skills and knowledge required to identify cyber security implications of using cloud-based services and develop an understanding of cloud architecture and design. It requires the ability to successfully maintain and secure cloud service and troubleshoot common cyber security issues related to managing cloud environments This unit is applies to individuals working as cyber security technicians and support their ability to work with cloud based security systems No licensing or certification requirements apply to this unit at the time of accreditation	
PRE-REQUISITE UNIT(S)		N/A	
ELEMENTS		**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. Assessment of performance is to be consistent with the evidence guide.	
1	Investigate testing in cloud-based environments	1.1	Testing techniques for cloud environments are identified
		1.2	Limitations of testing techniques across different cloud environments are explained
		1.3	Procedures for gaining approval to test are identified and applied
		1.4	Sandboxes for cloud infrastructure using two cloud services are created
2	Investigate security controls to cloud-based infrastructure	2.1	Approaches to securing cloud deployments are identified
		2.2	Cloud security services are examined
		2.3	Security services to meet a business needs are selected
3	Secure access to cloud resources	3.1	Access controls to meet business needs are identified and configured
		3.2	Testing methods are identified and applied against access controls

4	Secure access to storage	4.1	Storage controls to meet business needs are identified and configured
		4.2	Testing methods are identified and applied against storage controls
5	Investigate mechanism and techniques used to operate and support cloud environments	5.1	Security monitoring in the cloud is examined
		5.2	Monitoring services to meet business needs are selected
		5.3	Logging, monitoring and alerting to protect cloud environments are configured
		5.4	Simulated attacks to test monitoring services are applied

RANGE OF CONDITIONS

Range of examples provided in the Knowledge Evidence for various items may be replaced or added to.

FOUNDATION SKILLS

This section describes language, literacy, numeracy and employment skills that are essential to performance and are not explicitly expressed in the performance criteria of this unit of competency.

Skill	Description
Reading skills to:	interpret documented material and procedures
Writing skills to:	document incidents
Oral communication skills to:	report on incidents succinctly and effectively
Technology skills to:	install and demonstrate various cloud-related technologies with appropriate policies

UNIT MAPPING INFORMATION	New unit, no equivalent unit.

Assessment Requirements

TITLE	Assessment Requirements for **VU23224 - Identify the implications of cloud-based security services**
PERFORMANCE EVIDENCE	The learner must be able to demonstrate competency in all of the elements, performance criteria and foundation skills in this unit and provide evidence of their ability to: • implement appropriate security controls to managing risk in a cloud based environment • identify and troubleshoot common cloud based security problems • demonstrate mechanisms to operate and support cloud environments
KNOWLEDGE EVIDENCE	The learner must be able to demonstrate essential knowledge required to effectively do the task outlined in elements and performance criteria of this unit, manage the task and manage contingencies in the context of the work role. This includes knowledge of: • Cloud architecture and models. Examples are: o public o private o hybrid o Platform as a Service (PaaS) o Software as a Service (SaaS) o Infrastructure as a Service (IaaS) o sovereignty • Cloud environment limitations. Examples are: o auto-scaling o horizontal o bursting and vertical scaling o cluster o geo-locations o high availability network functions • Testing techniques for cloud environments. Examples are: o vulnerability o penetration o performance regression o usability o functional • Limitations of testing techniques across different cloud environments. Examples are: o Staging

	○ Production ○ Disaster Recovery (DR) ○ Quality Assurance (QA) ○ Development ○ Blue-green • Mechanisms to secure cloud services. Examples are: ○ firewall ○ Web Application Firewall (WAF) ○ Application Delivery Controller (ADC) ○ Data Loss Prevention (DLP) ○ Network Access Controller (NAC) ○ Domain Name System (DNS) over Hyper Text Transfer Protocol Secure (HTTPS) (DoH) ○ DNS over Transport Layer Security (TLS) (DoT) ○ Domain Name System Security Extensions (DNSSEC) ○ tunnelling techniques: Distributed Denial-of-Service (DDoS) protection ○ network segmentation types: ▪ micro ▪ tiering ▪ generic network virtualization encapsulation • Application security and Operating System (OS) controls • Compliance controls to protect data. Examples are: ○ Cloud Access Security Broker (CASB) ○ Data Loss Prevention (DLP) ○ Segmentation ○ data management ○ access controls ○ classification ○ encryption • Logging, alerting and monitoring tools. Example are: ○ collectors ○ analysis ○ categorization ○ audits ○ automation ○ baselines ○ tagging ○ scrubbing • Cloud environment policies and procedures. Examples are: ○ patching virtual machines (VMs) ○ hypervisors

