22610VIC

Advanced Diploma of Cyber Security

Version # 1

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

Accredited for the period: 1st April 2023 to 31st March 2028

Table of contents

Section A – Copyright and course classification information

1. Copyright owner of the course	Copyright of this course is held by the Department of Education and Training, Victoria. © State of Victoria (Department of Education and Training) 2022
2. Address	Executive Director Higher Education and Workforce Division Higher Education and Skills Department of Education and Training (DET) GPO Box 4367 Melbourne Vic 3001 Organisational Contact: Manager, Training and Learning Products Unit Portfolio Alignment Branch Higher Education and Workforce Division Higher Education and skills Department of education and Training (DET) Telephone: 131823 Email: *course.enquiry@education.vic.gov.au* **Day-to-Day contact:** Curriculum Maintenance Manager (CMM) CMM Engineering Industries Box Hill Institute Private Bag 2014 Box Hill, Victoria 3128 Telephone: (03) 9286 9934 Email: *steven.bryant@boxhill.edu.au*
3. Type of submission	This submission is for re-accreditation of: **22445VIC Advanced Diploma of Cyber Security**
4. Copyright acknowledgement	The following unit of competency: BSBTWK502 – Manage team effectiveness has been imported from the **BSB – Business Services Training Package** administered by the Commonwealth of Australia. © Commonwealth of Australia The following units of competency: ICTCLD601 – Develop cloud computing strategies for business ICTCYS612 – Design and implement virtualised cyber security infrastructure for organisations 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

	ICTNWK547 - Manage system security on operational systems ICTNWK553 – Configure enterprise virtual computing environments ICTNWK619 – Plan, configure and test advanced server based security ICTNWK620 – Design and implement wireless network security ICTPRG549 – Apply intermediate object-oriented language skills ICTPRG614 – Create cloud computing services ICTSAS524 – Develop, implement and evaluate an incident response plan ICTSAS526 – Review and update disaster recovery and contingency plans have been imported from the **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 (Department of Education and Training) 2022. This work is licensed under a Creative Commons Attribution-No Derivatives 4.0 International licence (see *Creative Commons* for more information). You are free to re-use the work under the licence, on the condition that you credit the State of Victoria (Department of Education and Training), provide a link to the licence, indication if changes were made, and comply with all other licence terms. You must not distribute modified material. **Request for other use should be addressed to:** Executive Director Higher Education and Workforce Division Higher Education and Skills Department of Education and Training (DET) GPO Box 4367 Melbourne Vic 3001 Email: *course.enquiry@education.vic.gov.au* Copies of this publication can be downloaded free of charge from the *DET website.*
6. Course accrediting body	Victorian Registration and Qualifications Authority
7. AVETMISS information	**ANZSCO code** Australian and New Zealand Standard Classification of Occupations 262116 – Cyber Security Analyst **ASCED Code**

	Field of Education 0299 – Other Information Technology **National course code** 22610VIC
8. Period of accreditation	1st April 2023 to 31st March 2028

CC BY ND

Section B – Course information

1. Nomenclature	Standard 4.1 and 5.8 AQTF 2021 Standards for Accredited Courses
1.1 Name of the qualification	Advanced Diploma of Cyber Security
1.2 Nominal duration of the course	825 – 1340 hours
2. Vocational or educational outcomes	**Standard 5.1 AQTF 2021 Standards for Accredited Courses**

2.1 Outcome(s) of the course	The vocational outcomes for the Advanced Diploma of Cyber Security are:
	• Manage and maintain cyber security in an organisation which includes:
	  ○ monitoring the risk of cyber security attacks
	  ○ gathering, analysing and interpreting threat data
	  ○ protecting critical infrastructure and configuring security devices
	  ○ evaluating and implementing appropriate security software
	  ○ implementing and using a range of tools and procedures to mitigate cyber security threats
	  ○ protecting an organisation from insider security breaches
	  ○ developing systems to minimise network vulnerabilities and risks
	  ○ developing cloud computing strategies
	• coordinate security projects which could include both internal and external expertise and resources
	• ensure an organisation's security policies, processes, procedures and codes of practice are consistent and in-line with relevant security standards, laws and codes of practice.

2.2 Course description	The Advanced Diploma of Cyber Security provides graduates with the knowledge and skills to enable them to manage and maintain cyber security in an organisation. Graduates of the course will be able to seek employment as cyber security para professionals in a range of commercial enterprises/organisations and government bodies seeking to improve and maintain their cyber security or, to work independently as a freelance cyber security analyst.

3. Development of the course	Standards 4.1, 5.1, 5.2, 5.3 and 5.4 AQTF 2021 Standards for Accredited Courses
3.1 Industry, education, legislative, enterprise or community needs	The Australian 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". *https://www.cyber.gov.au › acsc › reports-and-statistics* Ongoing availability of the Advanced Diploma of Cyber Security also aligns with Victoria's State Government Cyber Strategy: (*www.vic.gov.au/victorias-cyber-strategy-2021-threat-environment)* by providing quality training that leads to cyber employment opportunities in both government and non-government enterprises. Although much has been achieved in recent years the demand for personnel with cyber security knowledge and skills continues to remain high. 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 continued to expand the need for people with the knowledge and skills to identify, analyse, manage and prevent cyber interference and attacks. It is for this reason members of the Course Steering Committee who guided the review and redevelopment of the Certificate IV in Cyber Security, continued to volunteer their time to guide the review for reaccreditation of the Advanced Diploma of Cyber Security. It is acknowledged the Certificate IV provides an excellent grounding for persons who are seeking employment as cyber security technicians. The Certificate IV is also an ideal prerequisite qualification for entry into the Advanced Diploma. The Advanced Diploma builds on the Certificate IV by providing a higher level of knowledge and skills to enable graduates to seek employment as

cyber security practitioners. A cyber security practitioner is able to manage security projects, utilise advanced processes to access and analyse data to deal with cyber interference, plan and conduct security risk assessment of an organisation and equipped to provide a leadership role in a security team environment.

In addition to the core component, the Advanced Diploma's course structure includes a range of streams to enable participants to specialise in one or more security streams which now include a cloud security stream.

The Victorian Government, Department of Education and Training (DET) enrolment data indicates steady growth for the past four (4) years. Enrolments are expected to further increase due to the significant number of students completing the Certificate IV in Cyber Security.

DET enrolment figures are:

2019 = 29 enrolments

2020 = 76 enrolments

2021 = 83 enrolments

2022 = 58 enrolments (as @ 05/2022)

Currently six (6) Victorian public provides have the course on their scope of registration. The course is also delivered in NSW and QLD.

The review of 22445VIC - Advanced Diploma of Cyber Security was overseen by a Course Steering Committee (CSC) made up of the following personnel:

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 (NY, USA)
Matt Carling	National Cybersecurity Advisor Cisco Systems Inc.
Damian Manuel	Chief Executive Officer Australian Information Security Association (AISA)
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
Stephen Besford	RTO Cyber Security Course Adviser

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 (Course writer)	Project Officer, CMM – Engineering Industries Box Hill Institute
Jo Cave	Head of Cyber and Digital Transformation Programs Victoria University Polytechnic
Bavita Gupta and Steven Cahill	Digital Skills and Concepts Department Chisholm Institute

This course:

- does not duplicate, by title or coverage, the outcomes of an endorsed training package qualification
- 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

As part of the re-accreditation process each enterprise (VU coded) unit was reviewed by one or more subject matter expert (SME) and where required, updated to ensure currency. For some updated units the title has been amended to better reflect the unit revised content.

A new unit VU23309 - Undertake vulnerability and penetration testing for information technology infrastructure, has been added to the Penetration Testing Stream and one of the existing three units (VU23301 - Manage penetration testing processes for an organisation) has been significantly revised and given a new title. This unit is now a prerequisite to units VU23302 and VU23309.

In addition, a new stream to address Cloud Security requirements has been added to the course structure. The new stream contains one revised existing (VU coded) unit (VU23290) and one new VU coded unit (VU23307) and two imported units ICTCLD601 and ICTPRG614).

A new VU unit VU23308 covering Active Directory security concepts was added to the General Stream. Unit VU22258 - *Design and implement a virtual cyber security infrastructure for an organisation,* in the Security Engineering Stream of the superseded course has now been replaced with ICTCYS612 with a similar title.

Each imported unit has been checked to ensure the current version is included and reviewed for relevance to the vocational outcomes of the up dated qualification. As a consequence unit ICTNWK531 *Configure an internet gateway* was deleted.

RTO feedback indicated a preference for greater flexibility in unit choice but retaining the total number of units. This request was supported by the CSC and achieved by reducing the core component of the course from 9 to 5 units and increasing the required number of electives from 11 to 15 units. The total number of units required to complete for the qualification remains at 20 units.

The course 22610VIC Advanced Diploma of Cyber Security supersedes and is deemed *not equivalent* to 22445VIC Advanced Diploma of Cyber Security due to changes made to the core component of the course.

Refer to the **Transition Table** below for a detailed unit by unit comparison between the new and superseded course.

Transition Table:

22445VIC Advanced Diploma of Cyber Security	22610VIC Advanced Diploma of Cyber Security	Relationship
VU22240 Communicate cyber security incidents within the organisation	VU23288 Communicate cyber security incidents within the organisation	Equivalent
VU22241 Interpret and utilise key security frameworks, policies and procedures for an organisation	VU23289 Interpret and utilise key security frameworks, policies and procedures for an organisation	Equivalent
VU22242 Assess and secure cloud services	VU23290 Assess and secure cloud services	Equivalent
VU22243 Develop software skills for the cyber security practitioner	VU23291 Develop software skills for the cyber security practitioner	Not equivalent
VU22244 Implement best practices for identity management	VU23292 Configure identity management processes and procedures for an organisation	Not equivalent
VU22245 Plan and implement a cyber security project	VU23293 Plan and implement a cyber security project	Equivalent
VU22246 Evaluate an organisation's compliance with relevant cyber security standards and law	VU23294 Identify and monitor an organisation's cyber security legal compliance requirements	Equivalent
VU22247 Acquire digital forensic data from workstations	VU23295 Gather and validate digital forensic data from workstations	Equivalent
VU22248 Acquire digital forensic data from mobile devices	VU23296 Gather and validate digital forensic data from mobile devices	Equivalent
VU22249 Perform a security risk assessment for an organisation	VU23297Plan and conduct a security risk assessment for an organisation	Equivalent
VU22250 Respond to cyber security incidents	VU23298 Implement processes and procedures to deal with cyber security incidents	Equivalent
VU22251 Gather, analyse and interpret threat data	VU23299 Utilise tools to gather and interpret data anomalies	Equivalent
VU22252 Implement cyber security operations	VU23300 Detect and respond to cyber security threats	Equivalent
VU22253 Undertake penetration testing of the security infrastructure for an organisation	VU23301 Manage penetration testing processes for an organisation	Not equivalent

Transition Table:

22445VIC Advanced Diploma of Cyber Security	22610VIC Advanced Diploma of Cyber Security	Relationship
VU22254 Undertake advanced penetration testing for web site vulnerability	VU23302 Perform advanced penetration testing for web site vulnerabilities	Not equivalent (Pre-requisite added)
VU22255 Evaluate threats and vulnerabilities of Internet of Things (IoT) devices	VU23303 Develop mitigation strategies for Internet of Things devices	Equivalent
VU22256 Protect critical infrastructure for an organisation	VU23304 Protect industrial networks and operational technology for an organisation	Not equivalent
VU22257 Configure security devices for an organisation	VU23205 Select and configure security devices for an organisation	Equivalent
VU22258 Design and implement a virtualised cyber security infrastructure for an organisation		Deleted
	ICTCYS612 Design and implement virtualised cyber security infrastructure for organisations	Newly imported unit
VU22259 Utilise design methodologies for security architecture	VU23306 Design security architecture for an organisation	Equivalent
BSBWOR502 Lead and manage team effectiveness	BSBTWK502 Manage team effectiveness	Equivalent
ICTNWK525 Configure an enterprise virtual computing environment	ICTNWK553 Configure enterprise virtual computing environment	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
ICTNWK513 Manage system security	ICTNWK547 Manage system security on operational systems	Equivalent
ICTNWK607 Design and implement wireless network security	ICTNWK620 Design and implement wireless network security	Equivalent
ICTSAS501 Develop, implement and evaluate an incident response plan	ICTSAS524 Develop, implement and evaluate an incident response plan	Equivalent

Transition Table:

22445VIC Advanced Diploma of Cyber Security	22610VIC Advanced Diploma of Cyber Security	Relationship
ICTSAS505 Review and update disaster recovery and contingency plans	ICTSAS526 Review and update disaster recovery and contingency plans	Equivalent
ICTTEN811 Evaluate and apply network security	ICTNWK546 Manage network security	Equivalent
ICTNWK531 Configure an internet gateway		Deleted
	VU23307 Identify the implications of cloud based security services	New unit
	VU23308 Identify Active Directory security concepts	New unit
	VU23309 Undertake vulnerability and penetration testing for information technology infrastructure	New unit
	ICTCLD601 Develop cloud computing strategies for business	Newly imported unit
	ICTPRG614 Create cloud computing services	Newly imported unit
	ICTNWK619 Plan, configure and test advanced server based security	Newly imported unit
	ICTPRG549 Apply intermediate object-oriented language skills	Newly imported unit

4. Course outcomes	Standards 5.5, 5.6 and 5.7 AQTF 2021 Standards for Accredited Courses
4.1 Qualification level	This course is aligned with Level 6 of the Australian Qualifications Framework (AQF) in that: **Knowledge:** Graduates will have a specialised and integrated technical and theoretical knowledge with depth in the field of cyber security. **Skills:** Graduates of the Advanced Diploma will have: • Cognitive and communication skills to identify, analyse and act on cyber security risks, threats and incidents in an organisation • Cognitive and communication skills to transfer knowledge and skills to others concerning cyber security risks in workplace practices • demonstrate specialised knowledge in mitigation strategies • Cognitive and communication skills to formulate responses to complex cyber security problems such as protecting critical infrastructure • Wide-ranging specialised technical, creative or conceptual skills to express ideas and perspectives on compliance issues and design methodologies to improve an organisation's cyber security **Application of knowledge and skills:** Graduates of the Advanced Diploma of Cyber Security will demonstrate the application of knowledge and skills: • With depth in areas of organisational data security in a context subject to ongoing change • With initiative and judgement plan, design and manage cyber security projects with some direction • To adapt a range of fundamental principles and complex techniques to known and unknown cyber security situations • Across a broad range of technical cyber security functions with accountability for personal and/or team outputs within an organisational context The **Volume of Learning** for the Advanced Diploma of Cyber Security is typically 1.5 - 2 years. This incorporates structured training delivery and opportunities for practice and reinforcement of skills including, self-directed study, research, project work and written assignments.

4.2 Foundation skills

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.

Skill	Description
Reading skills to:	• interpret and review complex information from reference texts, vendor catalogues and websites associated with cyber security
Writing skills to:	• write technical reports that include analysis and/or research • 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 • use correct cyber security terminology and language appropriate to the situation and target audience
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 complex technical 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:	• make modification to work plans and schedules to overcome unforeseen difficulties or developments • respond appropriately to changes in equipment, standard operation procedures and the working environment • take appropriate actions in a diverse range of cyber security incidents • provide leadership during unforeseen cyber security activities
Teamwork skills to:	• collaborate with others and work effectively in team problem solving activities • work with diverse range of people within 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 • delegate and supervise work where appropriate
Self-management skills to:	• interpret and apply relevant enterprise procedures • establish and follow own work plans and schedules • manage time and priorities to meet work completion targets • ensure work activities are compliant with legislation, codes of practices national standards and company policy • • evaluate and monitor own work performance
Technology skills to:	• use testing software and tools to perform risk assessment and to

		protect critical infrastructure and systems • implement and monitor the application of security software • use security protection devices and software • secure cloud services • perform digital forensic investigation on workstations and mobile devices
	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

4.3 Recognition given to the course (if applicable)	Not applicable
4.4 Licensing/regulatory requirements (if applicable)	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 *22610VIC Advanced Diploma of Cyber Security* the learner must successfully complete a total of twenty (20) units comprising: • Five (5) core units • Fifteen (15) elective units which are to be selected as follows: o a minimum of two (2) units must be selected from each of the five (5) elective streams o the remaining five (5) units can be selected from any of the five (5) elective streams and/or from an endorsed Training Package or accredited course at Diploma/Advanced Diploma level. The units must be consistent with the vocational outcomes of the course and must not duplicate the core or elective units listed. o Where the full qualification is not completed, a VET Statement of Attainment will be issued for each unit successfully completed.

Unit of competency code	Unit of competency title	Field of Education code (six-digit)	Pre-requisite	Nominal hours
Core units: *(All core units must be completed)*				
BSBTWK502	Manage team effectiveness		Nil	60
ICTNWK553	Configure enterprise virtual computing environments		Nil	60
VU23289	Interpret and utilise key security frameworks, policies and procedures for an organisation	02991	Nil	40
VU23293	Plan and implement a cyber security project	02991	Nil	80
VU23294	Identify and monitor an organisation's cyber security legal compliance requirements	02991	Nil	40
			Total core unit hours =	**280**
Elective units: *(Refer above for selection advise)*				
General Stream:				
VU23291	Develop software skills for the cyber security practitioner	02991	Nil	80
VU23292	Configure identity management processes and procedures for an organisation	02991	Nil	40
VU23295	Gather and validate digital forensic data from workstations	02991	Nil	40
VU232996	Gather and validate digital forensic data from mobile devices	02991	Nil	40
VU23297	Plan and conduct a security risk assessment for an organisation	02991	Nil	40
VU23308	Identify Active Directory security concepts	02991	Nil	60
ICTNWK620	Design and implement wireless network security		Nil	60

ICTNWK537	Implement secure encryption technologies		Nil	20
ICTNWK538	Install and maintain valid authentication processes		Nil	25
ICTPRG549	Apply intermediate object-oriented language skills		Nil	60
ICTSAS526	Review and update disaster recovery and contingency plans		Nil	30
Intrusion Analysis Stream:				
VU23288	Communicate cyber security incidents within an organisation	02991	Nil	40
VU23298	Implement processes and procedures to deal with cyber security incidents	02991	Nil	40
VU23299	Utilise tools to gather and interpret data anomalies	02991	Nil	60
VU23300	Detect and respond to cyber security threats	02991	Nil	40
ICTSAS524	Develop, implement and evaluate an incident response plan		Nil	30
ICTNWK547	Manage system security on operational systems		Nil	50
Penetration Testing Stream:				
VU23301	Manage penetration testing processes for an organisation	02991	Nil	40
VU23302	Perform advanced penetration testing for web site vulnerabilities	02991	VU23301	80
VU23303	Develop mitigate strategies for Internet of Things devices	02991	Nil	40
VU23309	Undertake vulnerability and penetration testing for information technology infrastructure	02991	VU23301	80

Security Engineering Stream:				
VU23304	Protect industrial networks and operational technology infrastructure for an organisation	02991	Nil	40
VU23305	Select and configure security devices for an organisation	02991	Nil	80
VU23306	Design security architecture for an organisation	02991	Nil	40
ICTCYS612	Design and implement virtualised cyber security infrastructure for organisations		Nil	80
ICTNWK544	Design and implement a security perimeter for ICT networks		Nil	60
ICTNWK546	Manage network security		Nil	80
ICTNWK619	Plan, configure and test advanced server based security		Nil	80
Cloud Security Stream:				
VU23290	Assess and secure cloud services	02991	Nil	80
VU23307	Identify the implications of cloud based security systems	02991	Nil	60
ICTCLD601	Develop cloud computing strategies for business		Nil	40
ICTPRG614	Create cloud computing services		Nil	60
			Range of nominal hours for elective units =	**545 - 1060**
			Total range of nominal hours for the course =	**825 - 1340**

Standard 5.11 AQTF 2021 Standards for Accredited Courses

5.2 Entry requirements	The essential requirements for entry into the 22610VIC Advanced Diploma of Cyber Security are: • completion of the superseded (22334VIC) or current (22603VIC) – Certificate IV in Cyber Security or equivalent *or* • minimum of two (2) years cyber security work experience. In addition, applicants should 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 lower than recommended level may require additional support to successfully complete this course.

6. Assessment	**Standard 5.12 AQTF 2021 Standards for Accredited Courses**
6.1 Assessment strategy	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 include: • oral and/or written questioning • inspection of final process outcomes • portfolio of documentary on-site work evidence • practical demonstration of required physical tasks • investigative research and case study analysis. Questioning techniques should not require language, literacy and numeracy skills beyond the level required for course entry. 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	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	Standards 5.12, 5.13 and 5.14 AQTF 2021 Standards for Accredited Courses
7.1 Delivery modes	This course may be delivered either on a full-time or part-time basis or a combination of either full-time or 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. The use of industry experts as guest speakers especially persons with first-hand experience in responding to cyber interference and breaches in their own workplace, may enhance/support delivery for some units e.g. unit VU23298.
7.2 Resources	Workplace and/or training facilities which must simulate real workplace conditions and equipment including: • computers, internet access and cyber security software and tools

	• access to relevant texts, cyber security legislation, policies, guidelines, processes 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. Applicants for this course will gain a credit/s for any training package unit/s successfully completed from previous training which are also included in this qualification. 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**
	The *22610VIC Advanced Diploma of Cyber Security* will be monitored and maintained by the Curriculum Maintenance Manager (CMM) - Engineering Industries. A review of the course will take place at least once during the period of accreditation and will be informed by feedback from: • course participants and graduates • teaching and assessing staff • industry representatives and associations. 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.

Section C – Units of competency

Enterprise units (developed for this course)

VU23288	Communicate cyber security incidents within an organisation
VU23289	Interpret and utilise key security frameworks, policies and procedures for an organisation
VU23290	Assess and secure cloud services
VU23291	Develop software skills for the cyber security practitioner
VU23292	Configure identity management processes and procedures for an organisation
VU23293	Plan and implement a cyber security project
VU23294	Identify and monitor an organisation's cyber security legal compliance requirements
VU23295	Gather and validate digital forensic data from workstations
VU23296	Gather and validate digital forensic data from mobile devices
VU23297	Plan and conduct a security risk assessment for an organisation
VU23298	Implement processes and procedures to deal with cyber security incidents
VU23299	Utilise tools to gather and interpret data anomalies
VU23300	Detect and respond to cybersecurity threats
VU23301	Manage penetration testing processes for an organisation
VU23302	Perform advanced penetration testing for web site vulnerabilities
VU23303	Develop mitigation strategies for Internet of Things devices
VU23304	Protect industrial networks and operational technology infrastructure for an organisation
VU23305	Select and configure security devices for an organisation
VU23306	Design security architecture for an organisation
VU23307	Identify the implications of cloud based security systems
VU23308	Identify Active Directory security concepts
VU23309	Undertake vulnerability and penetration testing for information technology infrastructure

Endorsed Training Package Units:

These units can be download from the national data base *http://training .gov.au*

BSBTWK502	Manage team effectiveness
ICTCLD601	Develop cloud computing strategies for business
ICTCYS612	Design and implement virtualised cyber security infrastructure for organisations
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
ICTNWK547	Manage system security on operational systems
ICTNWK553	Configure enterprise virtual computing environments
ICTNWK619	Plan, configure and test advanced server based security
ICTNWK620	Design and implement wireless network security
ICTPRG549	Apply intermediate object-oriented language skills
ICTPRG614	Create cloud computing services
ICTSAS524	Develop, implement and evaluate an incident response plan
ICTSAS526	Review and update disaster recovery and contingency plans

Unit code	**VU23288**
Unit title	**Communicate cyber security incidents within an organisation**
Application	This unit describes the performance outcomes, skills and knowledge required to communicate the effects of cyber security incidents to appropriate personnel in an organisation. It requires the ability to use communication skills to effectively contribute as a team member dealing with cyber security incidents for an organisation. It also includes gathering and sorting the appropriate information and presenting it to different groups and/or individuals in an organisation. The unit is applies to persons working as cyber security practitioners and supports their ability to communicate effectively in an organisation. No licensing or certification requirements apply to this unit at the time of accreditation
Pre-requisite Unit(s)	Nil

Element		**Performance Criteria**	
Elements describe the essential outcomes of a unit of competency.		Performance criteria describe the required performance needed to demonstrate achievement of the element. Assessment of performance is to be consistent with the assessment requirements.	
1	Compile information on key groups who need to be notified on security breeches	1.1	Information on the organisation's ethical practices and security policies is sought and examined
		1.2	Organisational personnel structure documents are identified and collated
		1.3	Decision making responsibilities for each organisational group are interpreted and clarified
		1.4	Process of escalating an incident to appropriate organisational group/s is identified
		1.5	Negotiation process with appropriate groups to address cyber incidents is implemented
2	Collate information on communication styles	2.1	Different communication styles are identified and compared
		2.2	Appropriate communication style is identified to explain impact of an incident to different organisational groups and individuals
3	Address cyber security incidents	3.1	Data sources to detect incidents are selected
		3.2	Risk impact of the incidents is assessed
		3.3	Functional tasks within the team are allocated
		3.4	Communication expectations within the incident team are determined

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

Range of Conditions

There are no Range of Conditions.

Foundation Skills

Foundation skills essential to performance in this unit, but are *not explicit* in the performance criteria are listed here.