	○ virtual appliances ○ life-cycle management ○ backups ○ reporting • Disaster recovery in cloud environments. Examples are: ○ restoration ○ replication ○ Recovery Point Objective (RPO) ○ Recovery Time Objective (RTO) ○ Service Level Agreement (SLA) ○ playbook ○ failback ○ failover • Cloud migration strategies. Examples are: ○ physical to virtual ○ virtual to virtual ○ cloud to cloud • Cloud environment troubleshooting issues. Examples are: ○ privilege ○ authentication ○ authorisation ○ Public Key Infrastructure (PKI) policy misconfigurations ○ failed security appliances • Cloud deployment troubleshooting issues. Examples are: ○ connectivity issues with Cloud Service Provider (CSP) and Internet Service Provider (ISP) ○ performance degradation ○ misconfigured templates ○ latency ○ memory management ○ capacity issues ○ incorrect tagging ○ resource utilisation issues
ASSESSMENT CONDITIONS	This unit can be assessed either in the workplace or in a simulated workplace environment. Where the assessment is conducted in a simulated workplace then the range of conditions must reflect a realistic workplace environment. **Resources:** • access to cloud based environments **Assessor requirements**

	Assessors of this unit must satisfy the requirements for assessors in applicable vocational education and training legislation, frameworks and/or standards.

UNIT CODE		**VU23225**	
UNIT TITLE		**Investigate Windows security features**	
APPLICATION		This unit describes the performance outcomes skills and knowledge required to investigate the fundamentals of Windows security features. It requires the ability to comprehend the basic architecture of Windows, identify security features such as log files, instrumentation and how a basic attack might occur. The unit includes tools to collect security data centrally and query it to identify potential threats. This unit applies to individuals working as cyber security technicians either alone or as part of a team. No licensing or certification requirements apply to this unit at the time of accreditation.	
PRE-REQUISITE UNIT(S)		N/A	
ELEMENTS		**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. Assessment of performance is to be consistent with the evidence guide.	
1	Examine the structure of the Windows Operating System	1.1	File system formats and layouts are identified
		1.2	Purpose and structure of the registry is examined
		1.3	Program execution in the form of processes and threads is examined
		1.4	Role of the Dynamic Link Loader (DLL) is explained
		1.5	Role of the task scheduler is identified and demonstrated
2	Examine System Administration tools	2.1	Setting administration privileges is demonstrated
		2.2	Windows event logs are identified
		2.3	Windows Management Interface (WMI) is explained
3	Investigate tools used to examine basic Windows attacks	3.1	Tools to detect malware attacks are investigated
		3.2	Malware that reappears after being deleted is identified and exposed

		3.3	Common malware hiding techniques are identified and explained
4	Investigate the function and role of a Security Operation Centre (SOC) and Security Information Event Management (SIEM) tool	4.1	Types of SOC models are identified
		4.2	Central storage of log files is defined
		4.3	SIEM tool structure is defined
		4.4	Commands to use a SIEM tool are demonstrated
		4.5	Process to import log files to a SIEM tool is demonstrated
5	Examine methods to collect data from multiple end points into a SIEM tool	5.1	Log files created on a Windows end point are identified
		5.2	Importing log files from a Windows client to a SIEM tool is demonstrated
		5.3	Basic threat hunting is performed
		5.4	Process of querying the data in the SIEM tool is explained
6	Implement mitigation strategies for threats	6.1	Sources of mitigation strategies are identified
		6.2	Mitigation strategies on detected threats are applied

RANGE OF CONDITIONS

Optional Field

N/A

FOUNDATION SKILLS

This section describes language, literacy, numeracy and employment skills that are essential to performance and are not explicitly expressed in the performance criteria of this unit of competency.