Skill	Description
Reading skills to:	accurately interpret an organisation's policies and procedure documents relating to cyber security incidents
Writing skills to:	prepare technical documentation and reports with appropriate language and detail for the audience
Oral communication skills to:	make presentations to various groups and articulate relevant issues encountered in the work environment

Unit Mapping information	Code and Title Current Version	Code and Title Previous Version	Comments
	VU23288 Communicate cyber security incidents within an organisation	VU22240 Communicate cyber security incidents within the organisation	Equivalent

Assessment Requirements	
TITLE	Assessment Requirements for: **VU23288 - Communicate cyber security incidents within an organisation**
PERFORMANCE EVIDENCE	The candidate must demonstrate the ability to complete the tasks outlined in the elements, performance criteria and foundation skills of this unit, including evidence of the ability to: • use appropriate communication strategies for reporting a cyber security incident to at least two (2) different decision-making groups in an organisation and evaluate their feedback for own improvement.
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: • ethics and communication techniques • process of coordinating and managing an incident • group collaboration and decision making • presentation skills appropriate to decision making group • data gathering processes • identification of data sources • communication styles • organisation roles and responsibilities • organisation policies and procedures • incident response processes • escalation practices • engaging external contractors.
ASSESSMENT CONDITIONS	Knowledge and skills assessment must be in a real or simulated workplace environment. If simulated, it must reflect real workplace conditions with suitable facilities and equipment. Assessment must ensure access to: • relevant computer hardware /software • data sources to detect security incidents • communication and presentation technologies. • decision making groups **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	**VU23289**
Unit title	**Interpret and utilise key security frameworks, policies and procedures for an organisation**
Application	This unit describes the performance outcomes, skills and knowledge required to interpret and utilise key security frameworks, policies and procedures for an organisation. It also includes other bodies that offer resources and support to an organisation to address cyber security risk. It requires the ability to review the resources and information to determine what is appropriate to support the organisation to improve its security infrastructure. The unit applies to persons working as cyber security practitioners who are required to select, interpret and implement existing frameworks, policies and standards in an organisation. No licensing or certification requirements apply to this unit at the time of accreditation
Pre-requisite Unit(s)	Nil

Element		**Performance Criteria**	
Elements describe the essential outcomes of a unit of competency.		Performance criteria describe the required performance needed to demonstrate achievement of the element. Assessment of performance is to be consistent with the assessment requirements.	
1	Collate security frameworks, risk mitigation strategies and other supportive documents	1.1	Key organisations that provide useful cyber security resources to improve an organisation's security capability are identified
		1.2	Key Australian and overseas cyber security incident mitigation strategies that improve an organisation's security are accessed and reviewed
		1.3	Current working frameworks or practices that can support an organisation to improve its security capabilities are identified and assessed
		1.4	Current Australian cyber security legal and ethics documents are identified and reviewed
		1.5	Guidelines for security relating to Internet of Things (IOT) are identified and reviewed
2	Evaluate key information from relevant documents that will support an organisation to improve its security infrastructure	2.1	Australian compliance standards are identified and evaluated for an organisation
		2.2	Compulsory Australian cyber security legal and ethics documents are identified for an organisation
		2.3	Key strategies to mitigate cyber security risks are identified and evaluated
3		3.1	In consultation with relevant personnel, key incident response strategies including plans for an organisation are selected

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

Range of Conditions

Resources and tools are constantly being updated or replaced in this technology space. Where a resource or tool is no longer relevant or supported an updated resource or tool may be selected in its place. Those listed are examples at the time this unit was written.

- Security frameworks, risk mitigation strategies and other supportive documents. Examples are:
    - Australian Signals Directorate (ASD) Essential 8 (eight)
    - relevant aspects of the Australian Cybercrime Act
    - relevant aspects of the Australian Telecommunications Act
    - Outcomes of the Budapest Convention on Cybercrime
    - relevant aspects of the National Institute of Standards and Technology (NIST) cyber security framework
    - relevant aspects from NIST Computer Security Incident Handling Guide
    - relevant aspects of the European Union Agency for Network and Information Security (ENISA)
- Security standards, frameworks and resources. Examples are:
    - ISO/IEC 2700X – especially 27001 Information Security Management Systems
    - Cyber security legislative reform as it affects Treasury, Attorneys General (AG) and Department of Home Affairs (DoHA)

- Control Objectives for Information and Related Technologies (COBIT)
- Information Technology Infrastructure Library (ITIL)
- Open Web Application Security Project (OWASP)
- Cloud Security Alliance (CSA)
- Australian Signals Directorate Information Security Manual ((ASDISM)
- IoT Alliance Australia: Internet of Things Security Guideline

- New technologies in context of industry standards and frameworks. Examples are:
  - Applying Cloud Security Alliance Security, Trust & Assurance Registry (CSA STAR)
  - Information security Manual (ISM - principles).

Foundation Skills

Foundation skills essential to performance in this unit, but are *not explicit* in the performance criteria are listed here.

Skill	Description
Reading skills to:	accurately interpret documents and reports relating to cyber security incidents
Writing skills to:	prepare technical documentation and reports with appropriate language and detail for the audience
Oral communication skills to:	articulate relevant issues in the work environment
Digital literacy skills to:	produce text, graphs and charts using technology to communicate information to others

Unit Mapping information	Code and Title Current Version	Code and Title Previous Version	Comments
	VU23289 Interpret and utilise key security frameworks, policies and procedures for an organisation	VU22241 Interpret and utilise key security frameworks, policies and procedures for an organisation	Equivalent

Assessment Requirements	
TITLE	Assessment Requirements for: **VU23289 - Interpret and utilise key security frameworks, policies and procedures for an organisation**
PERFORMANCE EVIDENCE	The candidate must demonstrate the ability to complete the tasks outlined in the elements, performance criteria and foundation skills of this unit, including evidence of the ability to: • identify and select appropriate security frameworks, adopt incident response processes and cyber security incident mitigation strategies that will improve an organisation's resilience against cyber incidents.
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: • Security frameworks, risk mitigation strategies and other supportive documents. Refer Range of Conditions for examples. • Security standards, frameworks and resources. Refer Range of Conditions for examples. • Legal aspects of relevant standards and procedures • Differences between security frameworks, policies, standards, procedures and guidelines • Policies, standards and procedures effectiveness (continuous improvement) • New technologies in context of industry standards and frameworks. Refer Range of Conditions for examples.
ASSESSMENT CONDITIONS	Knowledge and skills assessment must be in a real or simulated workplace environment. If simulated, it must reflect real workplace conditions with suitable facilities and equipment. Assessment must ensure access to: • security frameworks, legislation, cyber security incident mitigation strategies and other supportive documents for the organisation • real or simulation organisations • relevant computer hardware/software • internet **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	**VU23290**
Unit title	**Assess and secure cloud services**
Application	This unit describes the performance outcomes, skills and knowledge required to apply the principles of operation for the cloud model and cloud services. It requires the ability to categorise and select cloud services for an organisation as well as the ability to examine the security issues relating to cloud data and services. The unit also includes current industry practices that support an organisation to secure its' cloud based data and application services The unit applies to persons working as a cyber security practitioners and are responsible for the security of cloud based services in an organisation. No licensing or certification requirements apply to this unit at the time of accreditation.
Pre-requisite Unit(s)	Nil

Element		**Performance Criteria**	
Elements describe the essential outcomes of a unit of competency.		Performance criteria describe the required performance needed to demonstrate achievement of the element. Assessment of performance is to be consistent with the assessment requirements.	
1	Categorise cloud service, security services and deployment models	1.1	Cloud service models are identified
		1.2	Cloud deployment models are classified
		1.3	Cloud infrastructure is explained
		1.4	Risk assessment for cloud based data services is performed
		1.5	Cloud security services are reviewed
2	Develop a risk management plan for cloud based data storage and services	2.1	Security risks and consequences in accordance with the Australian legislative requirements and relevant standards for cloud based data and services are identified
		2.2	Acceptable and unacceptable risks for cloud based data storage and services are identified
		2.3	For high priority risks of cloud based data storage and services appropriate controls are developed
		2.4	Existing controls to determine the impact on risk occurrence are monitored and modified if required
		2.5	Risk management plan for cloud based data storage and services for the organisation are documented

3	Implement legal and compliance issues of cloud data and services	3.1	Australian legislative requirements and relevant standards relating to cloud based services for the organisation are identified and evaluated
		3.2	Insurance of cloud data and services are recommended to the appropriate organisational bodies
4	Evaluate, select and implement cloud based services for the organisation	4.1	Cloud service providers for the organisation are evaluated and selected
		4.2	Cloud services to access the organisation's data are selected and deployed
		4.3	Deployment of cloud micro-services and containers utilised by an organisation are explained
		4.4	Cloud security services are selected and deployed
		4.5	Cloud Identity and Access Management (IAM) services are evaluated
5	Develop strategies to protect cloud services	5.1	Key personnel tasked to deal with user account management are identified
		5.2	Strategies to secure cloud services are developed for the organisation
		5.3	Back up strategies are developed for the organisation
		5.4	Disaster recovery (DR) strategies are developed for the organisation
		5.5	Strategies for cryptographic key management of cloud services are developed
		5.7	Shared security responsibility models for cloud services are identified
6	Monitor the effectiveness of strategies developed to protect cloud based data and services for the organisation	6.1	Tools used to audit and monitor cloud based services and data are evaluated, selected and deployed
		6.2	Changes to the strategies and tools used to monitor the cloud services and data are presented to appropriate organisational bodies

Range of Conditions

Resources and tools are constantly being updated or replaced in this technology space. Where a resource or tool is no longer relevant or supported an updated resource or tool may be selected in its place. Those listed are examples at the time this unit was written.

- Cloud based storage architectures: Examples are:
    - Infrastructure as a Service (IaaS)
    - Platform as a Service (PaaS)
    - Software as a Service (SaaS)
    - Communication as a Service (CaaS)
    - Mobility as a Service (MaaS)
    - Anything (X) as a service (XaaS)
- Cloud deployment models: Example are:

- public cloud
- private cloud
- single hosted cloud
- multi hosted cloud

- Cloud security services. Examples are:
  - Amazon Web Services (AWS) services
  - Azure services

Foundation Skills

Foundation skills essential to performance in this unit, but are *not explicit* in the performance criteria are listed here.

Skill	Description
Reading skills to:	accurately interpret documents reports relating to cloud services
Writing skills to:	prepare strategic documents and reports relating to cloud services that are appropriate for the intended audience

Unit Mapping information	Code and Title Current Version	Code and Title Previous Version	Comments
	VU23290 Assess and secure cloud services	VU22242 Assess and secure cloud services	Equivalent

Assessment Requirements	
TITLE	Assessment Requirements for: **VU23290 - Assess and secure cloud services**
PERFORMANCE EVIDENCE	The candidate must demonstrate the ability to complete the tasks outlined in the elements, performance criteria and foundation skills of this unit, including evidence of the ability to: • develop a risk strategy for cloud based services, then select and implement cloud based services for an organisation and apply strategies to protect the cloud services.
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: • cloud based storage architectures. Refer Ranges of Conditions for current examples • cloud deployment models. Refer Ranges of Conditions for current examples • cloud security services. Refer Ranges of Conditions for current examples • risk assessment of cloud based data and services • cloud infrastructure (storage, network and computing) • cloud management and monitoring • backup and data recovery (DR) aspects of cloud services • Government certification, accreditation and compliance implications of cloud services • legal and regulatory implications associated with using cloud based data storage (e.g. Records retention requirements) • data privacy issues of cloud services • options of cryptographic key management when using cloud services • data vulnerabilities of cloud based data storage • tools used to access cloud data and their limitations • strategies for protecting data in transit and at rest • secure backup strategies • data sovereignty risks associated with cloud storage
ASSESSMENT CONDITIONS	Knowledge and skills assessment must be in a real or simulated workplace environment. If simulated, it must reflect real workplace conditions with suitable facilities and equipment. Assessment must ensure access to: • real or simulated organisations utilising cloud based services • tools used to audit and monitor cloud based services • relevant reference materials e.g. Australian 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	**VU23291**
Unit title	**Develop software skills for the cyber security practitioner**
Application	The unit describes the performance outcomes, skills and knowledge to examine concepts and operation of how a program is executed on a computer and how programs are developed. It requires the ability to write and execute a program in both a script and a modern programming language. The unit also introduces the concept of frameworks and tools to develop secure code as well as tools that can be used to protect the execution of the program. The unit applies to persons who are working as cyber security practitioners responsible for writing and working with software scripts in a cyber security environment. No licensing or certification requirements apply to this unit at the time of accreditation
Pre-requisite Unit(s)	Nil

Element		**Performance Criteria**	
Elements describe the essential outcomes of a unit of competency.		Performance criteria describe the required performance needed to demonstrate achievement of the element. Assessment of performance is to be consistent with the assessment requirements.	
1	Identify the interplay of hardware and software of a computer when executing a program	1.1	Microprocessor architecture is identified
		1.2	Overview of an assembler instruction set is provided
		1.3	Operation of a program fetching and executing code is described
		1.4	Tools to develop and debug assembly language programs are defined
		1.5	Example of the structure and the compilation of an assembly language program is provided and interpreted
		1.6	Structure and operation of an exe file is examined and described
		1.7	Difference between a programming language that generates an executable file and a programming language that interprets instructions is compared
		1.8	Skills and tools to reverse engineer code are identified
2	Write programs using a modern programming language	2.1	Modern programming languages used in cyber security development applications is investigated
		2.2	Software tools to develop Web pages are identified
		2.3	Components of a programming language development environment are identified
		2.4	Programs that require data entry are written

		2.5	Tools to troubleshoot programs are selected and utilised as required
3	Write and interpret software scripts	3.1	A comparison of common scripting languages used in cyber security code development is performed
		3.2	Process of compiling a modern scripting language to bytecode is performed
		3.3	A script that accepts run time parameters is written
		3.4	Tools to troubleshoot the software script in the demonstration of the program operation are utilised
4	Identify methods and strategies as to how malware code is executed	4.1	Process of malware infecting executable code via extraneous jump instructions is identified and demonstrated
		4.2	Process of malware infecting executable code via stack overflow is identified and demonstrated
		4.3	Process of malware infecting executable code via buffer overruns is identified and demonstrated
		4.4	Other ways in which extraneous code is executed are described
5	Identify principles and practices used to develop secure code	5.1	Strategies and tools to develop secure software are investigated
		5.2	Software development lifecycle (SDLC) is defined
		5.3	Outcomes of the Open Web Application Security Project (OWASP) secure coding practise guide are identified
		5.4	Other tools and frameworks used to develop secure code are investigated
6	Investigate principles and practises to secure code execution	6.1	Operating system tools to secure code are examined
		6.2	Methods to protect and secure code are explained

Range of Conditions

Resources and tools are constantly being updated or replaced in this technology space. Where a resource or tool is no longer relevant or supported an updated resource or tool may be selected in its place. Those listed are examples at the time this unit was written.

- Frameworks to develop secure code. Examples are:
    - Open Web Application Security Project (OWASP) Secure Coding Practises
    - Software Development Life Cycle (SDLC)

Foundation Skills

Foundation skills essential to performance in this unit, but are *not explicit* in the performance criteria are listed here.

Skill	Description

Reading skills to:	accurately interpret documentation on the concepts and operation of how a program is executed on a computer and how programs are developed.

Unit Mapping information	Code and Title Current Version	Code and Title Previous Version	Comments
	VU23291 Develop software skills for the cyber security practitioner	VU22243 Develop software skills for the cyber security practitioner	Not equivalent

CC BY ND

Assessment Requirements	
TITLE	Assessment Requirements for: **VU23291 - Develop software skills for the cyber security practitioner**
PERFORMANCE EVIDENCE	The candidate must demonstrate the ability to complete the tasks outlined in the elements, performance criteria and foundation skills of this unit, including evidence of the ability to: • write, test, troubleshoot and secure two (2) programs one in a script and the other in modern programming language.

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:
	• Fundamentals of computer architecture including:
	  ○ memory structures
	  ○ registers
	  ○ stacks
	  ○ pointers
	  ○ core processing units
	  ○ sub processors:
	  ▪ memory management unit (MMU)
	  ▪ floating point units (FPU)
	• Microprocessor instruction sets including:
	  ○ registers
	  ○ stacks
	  ○ pointers (Index registers)
	  ○ instruction groupings:
	  ▪ arithmetic
	  ▪ logic
	  ▪ data transfer
	  ▪ control
	  ▪ floating point
	• Process of compiling a program
	• Structure of an assembler program
	• Introduction to the procedures to reverse engineer code
	• Tools and environments utilised to write programs
	• Structure and operation of an exe file
	• Software testing methodologies
	• Software troubleshooting techniques
	• Frameworks to develop secure code. Refer Range of condition for examples.
	• Operating systems tools used to protect code

ASSESSMENT CONDITIONS	Knowledge and skills assessment must be in a real or simulated workplace environment. If simulated, it must reflect real workplace conditions with suitable facilities and equipment. Assessment must ensure access to: • Secure Coding Practises *(https://owasp.org/www-pdf-archive/OWASP_SCP_Quick_Reference_Guide_v1.pdf* • computer and networking equipment • relevant software and troubleshooting tools • relevant reference 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	**VU23292**
Unit title	**Configure identity management processes and procedures for an organisation**
Application	This unit describes the performance outcomes, skills and knowledge required to apply strategies to deal with issues associated with fraudulent identity and account compromise. It requires the ability to employ best practices for identity and access management for an organisation The unit applies to cyber security or information technologist practitioners who are responsible for configuring, setting up, monitoring and decommissioning users in an organisation. No licensing or certification requirements apply to this unit at the time of accreditation
Pre-requisite Unit(s)	Nil

Element		**Performance Criteria**	
Elements describe the essential outcomes of a unit of competency.		Performance criteria describe the required performance needed to demonstrate achievement of the element. Assessment of performance is to be consistent with the assessment requirements.	
1	Explore the function and operation of key identity and access management features and operations	1.1	Differences between identities, accounts, access, authorisation and authentication are identified.
		1.2	Function and operation of common authentication services are compared
		1.3	Types of authorisation services are identified
		1.4	Function and operation of access control services are evaluated
		1.5	Privileged account management processes are examined
		1.6	Identification and access management technologies are identified and evaluated
		1.7	Identity and access management documentation processes are performed
		1.8	Current and emerging best practices in password management for the organisation are compared
2	Implement best practices for user account management	2.1	Identity theft and identity fraud methods are evaluated
		2.2	Components of an account management service are defined
		2.3	Fundamentals of secure account management are defined
		2.4	Testing strategies for weak account management are utilised

		2.5	Account management for an organisation is implemented
3	Identify, configure and monitor identity management for an organisation	3.1	Working principles for identity management are examined
		3.2	Components of an identity management service are examined
		3.3	Fundamentals of secure identity management is investigated
		3.4	Differences between Identity Federation and Single Sign On (SSO) are defined
		3.5	Identity management processes are evaluated with key personnel and modified if required to improve security
		3.6	Identity management for an organisation is implemented
4	Identify, configure and monitor authentication and authorisation services for an organisation	4.1	Performance of a selected authentication and authorisation service is monitored
		4.2	Testing strategies for vulnerabilities in authentication and authorisation are developed

Range of Conditions

Resources and tools are constantly being updated or replaced in this technology space. Where a resource or tool is no longer relevant or supported an updated resource or tool may be selected in its place. Those listed are examples at the time this unit was written.

- Authentication services. Examples are:
    - Kerberos
    - session timeout controls
- Authorisation services. Examples are:
    - role-based access control (RBAC)
    - list-based access control (LBAC)
- Testing Strategies for account management. An example is:
    - active directory vulnerabilities (The Most Common Active Directory Security Issues and What You Can Do to Fix Them – Active Directory Security (adsecurity.org
    - session timeout controls

Foundation Skills

Foundation skills essential to performance in this unit, but are *not explicit* in the performance criteria are listed here.

Skill	Description
Reading skills to:	accurately interpret documents and reports relevant to identity management

Writing skills to:	prepare technical documentation with appropriate language and detail for the intended audience
Oral communication skills to:	Liaise with personnel tasked with the responsibility for user account management

Unit Mapping information	Code and Title Current Version	Code and Title Previous Version	Comments
	VU23292 Configure identify management processes and procedures for an organisation	VU22244 Implement best practices for identity management	Not equivalent

Assessment Requirements	
TITLE	Assessment Requirements for: **VU23292 – Configure identity management processes and procedures for an organisation**
PERFORMANCE EVIDENCE	The candidate must demonstrate the ability to complete the tasks outlined in the elements, performance criteria and foundation skills of this unit, including evidence of the ability to: • configure, set up, monitor and decommission at least two (2) users in an organisation.

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:
	• Identity & account management lifecycle including:
	  ○ segregation of duties
	  ○ periodic review
	  ○ default setting and overly permissive account permissions
	  ○ onboarding
	  ○ offboarding
	• identity theft
	• identity fraud
	• identity federation
	• identification and access management technologies such as Blockchain
	• Authentication services. Refer Range of Conditions for examples.
	• Authorisation services. Refer Range of Conditions for examples.
	• Testing Strategies for account management. Refer Range of Conditions for example.
	• Identity management services

ASSESSMENT CONDITIONS	Knowledge and skills assessment must be in a real or simulated workplace environment. If simulated, it must reflect real workplace conditions with suitable facilities and equipment. Assessment must ensure access to: • two users' accounts • computer equipment • networking equipment • 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	**VU23293**
Unit title	**Plan and implement a cyber security project**
Application	This unit describes the performance outcomes, skills and knowledge required to plan and implement a cyber security project. The project can either be created and carried out in a simulated cyber security environment or be an actual workplace cyber security project. It requires the ability to actively contribute to each stage of the project as a team member which includes receiving tasks, designing solutions, solving problems and ensuring delivery of the project within a given timeframe. The project will include using a Cyber Security Operations Centre (CSOC) sandbox or equivalent laboratory environment to demonstrate configuring and testing of firewalls, implementing Intrusion Detection System (IDS) and evaluating and identifying any traffic anomalies. The use of Red and Blue teaming exercises to identify security breaches and apply mitigation strategies to minimise further risk should be included as part of the project. The unit applies to cyber security practitioners who, as part of a team are responsible for the delivery of cyber security projects in an organisation. No licensing or certification requirements apply to this unit at the time of accreditation
Pre-requisite Unit(s)	Nil

Element		**Performance Criteria**	
Elements describe the essential outcomes of a unit of competency.		Performance criteria describe the required performance needed to demonstrate achievement of the element. Assessment of performance is to be consistent with the assessment requirements.	
1	Identify the strategic and operational needs for an organisation during the planning phase	1.1	Strategic and operational needs of the cyber security project during the planning phase are identified
		1.2	Cyber security project's strategic context and requirements are identified
		1.3	Implications of the organisation's strategic and business plans and the projects' output requirements are identified and considered
		1.4	Client requirements and the impact of legislation and industry standards and codes are examined
		1.5	Risk management analysis is conducted and a risk management plan is prepared and documented
2	Support the preparation of the	2.1	Precise specifications and terms of reference for the cyber security project are defined and documented

	project design plan	2.2	Physical and other resources required to support the cyber security project are defined, documented and secured
		2.3	Timelines, schedules and critical paths for the cyber security project, taking into consideration contingencies and planning for time slippages are developed and documented
		2.4	Project budget taking into consideration the cost of the primary project, management of a range of sub-tasks and contingencies is prepared
		2.5	Consultation strategies used to inform clients, contractors and other interested parties of the cyber security project's progress are defined and documented
3	Support the assembly of personnel for the project team	3.1	Required skills needed for the successful completion of the cyber security project are identified
		3.2	Required skills for the cyber security project are mapped against the available personnel
		3.3	Effective communication processes to coordinate work are implemented
		3.4	Clear reporting processes are identified and communicated
		3.5	Modifications and improvements to the cyber security project are considered and implemented
4	Design the sub-task for the project	4.1	Delegated tasks for the project are defined and communicated
		4.2	Action plan for each project sub-task is prepared and where possible tested for functionality
		4.3	Where possible outputs of the sub-task are tested for interconnectivity and functionality
5	Gather resources and test the system design	5.1	Project resources are acquired according to organisational policy
		5.2	Vendor documentation for the equipment purchased is collated
		5.3	Operation and functionality of the acquired equipment to achieve the project outcomes is investigated
		5.4	Project sub-tasks are built, and where appropriate tested for functionality
6	Implement the project solution	6.1	Each sub-task of the project is interconnected and tested for functionality
		6.2	Verification of end to end functionality of the project design is performed and changes are made if required to ensure the design brief is achieved

		6.3	Red and Blue teaming exercises are planned and applied
		6.4	Further testing and modification are undertaken to the system if required to ensure the design brief is achieved
7	Finalise the project and facilitate handover	7.1	Cyber security project is completed in line with the requirements of the project design plan
		7.2	Project handover is undertaken in accordance with organisational procedures to staff responsible for ongoing implementation and maintenance
		7.3	Team members and relevant stakeholders are debriefed concerning the conduct of the project and outcomes achieved
		7.4	Report analysing the strengths and weaknesses of the project design plan and the conduct of the project is prepared
		7.5	If required training for the organisation' staff is prepared and conducted

Range of Conditions

There are no Range of Conditions.

Foundation Skills

Foundation skills essential to performance in this unit, but are *not explicit* in the performance criteria are listed here.