Skill	**Description**
Reading skills to:	comprehend technical procedures and documents
Technology skills to:	import and/or load tools to investigate threats and malware attacks

UNIT MAPPING INFORMATION	New unit, no equivalent unit

Assessment Requirements

TITLE	Assessment Requirements for **VU23225 - Investigate Windows security features**
PERFORMANCE EVIDENCE	The learner must be able to demonstrate the ability to complete the tasks outlined in the elements, performance criteria and foundation skills in this unit and provide evidence of the ability to: • identify the structure of the Windows operating structure • exploit Windows vulnerabilities • implement Windows operating system features to mitigate threats and malware interference

KNOWLEDGE EVIDENCE	The learner must be able to demonstrate essential knowledge required to effectively do the task outlined in elements and performance criteria of this unit, manage the task and manage contingencies in the context of the work role. This includes knowledge of:
	• Windows structure:
	  ○ file formats & layouts
	  ○ event logs
	  ○ registry
	  ○ program execution
	• System administration privileges
	• Windows Management Interface (WMI)
	• Security Operation Centre (SOC) types
	• Security Information Event Management (SIEM) features and operation
	• Windows log files
	• Importing log files into a SIEM
	• Threat hunting
	• Mitigation strategies for types of incidents

ASSESSMENT CONDITIONS	This unit can be assessed either in the workplace or in a simulated workplace environment. Where the assessment is conducted in a simulated workplace then the range of conditions must reflect a realistic workplace environment.
	Resources:
	• access to virtual lab environment including Virtual Windows machines & SIEM tool
	• relevant documentation including:
	  ○ workplace procedures
	  ○ codes/standards
	  ○ manuals and reference material
	Assessor requirements

	Assessors of this unit must satisfy the requirements for assessors in applicable vocational education and training legislation, frameworks and/or standards.

UNIT CODE		**VU23226**	
UNIT TITLE		**Test concepts and procedures for cyber exploitation**	
APPLICATION		This unit describes the performance outcomes, skills and knowledge required to implement testing procedures for systems in an organisation. It requires the ability to apply a treatment of exploit-based intrusions and defensive techniques using various exploitation testing tools. This unit applies to individuals working as cyber security technicians either alone or as part of a team. No licensing or certification requirements apply to this unit at the time of accreditation.	
PREREQUISITE UNIT		VU23215 – Test concepts and procedures for cyber security	
ELEMENTS		**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. Assessment of performance is to be consistent with the evidence guide.	
1	Investigate the use of exploit testing frameworks	1.1	Frameworks for managing executable cyber security tests based on known vulnerabilities are investigated
		1.2	Known vulnerability repositories and the methods of downloading and executing exploits are examined
		1.3	Exposure to methods of building exploit payloads are identified
		1.4	Methods of creating shells for a range of environments are identified and their uses explained
		1.5	Methods of uploading and downloading files from targets are investigated
		1.6	Deliberate flaws in open source exploits are identified and remediations are explored
2	Interpret exploits using Tactics, Techniques and Procedures (TTP) exploitation	2.1	Common TTP frameworks are identified
		2.2	Practical application of a representative selection of exploits are assessed to determine exploit mapping to a commonly used TTP framework
		2.3	Common vulnerability enumeration (CVE) and common weakness enumeration (CWE) frameworks are examined and their relationship to TTP frameworks are investigated