Skill	Description
Reading skills to:	interpret vendor equipment documents and other project related documentation
Writing skills to:	prepare technical documents with appropriate language and detail for the intended audience
Oral communication skills to:	articulate relevant issues with team members and other stakeholders
Teamwork skills to:	effectively contribute to all stages of a cyber security project
Self-management skills to:	be responsible for carrying out own tasks as part of the cyber security project team

Unit Mapping information	Code and Title Current Version	Code and Title Previous Version	Comments
	VU23293 Plan and implement a cyber security project	VU22245 Plan and implement a cyber security project	Equivalent

Assessment Requirements	
TITLE	Assessment Requirements for: **VU23293 - Plan and implement a cyber security project**
PERFORMANCE EVIDENCE	The candidate must demonstrate the ability to complete the tasks outlined in the elements, performance criteria and foundation skills of this unit, including evidence of the ability as part of a team to: • identify the project scope, risk and plan a solution to achieve an appropriate outcome for the client • implemented the solution in part or full in a virtual or physical environment with red and blue teaming tests performed to assess the implementation's resilience to cyber security breaches • project management concepts of resourcing, planning and handover are implemented
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: • concepts of risk management planning processes and assessment • relevant current legislation, codes and standards • tools and models of project management • testing tools and methods • troubleshooting techniques • working in teams • design of cyber security infrastructure • operating systems (Windows or Linux) • virtualisation systems • project handover strategies • introductory red and blue teaming exercises • Cyber Security Operations Centre (CSOC) sandbox or equivalent laboratory environment.
ASSESSMENT CONDITIONS	Knowledge and skills assessment must be in a real or simulated workplace environment. If simulated, it must reflect real workplace conditions with suitable facilities and equipment. Assessment must ensure access to: • personnel to form a cyber security project team • computer and networking equipment • computer software • Cyber Security Operations Centre (CSOC) sandbox or equivalent laboratory 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	**VU23294**
Unit title	**Identify and monitor an organisation's cyber security legal compliance requirements**
Application	This unit describes the performance outcomes, skills and knowledge required to identify relevant cyber standards and laws pertaining to an organisation. It requires the ability to evaluate current working practices and to plan and implement any required work practice changes to ensure the organisations compliance with the relevant Australian, international standards and laws. The unit applies to cyber security practitioners who, as part of a team are responsible for implementing and monitoring an organisation's compliance to relevant Australian, international standards and law. No licensing or certification requirements apply to this unit at the time of accreditation
Pre-requisite Units	Nil

Element		**Performance Criteria**	
Elements describe the essential outcomes of a unit of competency.		Performance criteria describe the required performance needed to demonstrate achievement of the element. Assessment of performance is to be consistent with the assessment requirements.	
1	Identify the structure of the Australian legal system	1.1	Key legal terms are defined
		1.2	Structure of the Australian legal systems are investigated
		1.3	Common laws are identified
		1.4	Structure of the Australian federal system of government is defined
		1.5	Relationship between federal and state regulation is clarified
2	Define Australian cyber law	2.1	Model laws on electronic commerce are investigated
		2.2	Conventions on the use of electronic communications are defined
		2.3	Relevant international cybercrime convention is investigated
		2.4	Repercussions of the international General Data Protection Regulation (GDPR) and its adoption in Australia is investigated
		2.5	Implication of Australian electronic transactions law is investigated
3	Identify mandatory and discretionary cyber laws and	3.1	Categories of information the law affords cyber security protection for an organisation are identified

	practices	3.2	Legal resources pertaining to cyber law are identified
		3.3	Relevant laws for particular industry sectors are identified and collated
		3.4	Difference between State and federal legislation for relevant laws pertaining to cyber security are identified
		3.5	Outcomes of current Commonwealth Acts as they pertain to cyber security for an organisation are identified
		3.6	Mandatory outcomes of current State based Acts as they pertain to cyber security for an organisation are identified
		3.7	Codes pertinent to an organisation's industry sector are identified
		3.8	Frameworks pertinent to an organisation's industry sector are identified
		3.9	Voluntary codes and best practices for the industry sector aligned to an organisation are identified
4	Evaluate and select relevant Australian regulation and practices pertaining to security for an organisation	4.1	Methodology of utilising legal resources relevant to cyber law for an organisation is defined and demonstrated
		4.2	Mandatory regulations, standards, codes and frameworks pertaining to cyber security for an organisation are evaluated and selected
		4.3	Discretionary standards, codes and frameworks pertaining to cyber security for an organisation are evaluated and selected
		4.4	Voluntary codes and best practice for the industry sector aligned to an organisation are evaluated and selected
5	Implement relevant Australian regulation and practices pertaining to security for an organisation	5.1	Strategies to implement mandatory regulations, standards, codes and frameworks for an organisation are developed
		5.2	Strategies to implement discretionary standards, codes and frameworks for an organisation are developed
		5.3	Strategies to implement voluntary codes and best practice guidelines for an organisation are developed
		5.4	Organisational changes to appropriate personnel within an organisation are articulated
6	Monitor the effectiveness of an organisation's implementation of regulation and practices	6.1	Criteria to measure the effectiveness of implemented changes to work practices adopted by an organisation is created
		6.2	Utilising the developed criteria, the effectiveness of changes to an organisation's work practices are measured and monitored
		6.3	Changes to the organisation's working practices are documented and reported to appropriate personnel

Range of Conditions

Resources and tools are constantly being updated or replaced in this technology space. Where a resource or tool is no longer relevant or supported an updated resource or tool may be selected in its place. Those listed are examples at the time this unit was written.

- Federal Mandatory Acts pertaining to cyber security are but not limited to:
    - Electronic Transactions Act 1999
    - Corporations Act 2001
    - Criminal Code Act 1995
    - Privacy Act 1988
    - Freedom of Information Act 1982
    - Telecommunications (Interception and Access) Act 1979
    - Competition and Consumer Act 2010 (Can include SPAM Act 2003)
- State legislation pertaining to Cyber Security are but not limited to:
    - Wrongs Act 1958
    - Electronic Transactions (Victoria) Act 2000

Foundation Skills

Foundation skills essential to performance in this unit, but are *not explicit* in the performance criteria are listed here.

Skill	Description
Reading skills to:	accurately interpret documents such as legislation, laws, standards, regulations and codes of practices which apply to cyber security compliance requirements
Writing skills to:	prepare technical documents with appropriate language and detail for the intended readers
Oral communication skills to:	articulate relevant issues with team members and others in the work environment

Unit Mapping information	Code and Title Current Version	Code and Title Previous Version	Comments
	VU23294 Identify and monitor an organisation's cyber security legal compliance requirements	VU22246 Evaluate an organisation's compliance with relevant cyber security standards and Law	Equivalent

Assessment Requirements	
TITLE	Assessment Requirements for: **VU23294 - Identify and monitor an organisation's cyber security legal compliance requirements**
PERFORMANCE EVIDENCE	The candidate must demonstrate the ability to complete the tasks outlined in the elements, performance criteria and foundation skills of this unit, including evidence of the ability to: • evaluate two (2) real or virtual organisations for compliance with relevant legislation, laws, standards, regulations and codes of practices and identify areas of non-compliance. • document recommend change/s where required to improve each organisations' compliance and cyber security resilience.
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: • Australian federal system of Government • difference between federal and state regulation • accessing state and federal Acts (statutes) • interpreting cyber law requirements for the organisation from State and federal acts • mandatory, discretionary and voluntary codes and best practices for the industry sector • Federal Register of Legislation • Federal Mandatory Acts pertaining to cyber security. Refer Range of Conditions for examples • State legislation pertaining to Cyber Security. Refer Range of Conditions for examples. • supporting work practices and standards (Discretionary adoption) • National Institute of Standards and Technology (NIST) Cybersecurity Framework • ISO 31000 Risk Management • ISO/IEC 38500:2015 Preview Information technology - Governance of IT for the organisation • ISO 15489 -1:2016 Preview Information and documentation - Records management - Part 1: Concepts and principles • ISO/IEC 27000 family - Information security management systems, particularly 27701 Privacy in a public cloud • BS 10008 - Evidential Weight and Legal Admissibility of Electronic Information • ISO/IEC 29100:2011 Preview Information technology - Security techniques - Privacy framework • Victorian Protective Data Security Framework (VPDSF) • key feature of Control Objectives for Information and Related Technologies (COBIT) as they pertain to Risk and IT governance

	• key feature of Information Technology Infrastructure Library (ITIL) as they pertain to risk and IT governance • legal implications of adopted standards and procedures • risk assessment methodologies • differences between cyber security legislation, law, standards, • frameworks, policies, procedures and guidelines.
ASSESSMENT CONDITIONS	Knowledge and skills assessment must be in a real or simulated workplace environment. If simulated, it must reflect real workplace conditions with suitable facilities and equipment. Assessment must ensure access to: • relevant cyber security compliance documentation • current State and Federal acts (http://www.austlii.edu.au/) • Federal register of Legislation (https://www.legislation.gov.au) **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	**VU23295**
Unit title	**Gather and validate digital forensic data from workstations**
Application	This unit describes the performance outcomes, skills and knowledge required to select tools and apply techniques to gather and validate digital forensic data from workstations by physical or virtual means or through email or web applications. The unit applies to persons working as cyber security practitioners who, as part of a team responds to cyber security incidents in an organisation. The unit is not intended to prepare a cyber security practitioner to gather evidence for legal purposes. No licensing or certification requirements apply to this unit at the time of accreditation
Pre-requisite Units	Nil

Element		**Performance Criteria**	
Elements describe the essential outcomes of a unit of competency.		Performance criteria describe the required performance needed to demonstrate achievement of the element. Assessment of performance is to be consistent with the assessment requirements.	
1	Examine privacy laws and ethical practises pertaining to digital forensics	1.1	Difference between acquiring digital data and digital forensics for workstations is explained
		1.2	Processes of forensic science and investigation for workstations are identified
		1.3	Current Australian privacy laws and digital forensic legislation are collated and evaluated
		1.4	Current Australian ethical practises for digital forensics are collated and evaluated
		1.5	An ethical code of practise for an organisation performing digital forensics is identified and adopted
2	Define data to be recovered using digital forensic tools	2.1	Forensic data to be recovered from the workstation is defined
		2.2	Triage principles for acquiring and securing data for an organisation are developed
		2.3	Tools for digital forensics are evaluated and selected
3	Acquire defined forensic data from storage media	3.1	Structure and operation of the workstation's file system structure is identified and examined
		3.2	Forensic data provided by the Windows registry structure and content is identified and evaluated
		3.3	Data from disk drives is acquired

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

Range of Conditions

There are no Range of Conditions.

Foundation Skills

Foundation skills essential to performance in this unit, but are *not explicit* in the performance criteria are listed here.

Skill	Description
Reading skills to:	accurately interpret documents and reports relating to digital forensic data
Writing skills to:	prepare technical documentation on acquired data
Oral communication skills to:	articulate relevant issues with team members and/or other stakeholders

Unit Mapping information	Code and Title Current Version	Code and Title Previous Version	Comments
	VU23295 Gather and validate digital forensic data from workstations	VU22247 Gather and validate digital forensic data from workstations	Equivalent

Assessment Requirements	
TITLE	Assessment Requirements for: **VU23295 - Gather and validate digital forensic data from workstations**
PERFORMANCE EVIDENCE	The candidate must demonstrate the ability to complete the tasks outlined in the elements, performance criteria and foundation skills of this unit, including evidence of the ability to: • select digital forensic tools and apply techniques to gather and evaluate forensic data from three (3) workstations each with a different type of file structure e.g.Windows, Unix/Linux and MAC OS.

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:
	• ethics and digital forensics
	• privacy and digital forensics
	• forensic science and investigation
	• file system structures:
	  ○ Windows
	  ○ Unix/Linux
	  ○ MAC OS
	• digital forensic tools and techniques for:
	  ○ storage files
	  ○ email
	  ○ web
	• file meta data
	• extracting key information from EXIF image files
	• methodological problem solving

ASSESSMENT CONDITIONS	Knowledge and skills assessment must be in a real or simulated workplace environment. If simulated, it must real workplace conditions with suitable facilities and equipment. Assessment must ensure access to: • computer equipment • networking equipment • digital forensic tools • 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	**VU23296**
Unit title	**Gather and validate digital forensic data from mobile devices**
Application	This unit describes the performance outcomes, skills and knowledge required to select tools and apply techniques to gather and validate digital forensic data from mobile devices. It requires the ability to use mobile forensic data tools to acquire data from mobile devices for review and validation. The unit also covers the relevant legislation, privacy laws, and regulations to enable the practitioner to review an organisations policies and procedures to validate compliance regarding the use of mobile devices. The unit applies to cyber security practitioners who, as part of a team respond to cyber security incidents. The unit is not intended to prepare a cyber security practitioner to gather evidence for legal purposes. No licensing or certification requirements apply to this unit at the time of accreditation
Pre-requisite Units	Nil

Element		**Performance Criteria**	
Elements describe the essential outcomes of a unit of competency.		Performance criteria describe the required performance needed to demonstrate achievement of the element. Assessment of performance is to be consistent with the assessment requirements.	
1	Examine relevant privacy laws, procedures and processes pertaining to mobile digital forensics	1.1	Difference between acquiring digital data and digital forensics for mobile devices is clarified
		1.2	Process of forensic science and investigation for mobile devices is identified
		1.3	Current Australian privacy laws and mobile digital forensic legislation is collated and evaluated
		1.4	Current Australian ethical practises for mobile forensics are collated and evaluated
		1.5	An ethical code of practise for an organisation performing mobile forensics is adopted
		1.6	Layered models of mobile forensic data acquisition are defined and evaluated
2	Determine smartphone fundamentals and select mobile digital forensic tools	2.1	Smartphone fundamentals for dealing with data are defined
		2.2	Components of, and foundational operation of the digital cellular network are investigated
		2.3	Mobile forensic data tools are identified and evaluated

		2.4	File system structure and operation of a Android and IPhone smartphones are examined and compared
3	Acquire mobile forensic data	3.1	Tools and techniques to access the mobile device where passwords are not known are identified
		3.2	Software drivers, cables and tools to synchronise phone data with a workstation from a phone are selected
		3.3	Key data to be acquired from a mobile device is identified
		3.4	Mobile forensic data tool to acquire key data for the phone is selected
		3.5	Mobile forensic data tool selected is installed and commissioned
		3.6	Users are familiarised with the tool selected to acquire the mobile device data
		3.7	Data from the mobile device is acquired
4	Review defined recovered data	4.1	Acquired data from the mobile device is collated
		4.2	Acquired data is checked for readability and completeness
		4.3	Report on the acquired data is compiled and discussed with appropriate personnel
5	Investigate the function and operation of further tools and techniques for mobile devices	5.1	Joint Test Action Group (JTAG) methods and tools to acquire and analyse data from mobile devices are examined
		5.2	Data encryption use in mobile devices is examined
		5.3	Cloud based mobile forensic tools are evaluated and selected
		5.4	Tools and techniques to examine mobile forensic data on Universal Integrated Circuit Card (UICC) devices are evaluated
		5.5	Hardware tools used to acquire erased data files for mobile devices are researched
		5.6	Developments in mobile data collection forensic tools are identified and classified

Range of Conditions

Resources and tools are constantly being updated or replaced in this technology space. Where a resource or tool is no longer relevant or supported an updated resource or tool may be selected in its place. Those listed are examples at the time this unit was written.