3	Demonstrate the use of enumeration tools and techniques to identify exploits	3.1	Enumeration tools and techniques for identifying suitable exploits are identified
		3.2	Range of accessible services and tools are used to enumerate a system remotely
		3.3	Enumeration of a target from a foothold or user shell is undertaken to identify exploitation strategies for gaining root access
		3.4	Conditions necessary for an exploit to succeed are identified and tests are investigated
		3.5	Potential exploits in web sites are identified
		3.6	Tools and capabilities built into a target environment to enumerate targets stealthily are applied
4	Investigate the privilege models used in common operating environments	4.1	Method by which access is controlled in common operating environments is explored
		4.2	Ways in which to architect an infiltrated network for security is investigated
		4.3	Use of privileges in common operating environments, and how they are used to protect against exploitation are investigated
		4.4	Ways in which privileges might be misconfigured are identified
		4.5	Ways in which privileges can be used to enable an attacker to escalate the privileges in a normal user shell is investigated
5	Investigate the effectiveness of real time defences	5.1	Common technologies to defend workstations and servers against malware are identified and applied
		5.2	Effectiveness of defences against a range of exemplar attacks are examined
		5.3	Methods of defence evasion are identified and the effectiveness of obfuscation and encryption is investigated
		5.4	Effectiveness of evasive techniques against the different defences is investigated

RANGE OF CONDITIONS

Range of examples provided in the Knowledge Evidence for various items may be replaced or added to.

FOUNDATION SKILLS

This section describes language, literacy, numeracy and employment skills that are essential to performance and are not explicitly expressed in the performance criteria of this unit of competency.

Skill	Description
Problem solving skills to:	explore and interpret results from a range of investigations for remediation's of cyber exploits
Writing skills to:	generate appropriate reports
Self-management skills to:	undertake various investigations into the treatment of exploit-based intrusions and defensive techniques using various exploitation testing tools.

UNIT MAPPING INFORMATION	New unit, no equivalent unit.

Assessment Requirements

TITLE	Assessment Requirements for **VU23226 - Test concepts and procedures for cyber exploitations**
PERFORMANCE EVIDENCE	The candidate must demonstrate the ability to complete the tasks outlined in the elements, performance criteria and foundation skills of this unit and provide evidence of their ability to: • demonstrate testing procedures for systems and apply a treatment of exploit-based intrusions and defensive techniques using exploitation testing tools for two (2) scenarois.

KNOWLEDGE EVIDENCE	The candidate must be able to demonstrate essential knowledge required to effectively do the task outlined in elements and performance criteria of this unit, manage the task and manage contingencies in the context of the work role. This includes knowledge of:
	• Zero trust networking
	• Enumeration tools. Examples are:
	  ○ Linux Privilege Escalation Awesome Script (LinPEAS)
	  ○ Windows Privilege Escalation Awesome Script (WinPEAS)
	  ○ Windows Exploit Suggester
	• Exploit payloads. Examples are:
	  ○ Aspx shells
	  ○ Command shells
	  ○ Php shells
	  ○ Malicious jpgs
	• Exploit repositories. Examples are:
	  ○ ExploitDB
	  ○ Searchsploit
	  ○ Metasploit search
	• Exploit techniques. Examples are:
	  ○ exploitation of Linux Sudo
	  ○ exploitation of Linux Set User Identification (SUID) and Set Group Identification (SGID)
	  ○ exploitation of Windows unquoted service paths
	  ○ password spraying
	• Selected exploits:
	  ○ one against an operating system
	  ○ one against an application
	• Testing tools. Examples are:
	  ○ Kali
	  ○ Metasploit
	  ○ Metasploit Framework (MSFvenom)
	  ○ John the Ripper
	  ○ Hydra
	  ○ Structured Query Language (SQL) map
	  ○ Jhead (or equivalent)

	• MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) framework

ASSESSMENT CONDITIONS	This unit can be assessed either in the workplace or in a simulated workplace environment. Where the assessment is conducted in a simulated workplace then the range of conditions must reflect a realistic workplace environment.
	Resources:
	• access to virtualisation testing environment
	• access to exploitation testing and enumeration tools
	• workplace procedures
	• relevant documentation including:
	  ○ codes
	  ○ standards
	  ○ manuals
	Assessor requirements
	Assessors of this unit must satisfy the requirements for assessors in applicable vocational education and training legislation, frameworks and/or standards.