- Strategies and tools to access a locked phone. Examples are:
    - access via iCloud attached account
    - tools from companies like Cellbrite and Niv, Shalev and Omir (NSO) Group Technologies - Pegasus
    - case study of San Bernadino bombers and FBI access
    - Joint Test Action Group (JTAG) methods and tools

Foundation Skills

Foundation skills essential to performance in this unit, but are *not explicit* in the performance criteria are listed here.

Skill	Description
Reading skills to:	interpret technical documents, papers, vendor product specifications, reports and research papers
Writing skills to:	prepare technical documents with appropriate language and detail for the intended readers

Unit Mapping information	Code and Title Current Version	Code and Title Previous Version	Comments
	VU23296 Gather and validate digital forensic data from mobile devices	VU22248 Acquire digital forensic data from mobile devices	Equivalent

Assessment Requirements	
TITLE	Assessment Requirements for: **VU23296 - Gather and validate digital forensic data from mobile devices**
PERFORMANCE EVIDENCE	The candidate must demonstrate the ability to complete the tasks outlined in the elements, performance criteria and foundation skills of this unit, including evidence of the ability to: • select and apply digital forensic tools and techniques to acquire forensic data from two (2) types of mobile devices.

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:
	• ethics and digital forensics
	• mobile digital forensic legislation
	• introduction to forensic science and investigation
	• mobile device file system structures for:
	  ○ IPhone Operating System (IOS)
	  ○ Android
	• mobile forensic tools and techniques
	• tools to acquire mobile device forensic data
	• methodological problem solving
	• strategies and tools to access a locked phone. Refer Range of Conditions for examples.
	• tools and techniques to examine mobile forensic data on Universal Integrated Circuit Card (UICC) devices

ASSESSMENT CONDITIONS	Knowledge and skills assessment must be in a real or simulated workplace environment. If simulated, it must reflect real workplace conditions with suitable facilities and equipment. Assessment must ensure access to: • computer equipment • networking equipment • computer software • mobile devices • digital forensic tools for mobile devices • 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	**VU23297**
Unit title	**Plan and conduct a security risk assessment for an organisation**
Application	This unit describes the performance outcomes, skills and knowledge required to plan and conduct a risk assessment for the organisation. It requires the ability to assess current assets, identify current threats and vulnerabilities, identify a risk process and perform an assessment This unit applies to cyber security practitioners working as a team member and as part of the role required to perform or review a risk assessment for an organisation. No licensing or certification requirements apply to this unit at the time of accreditation
Pre-requisite Units	Nil

Element		**Performance Criteria**	
Elements describe the essential outcomes of a unit of competency.		Performance criteria describe the required performance needed to demonstrate achievement of the element. Assessment of performance is to be consistent with the assessment requirements.	
1	Compile and evaluate risk management plan for the organisation	1.1	Methodologies for risk assessment are investigated
		1.2	Vulnerabilities and threats for an organisation are identified
		1.3	Risk management plan for the organisation is sourced
		1.4	Risk assessment analysis process for an organisation is defined
		1.5	A cyber security disaster recovery plan for an organisation is developed
2	Compile risk categories for the security system	2.1	Information assets for the organisation are ranked and documented
		2.2	Risk analysis classification criteria is determined
		2.3	Use risk analysis processes to qualify and quantify risks and threats
		2.4	Risk priorities for information assets are allocated
		2.5	Risk analysis outcomes for inclusion in the risk register and the risk management plan are documented
3	Implement appropriate security system controls for managing the risk	3.1	Effective controls to manage risk are devised documented and implemented
		3.2	Emerging risks or threats are monitored with corrective measures planned documented
4	Monitor security system controls and processes	4.1	Controls that manage risks are reviewed and monitored for their continued effectiveness

		4.2	Regular risk review processes to maintain currency of risk plans are established
		4.3	Environment is regularly monitored to determine changed conditions
		4.4	If environment or a condition changes, implement and document appropriate changes to the risk controls and report changes to appropriate personnel
5	Promote cybersecurity awareness in the organisation	5.1	Implications of the organisation's security policy are defined and evaluated
		5.2	Strategies to promote security policy awareness in the organisation are planned and implemented
		5.3	Organisation's security policy awareness strategies are evaluated for their effectiveness and if required, modified to increase their effectiveness

Range of Conditions

There are no Range of Conditions.

Foundation Skills

Foundation skills essential to performance in this unit, but are *not explicit* in the performance criteria are listed here.

Skill	Description
Reading skills to:	interpret the detail in organisational policies and procedures that impact may impact upon risk management processes
Writing skills to:	prepare technical documents with appropriate language and detail for the intended readers
Oral communication skills to:	present information to organisational stakeholders concisely and articulately

Unit Mapping information	Code and Title Current Version	Code and Title Previous Version	Comments
	VU23297 Plan and conduct a security risk assessment for an organisation	VU22249 Perform a security risk assessment for an organisation	Equivalent

Assessment Requirements	
TITLE	Assessment Requirements for: **VU23297 - Plan and conduct a security risk assessment for an organisation**

PERFORMANCE EVIDENCE	The candidate must demonstrate the ability to complete the tasks outlined in the elements, performance criteria and foundation skills of this unit, including evidence of the ability to:
	• perform a cyber security risk assessment for a real or virtual organisation. In doing so the candidate must:
	  ○ prepare a risk management plan for the organisation
	  ○ determine appropriate security system controls for managing the risk and;
	  ○ develop strategies to promote cyber security awareness in the organisation.

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: • methods of cyber security attacks • threats and vulnerability's identity • risk assessment methodologies • tools and methods used to protect an organisation's data and privacy • cyber security risk management plans and policies • interpreting risk assessment data, ISO 27001 standards for compliance • risk frameworks defined in ISO 31000 • risk control selection, implementation and monitoring.
ASSESSMENT CONDITIONS	Knowledge and skills assessment must be in a real or simulated workplace environment. If simulated, it must reflect real workplace conditions with suitable facilities and equipment. Assessment must ensure access to: • real or simulated organisation for risk assessment • computer equipment • networking equipment • 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	**VU23298**
Unit title	**Implement processes and procedures to deal with cyber security incidents**
Application	This unit describes the performance outcomes, skills and knowledge required to prepare for and respond to a cyber security incident within an organisation. The unit also includes the skills and knowledge to accurately document the incident and to update the organisation's incident response plan to reduce the risk of further incidents. It requires the ability to identify when the incident occurred, develop and implement an appropriate response' strategy, evaluate the success of the response and any long term effects of the incident. The unit applies to cyber security practitioners who as part of a team, are responsible for the control and ongoing management of cyber incidents in an organisation. No licensing or certification requirements apply to this unit at the time of accreditation
Pre-requisite Units	Nil

Element		**Performance Criteria**	
Elements describe the essential outcomes of a unit of competency.		Performance criteria describe the required performance needed to demonstrate achievement of the element. Assessment of performance is to be consistent with the assessment requirements.	
1	Prepare to respond to an incident	1.1	Procedures to address incidents in the organisation's incident response plan (IRP) are identified and reviewed
		1.2	Organisation's processes to deal with incident responses are benchmarked against published incident response strategies
		1.3	Incident response team (IRT) members to deal with the incident are identified
		1.4	IRT member's roles and responsibilities are clearly defined
		1.5	IRT member's communication expectations during incidents are clarified
		1.6	IRT reporting and communication procedures to relevant organisational groups are defined
		1.7	Function and role of cyber security tools and techniques chosen to detect incidents are defined
		1.8	Data sources to gather incident information are identified
2	Identify the cyber security	2.1	System messages and events to identify malicious activity are evaluated

	incident	2.2	Data is collected from appropriate data sources
		2.3	Initial triage of the incident is performed
		2.4	Risk assessment of the incident is performed
		2.5	Need to escalate the incident is assessed
3	Respond to the incident	3.1	IRT members are recruited to deal with the incident
		3.2	Defined incident response strategy is implemented if the incident is part of the organisation's incident response strategy plan
		3.3	Strategy to deal with the incident is planned if the incident is not part of the organisation's incident response strategy plan
		3.4	Mitigation strategies that quarantine the incident are planned and implemented
4	Monitor effectiveness of the strategies to deal with the incident	4.1	Effectiveness of the strategies to deal with the incident are monitored, evaluated and if required modified
		4.2	Additional IRT members are recruited if required to develop strategies to deal with the incident
		4.3	Incident response is escalated where appropriate
		4.4	Incident is communicated within the organisation according to defined communication strategies
5	Evaluate the impact of the incident	5.1	Impact of the incident is evaluated with appropriate personnel
		5.2	Strategies to deal with any lost or compromised data or resources are planned and implemented
6	Communicate and document the incident	6.1	Incident is documented according to standard organisational templates
		6.2	Incident is communicated to relevant personnel within the organisation
7	Implement post incident review and actions	7.1	Existing incident response strategies are reviewed, modified and documented as required
		7.2	New incident response strategies developed for the incident are included in the organisation's incident response strategy procedure's document
		7.3	Incident response procedure is stored for future reference and used when inducting new staff
		7.4	Business plans and processes are evaluated for change if required with appropriate personnel
		7.5	Existing security equipment and security infrastructure are reviewed
		7.6	Procurement of new security equipment is organised with appropriate personnel if required

Range of Conditions

There are no Range of Conditions.

Foundation Skills

Foundation skills essential to performance in this unit, but are *not explicit* in the performance criteria are listed here.

Skill	Description
Reading skills to:	accurately interpret documents and reports regarding cyber security incidents
Writing skills to:	prepare technical documents with appropriate language and detail for the intended readers
Oral communication skills to:	articulate relevant issues with team members and other stakeholders

Unit Mapping information	Code and Title Current Version	Code and Title Previous Version	Comments
	VU23298 Implement processes and procedures to deal with cyber security incidents	VU22250 Respond to cyber security incidents	Equivalent

Assessment Requirements	
TITLE	Assessment Requirements for: **VU23298 - Implement processes and procedures to deal with cyber security incidents**
PERFORMANCE EVIDENCE	The candidate must demonstrate the ability to complete the tasks outlined in the elements, performance criteria and foundation skills of this unit, including evidence of the ability to: • contribute as part of an incident response team working in a real or virtual organisational environment, to deal with at least two (2) cyber security incidents. In doing so, the candidate must document their contribution to the team's response for each occasion.
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: • coordinating/managing an incident • group collaboration & decision making • incident response procedures • tools and techniques used in the organisation to deal with incidents • function and role of the monitoring equipment and software • sources of data threats • data gathering processes • organisational members roles and responsibilities • when and who to communicate incidents • escalation strategies • risk assessment of incidents • policies, standards and procedures effectiveness for continuous improvement • requirements of incident response documentation.
ASSESSMENT CONDITIONS	Knowledge and skills assessment must be in a real or simulated workplace environment. If simulated, it must reflect real workplace conditions with suitable facilities and equipment. Assessment must ensure access to: **Resources:** • computer equipment • 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	**VU23299**
Unit title	**Utilise tools to gather and interpret data anomalies**
Application	This unit describes the performance outcomes, skills and knowledge required to utilise tools to gather, analyse and interpret data anomalies. It requires the ability to operate hardware and software tools to detect cyber incidents. The unit includes the selection and use of tools to analyse logged data, detection of malicious data streams as well as analysis of the results and evaluation of the selected tools for their effectiveness in detecting data patterns. The unit applies to cyber security practitioners who, as part of a team respond to cyber security incidents in an organization. No licensing or certification requirements apply to this unit at the time of accreditation
Pre-requisite Units	Nil

Element		**Performance Criteria**	
Elements describe the essential outcomes of a unit of competency.		Performance criteria describe the required performance needed to demonstrate achievement of the element. Assessment of performance is to be consistent with the assessment requirements.	
1	Identify the function and operation of hardware and software tools deployed to detect cyber incidents	1.1	Hardware devices used to detect incidents for an organisation are evaluated
		1.2	Software used to detect incidents for an organisation is evaluated
		1.3	Data sources used to gather incident information are identified
		1.4	Types of data sources for a particular incidents are selected
		1.5	Effectiveness of data sources used to detect incidents for an organisation are evaluated
2	Select and use tools that analyse logged data	2.1	Tools that support the interpretation of logged data are evaluated
		2.2	Features of the logged data tool environment are identified and evaluated
		2.3	Plans for data and log management are identified
		2.4	Appropriate tool to analyse logged data is selected
3	Develop skills for analysing data	3.1	Data source to perform analyse is selected
		3.2	Normal baseline data standard for the network is identified
		3.3	Correlation of sampled data to other data sets is preformed

		3.3	Techniques and procedures to identify irregular events are developed including assigning significance to alerts, derivation from baselines and correlation of events with other data sets
		3.4	Effectiveness of the strategy to detect irregular events is evaluated and modified if required
4	Apply tools to detect and analyse logged data stream anomalies	4.1	Most appropriate tool to analyse logged data stream is selected from the working environment
		4.2	Skills using tools to detect data stream anomalies and correlating events are developed and demonstrated
		4.3	An overview of incident playbooks and their role in responding to incidents is investigated
		4.4	Overview of the methodology to integrate scripts to the logged data analysis tool in order to detect data patterns are demonstrated
		4.5	Typical features of Security Orchestration, Automation and Response (SOAR) tools are identified
5	Develop continuous improvement strategies to detect anomalous events for an organisation	5.1	Effectiveness of the tools used to detect data patterns is evaluated
		5.2	Strategies to detect data patterns are evaluated and modified if required

Range of Conditions

- There are no Range of Conditions

Foundation Skills

Foundation skills essential to performance in this unit, but are *not explicit* in the performance criteria are listed here.

Skill	**Description**
Reading skills to:	interpret vendor equipment documents and other related documentation
Writing skills to:	prepare technical documents with appropriate language and detail for the intended readers
Oral communication skills to:	articulate relevant issues encounted in the work environment and making presentations to clients

Unit Mapping information	Code and Title Current Version	Code and Title Previous Version	Comments
	VU23299 Utilise tools to gather and interpret data anomalies	VU22251 Gather, analyse and interpret threat data	Equivalent

Assessment Requirements	
TITLE	Assessment Requirements for: **VU23299 - Utilise tools to gather and interpret data anomalies**
PERFORMANCE EVIDENCE	The candidate must demonstrate the ability to complete the tasks outlined in the elements, performance criteria and foundation skills of this unit, including evidence of the ability to: • operate hardware and software tools to detect, gather, analyse and interpret two (2) types of threat data from a real or virtual workplace environments and document findings including the effectiveness of the tools used and process.
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: • Hardware devices used to detect incidents including: ○ firewall ○ intrusion detection systems and intrusion prevention systems (IDS/IPs) ○ servers used to store log files • Software devices used to detect incidents including: ○ network security monitoring tools ○ web vulnerability scanning tools ○ network defence wireless tools ○ packet sniffers ○ antivirus software ○ virtual firewall ○ infrastructure logs ○ telemetry operation system and application logs • Data and log management planning including: ○ centralisation ○ synchronisation ○ exclusion ○ retention • Techniques and procedures to identify irregular events including: ○ assigning significance to alerts ○ derivation from baselines ○ correlation of events with data sets • Tools that support data analysis of log files

ASSESSMENT CONDITIONS	Knowledge and skills assessment must be in a real or simulated workplace environment. If simulated it must reflect real workplace conditions with suitable facilities and equipment. Assessment must ensure access to: ○ relevant tools for gathering, analysing and interpreting threat data ○ computer equipment ○ networking equipment ○ 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	**VU23300**
Unit title	**Detect and respond to cyber security threats**
Application	This unit describes the performance outcomes, skills and knowledge required to detect and respond to cyber security threats in an organisation. It requires the ability to prepare an organisation for an incident, know how the incident could occur and the processes and procedures to respond. The unit also includes the use of tools and processes to analyse data and detect intrusions. The unit applies to cyber security practitioners who are responsible for implementing and monitoring cyber security operations for an organisation. (The unit applies procedures and processes developed by the National Institute of Standards and Technology (NIST) and is aligned with the Cisco Cyber Operations course). No licensing or certification requirements apply to this unit at the time of accreditation
Pre-requisite Units	Nil

Element		**Performance Criteria**	
Elements describe the essential outcomes of a unit of competency.		Performance criteria describe the required performance needed to demonstrate achievement of the element. Assessment of performance is to be consistent with the assessment requirements.	
1	Define endpoint threat analysis and computer forensics	1.1	Common Vulnerability Scoring System CVSS 3.0 for risk assessment is defined
		1.2	Cyber security features are classified for risk assessment
		1.3	Windows file system components are defined
		1.4	Linux file system components are defined
		1.5	Evidence types are contrasted
		1.6	Altered and unaltered disk images are contrasted
		1.7	Role of assets and threat actors are defined
2	Analyse network intrusion events	2.1	Vulnerabilities in networking protocols are evaluated
		2.2	Elements from a NetFlow record of a security event are analysed
		2.3	Network monitoring tools are identified, evaluated and selected
		2.4	Key elements in an intrusion are identified
		2.5	Data from an event is acquired

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

Range of Conditions

There are no Range of Conditions.

Foundation Skills

Foundation skills essential to performance in this unit, but are *not explicit* in the performance criteria are listed here.

Skill	Description
Reading skills to:	accurately interpret vendor equipment documents and other project related documentation
Writing skills to:	prepare technical documents with appropriate language and detail for the intended readers
Technology skills to:	evaluate new technologies and install and use software packages

Unit Mapping information	Code and Title Current Version	Code and Title Previous Version	Comments
	VU23300 Detect and respond to cyber security threats	VU22252 Implement cyber security operations	Equivalent

Assessment Requirements	
TITLE	Assessment Requirements for: **VU23300 - Detect and respond to cyber security threats**
PERFORMANCE EVIDENCE	The candidate must demonstrate the ability to complete the tasks outlined in the elements, performance criteria and foundation skills of this unit, including evidence of the ability to: • prepare to and deal with at least two (2) cyber incidents, and apply relevant processes and procedures to access and analyse the event data to determine the type of intrusion and review and update the security of the site.

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:
	• Common Vulnerability Scoring System CVSS for incidents
	• Windows file system components include:
	  ○ File Allocation Table - FAT32 New technology File System (NTFS)
	  ○ Alternative data streams
	  ○ Macintosh Application Compatibility Environment (MACE)
	  ○ Extensible Firmware Interface **(**EFI)
	  ○ Free space
	  ○ Timestamps on a file system
	• Linux file system components include:
	  ○ Extended Filesystem (EXT-4)
	  ○ journaling
	  ○ Master Boot Record (MBR)
	  ○ swap file system
	• Key items in an intrusion include:
	  ○ source address
	  ○ destination address
	  ○ source port
	  ○ destination port
	  ○ protocols
	• components of incident response plan
	• steps and methods used to gather data
	• Mitre Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) framework
	• activities performed in incident handling include:
	  ○ scoping
	  ○ containment

	○ remediation ○ lesson-based hardening ○ reporting • Roles and responsibilities within an organisation and to whom to communicate an incident • Escalation strategies • Risk assessment of incidents • Tools and techniques used in the organisation to deal with incidents • Structured Threat Information Expression (STIX) language for describing cyber threat information
ASSESSMENT CONDITIONS	Knowledge and skills assessment must be in a real or simulated workplace environment. If simulated it must reflect real workplace conditions with suitable facilities and equipment. Assessment must ensure access to: • real or simulated cyber intrusion events • computer equipment • networking equipment • relevant tools to detect intrusions and analyse data • 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	**VU23301**
Unit title	**Manage penetration testing processes for an organisation**
Application	This unit describes the performance outcomes, skills and knowledge required to manage the Vulnerability and Penetration Testing (VPEN) for an organisation. It requires the ability to compile information on the existing information technology (IT) and security infrastructure design, evaluate and select testing tools and establish a vulnerability baseline. The unit applies to cyber security practitioners who are required to test an organisations' security infrastructure for vulnerabilities. No licensing or certification requirements apply to this unit at the time of accreditation
Pre-requisite Units	Nil

Element		**Performance Criteria**	
Elements describe the essential outcomes of a unit of competency.		Performance criteria describe the required performance needed to demonstrate achievement of the element. Assessment of performance is to be consistent with the assessment requirements.	
1	Compile information on the organisation's technology	1.1	Information regarding the organisation's IT security infrastructure, web systems, cloud services and security infrastructure is sourced
		1.2	Information on the function and operation on each item of the IT infrastructure, web systems, cloud services and security infrastructure is collated
		1.3	Design of the IT infrastructure, web systems, cloud services, and security infrastructure is evaluated
		1.4	Secure Development Lifecycle (SDLC) and the importance of integrating it with security during all phases of development is established
2	Evaluate and select tools to test the security infrastructure	2.1	Tools used to perform Vulnerability and Penetration (VPEN) testing on the organisation's IT infrastructure, web systems and cloud services are sourced and evaluated
		2.2	Tools to perform VPEN testing are selected
		2.3	Testing environment is setup and configured
		2.4	Web site testing frameworks are evaluated and selected
		2.5	Vulnerabilities within a testing environment are identified
3	Develop penetration testing	3.1	Familiarity with the function and configuration of the VPEN testing tools is developed

	skills	3.2	Skills in using the VPEN testing tools for detecting vulnerabilities in security infrastructure are developed
		3.3	Familiarity with sources of information for vulnerabilities, threat intelligence and exploits is developed
		3.4	Differences between infrastructure vulnerability scanning, web vulnerability scanning, cloud security assessment, and penetration testing are articulated
		3.5	Familiarity with identifying and using sources of threat intelligence and exploit information is developed
4	Identify tools to establish a vulnerability baseline	4.1	Locations and devices where vulnerability information comes from within the organisation are identified and documented
		4.2	Tools to determine the vulnerability baseline within the organisation are identified and documented
		4.3	Regular procedures and processes for VPEN testing for the organisation are proposed
5	Research new security technology developments	5.1	Current developments in cyber security infrastructure testing developments are sourced and reviewed
		5.2	New tools for VPEN testing are researched

Range of Conditions

There are no Range of Conditions.

Foundation Skills

Foundation skills essential to performance in this unit, but are *not explicit* in the performance criteria are listed here.

Skill	Description
Reading skills to:	accurately interpret documents and reports relating to IT security infrastructure, web systems, cloud services and security infrastructure
Writing skills to:	prepare technical documents with appropriate language and detail for the intended readers
Oral communication skills to:	articulate relevant issues encounted in the work environment with other personnel

Unit Mapping information	Code and Title Current Version	Code and Title Previous Version	Comments
	VU23301 Manage penetration testing processes for an organisation	VU22253 Undertake penetration testing of the security infrastructure for an organisation	Not equivalent

Assessment Requirements	
TITLE	Assessment Requirements for: **VU23301- Manage penetration testing processes for an organisation**

PERFORMANCE EVIDENCE	The candidate must demonstrate the ability to complete the tasks outlined in the elements, performance criteria and foundation skills of this unit, including evidence of the ability to:
	• manage the VPEN testing process for a real or simulated organisation. In doing so:
	  ○ document the organisation's technology items that are potentially vulnerable
	  ○ identify and use a tool to generate a data traffic baseline for the organisation.

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: • physical and virtual cyber security infrastructure • types of testing • tools used to document VPEN tests • vulnerability scanning and penetration testing tools • vulnerabilities of virtualised systems (shared hosting) • introduction to Secure Development Lifecycle (SDLC)
ASSESSMENT CONDITIONS	Knowledge and skills assessment must be in a real or simulated workplace environment. If simulated it must reflect real workplace conditions with suitable facilities and equipment. Assessment must ensure access to: • real or simulated organisation security infrastructure for testing • computer hardware and software and VPEN testing tools • networking equipment • 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	**VU23302**
Unit title	**Perform advanced penetration testing for web site vulnerabilities**
Application	This unit describes the performance outcomes, skills and knowledge required to expand the testing capability for web vulnerabilities. It includes skills in using advanced features of current toolsets in order to identify weaknesses in the security of an organisation's website. It requires the ability to utilise the current security framework Open Web Application Security Project (OWASP) security methodology and open source tools to provide a sound foundation to develop these skills. The unit applies to cyber security practitioners who are required to use advanced testing tools to determine vulnerabilities in an organisation's web site. No licensing or certification requirements apply to this unit at the time of accreditation
Pre-requisite Units	VU23301 - Manage penetration testing processes for an organisation

Element		**Performance Criteria**	
Elements describe the essential outcomes of a unit of competency.		Performance criteria describe the required performance needed to demonstrate achievement of the element. Assessment of performance is to be consistent with the assessment requirements.	
1	Comprehend the web application development process	1.1	Web application development process is explained
		1.2	Web application development environment and associated test phases are determined
		1.3	Web architecture concepts are reviewed
		1.4	Examples of web frameworks are reviewed
2	Utilise tools and technology for testing web site content	2.1	Tools used to determine the technology stack used in web applications and web servers are utilised
		2.2	Custom wordlists for spidering are created
		2.3	Value of user-agent strings used in testing tools are evaluated
		2.4	Identifying the technology stack of a web application utilising current resources are investigated
3	Examine the advanced features of a current proxy testing tool suite	3.1	Review of a current proxy tool suite is demonstrated
		3.2	Dangers of live scanning are explained
		3.3	Utilising extended features of a current proxy testing tool, the vulnerabilities of the organisation's web site are explored
4	Perform vulnerability scanning	4.1	Difference between automated testing and manual testing is compared

		4.2	Use of an automated web application scanner to test an application is demonstrated
		4.3	Results from the automated scanner report are interpreted
		4.4	Use of manual testing of a web application is explored
5	Identify common web application vulnerabilities	5.1	Common web application vulnerabilities are reviewed
		5.2	Content and vulnerabilities of Content Management Systems and plugin are investigated
		5.3	Remediation strategies to mitigate the defined web application vulnerabilities are formulated
		5.4	Vulnerabilities for software rework are reported to the developer
6	Exploit web application vulnerabilities	6.1	Testing tools and manual methods used to exploit web application vulnerabilities are selected
		6.2	Advantages and disadvantages of web application testing tools are evaluated
		6.3	Use of testing tool operation to exploit web site vulnerabilities is demonstrated

Range of Conditions

There are no Range of Conditions

Foundation Skills

Foundation skills essential to performance in this unit, but are *not explicit* in the performance criteria are listed here.

Skill	Description
Reading skills to:	accurately interpret documents and reports relating to security infrastructure and penetration testing
Writing skills to:	prepare technical documents with appropriate language and detail for the intended readers
Oral communication skills to:	articulate relevant issues encounted in the work environment with other personnel
Learning skills to:	expand own testing capability for web site vulnerabilities

Unit Mapping information	Code and Title Current Version	Code and Title Previous Version	Comments
	VU23302 Perform advanced penetration testing for web site vulnerabilities	VU22254 Undertake advanced penetration testing for web site vulnerabilities	Not equivalent

Assessment Requirements	
TITLE	Assessment Requirements for: **VU23202 – Perform advanced penetration testing for web site vulnerabilities**
PERFORMANCE EVIDENCE	The candidate must demonstrate the ability to complete the tasks outlined in the elements, performance criteria and foundation skills of this unit, including evidence of the ability to: • perform penetration testing of two (2) real or simulated organisational web sites to exploit weaknesses and document strategies for improvements.
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: • web application development practices (e.g. waterfall, agile) • web application development environment • web architectures • web frameworks • web application enumeration tools • custom wordlists for spidering • user agent string values • web application technology stack • web application proxy tools e.g. (burp) • spider and scanning tools (e.g. burp spider) • penetration testing frameworks (e.g. OWASP) • common web site vulnerabilities including: o injection weaknesses o broken Authentication and Session Management weakness o Cross Site Scripting (XSS) weaknesses o insecure Direct Object References weaknesses o identify Security Misconfiguration weaknesses o Identify Sensitive Data Exposure weaknesses o missing function level access control weaknesses o identify Cross Site Request Forgery (CSRF) weaknesses o using known vulnerable components weaknesses o invalidate redirects and forwards weaknesses.
ASSESSMENT CONDITIONS	Knowledge and skills assessment must be in a real or simulated workplace environment. If simulated it must reflect real workplace conditions with suitable facilities and equipment. Assessment must ensure access to: • web testing environment • scanning and penetration testing tools • relevant reference documentation **Assessor requirements:**

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

CC BY ND

Unit code	**VU23303**
Unit title	**Develop mitigation strategies for Internet of Things devices**
Application	This unit describes the performance outcomes, skills and knowledge required to examine the function and operation of Internet of Things (IoT) devices. It requires the ability to identify what threats and vulnerabilities exist when using IoT and to apply strategies to minimise them. The unit applies to cyber security practitioners who utilise IoT devices. No licensing or certification requirements apply to this unit at the time of accreditation
Pre-requisite Units	Nil

Element		**Performance Criteria**	
Elements describe the essential outcomes of a unit of competency.		Performance criteria describe the required performance needed to demonstrate achievement of the element. Assessment of performance is to be consistent with the assessment requirements.	
1	Identify IoT device function and operation	1.1	Impact and use of IoT devices is defined
		1.2	IoT devices are classified
		1.3	Approaches to capture IoT device function (such as Devise Intent) is investigated in order to select security frameworks and approaches
		1.4	Operation of an example IoT device is described and demonstrated
		1.5	IoT device data collected , generated, or accessed is analysed and the identification of risks to confidentiality, privacy, data integrity, or system control is performed
2	Identify current threats and vulnerability issues for IoT devices	2.1	IoT device lifecycle is explained
		2.2	Complexity of security issues for IoT devices across the entire lifecycle is investigated
		2.3	Example of a current threat for an IoT device is investigated
		2.4	Key strategies and guidance to mitigate IoT cyber security risks are identified and evaluated
3	Select relevant security frameworks and mitigating strategies for IoT incidents	3.1	Three, four or five (3, 4 or 5) layered models for IoT devices are compared
		3.2	Appropriate strategies and guidance to mitigate IoT cyber security risks are selected in consultation with key personnel

		3.3	Emerging and current mitigating strategies for application layer vulnerabilities across all phases of the IoT device lifecycle are identified and documented
		3.4	Emerging and current mitigating strategies for network layer vulnerabilities across all phases of the IoT device lifecycle are identified and documented
4	Implement relevant security frameworks for IoT incident mitigation strategies	4.1	Appropriate IoT security frameworks are implemented in consultation with key organisational personnel
		4.2	Training for staff to improve the IoT security culture in the organisation is implemented
		4.3	Mitigating strategies for application layer vulnerabilities across all phases of the IoT device lifecycle are implemented
		4.4	Mitigating strategies for network layer vulnerabilities across all phases of the IoT device lifecycle are implemented
5	Monitor the vulnerabilities of the IoT devices	5.1	Existing security infrastructure is configured to detect for IoT device vulnerabilities
		5.2	System messages and events to identify IoT malicious activity are evaluated
		5.3	Organisational policies and processes are reviewed and followed upon the detection of IoT initiated incidents

Range of Conditions

Resources and tools are constantly being updated or replaced in this technology space. Where a resource or tool is no longer relevant or supported an updated resource or tool may be selected in its place. Those listed are examples at the time this unit was written.

- IoT security frameworks, vulnerabilities and mitigation tools and strategies resources. Examples include:
    - documents from the National Institute of Standards and Technology (NIST) Cybersecurity Framework
    - key documents from the Industrial Control Systems - Cyber Emergency Response Team (ICS-CERT) organisation relating to securing ICS infrastructure *(https://ics-cert.us-cert.gov/)*
    - key IoT documents from the European Union Agency for Network and Information Security (ENISA)
    - https://www.enisa.europa.eu
    - key aspects of the IoT Alliance Australia: Internet of Things Security Guideline
- Monitoring tools and techniques for IoT devices. An example is:
    - resources provided by IoTopia

Foundation Skills

Foundation skills essential to performance in this unit, but are *not explicit* in the performance criteria are listed here.

Skill	Description
Reading skills to:	interpret vendor IoT devices documents and other related information
Writing skills to:	prepare technical documents with appropriate language and detail for the intended readers
Oral communication skills to:	articulate relevant IoT issues with users and other relevant stakeholders
Technology skills to:	interpret network diagrams, install and using software packages, connect cyber security equipment and network devices

Unit Mapping information	Code and Title Current Version	Code and Title Previous Version	Comments
	VU23303 Develop mitigation strategies for Internet of Things devices	VU22255 Evaluate threats and vulnerabilities for Internet of Things devices	Equivalent

Assessment Requirements	
TITLE	Assessment Requirements for: **VU23303 – Develop mitigation strategies for Internet of Things devices**
PERFORMANCE EVIDENCE	The candidate must demonstrate the ability to complete the tasks outlined in the elements, performance criteria and foundation skills of this unit, including evidence of the ability to: • examine three (3) different IoT devices, identify each device's function and operation and what mitigation strategies should be employed to protect each from threats and vulnerabilities.
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: • IoT security frameworks, vulnerabilities and mitigation tools and strategies resources, (Refer Range of Condition for examples • IoT device lifecycle • IoT device classification • risk assessment for IoT devices • differences between security frameworks, policies, standards, procedures, guidelines, and legislation. • Monitor tools and techniques for IoT devices.(Refer Range of Conditions for examples)
ASSESSMENT CONDITIONS	Knowledge and skills assessment must be in a real or simulated workplace environment. If simulated it must reflect real workplace conditions with suitable facilities and equipment. Assessment must ensure access to: • securing ICS infrastructure (https://ics-cert.us-cert.gov/) • IoT documents from ENISA (https://www.enisa.europa.eu) • monitoring tools from IoT devices (https://globalplatform.org/iotopia/) • selection of IoT devices • computer equipment • networking equipment • relevant computer software tools • relevant references and 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	**VU23304**
Unit title	**Protect industrial networks and operational technology infrastructure for an organisation**
Application	This unit describes the performance outcomes, skills and knowledge required to examine the key standard bodies and frameworks that offer constructive support for addressing threats and vulnerabilities of Internet of Things (IoT) devices and Industrial Control System ((ICS) infrastructure for an organisation. It requires the ability to identify the vulnerabilities of existing IoT and ICS systems and then apply mitigation strategies to protect an organisation's IoT and ICS infrastructure. The mitigating strategies are then monitored for their effectiveness. The unit applies to cyber security practitioners who are required to protect IoT and ICS infrastructure from cyber security threats and vulnerabilities. No licensing or certification requirements apply to this unit at the time of accreditation
Pre-requisite Units	Nil

Element		**Performance Criteria**	
Elements describe the essential outcomes of a unit of competency.		Performance criteria describe the required performance needed to demonstrate achievement of the element. Assessment of performance is to be consistent with the assessment requirements.	
1	Define IoT and ICS differences and relevant security frameworks	1.1	Differences between IoT and ICS is identified
		1.2	Key standards bodies and organisations that provide useful resources that address security issues for IoT and ICS infrastructure are identified
		1.3	Current IoT infrastructure architectures are reviewed and evaluated
		1.4	Current working frameworks or practices that can support the improvement of IoT and ICS from cyber security attack are identified
2	Evaluate current IoT and ICS infrastructure for an organisation with related vulnerabilities	2.1	ICS devices used in an organisation are identified and classified
		2.2	IoT devices used in an organisation are identified and classified
		2.3	Responsibility for the installation and maintenance of the IoT and ICS devices for the organisation is identified
		2.4	Connectivity of the ICS and IoT devices for the organisation is determined
		2.5	Current vulnerabilities of the IoT and ICS devices for an organisation are identified

		2.6	Risk assessment for ICS and IOT devices used in an organisation is performed
		2.7	Case studies of two critical infrastructure attacks performed on an organisation are investigated
		2.8	Cyber-attacks on critical infrastructure as part of military campaigns are identified
3	Classify current cyber security vulnerabilities for IoT and ICS devices	3.1	Classification of current cyber security vulnerabilities for ICS's and IoT devices are identified
		3.2	Risk assessment of vulnerabilities for current organisation's IoT and ICS devices is conducted
4	Select relevant cyber security frameworks and security critical infrastructure for IoT and ICS mitigation strategies	4.1	Resources that provide strategies to protect IoT and ICS infrastructure are sourced
		4.2	Organisational security policies to protect IoT and ICS infrastructure are evaluated and selected
		4.3	Strategies to enhance the protection of IoT and ICS infrastructure are adopted
		4.4	Training for staff to improve the security culture is planned and implemented
5	Monitor the effectiveness of adopted IoT and ICS infrastructure mitigation strategies	5.1	Criteria to measure the effectiveness of implemented IoT and ICS mitigation strategies is developed
		5.2	Tools to monitor the organisation's IoT and ICS from cyber attacks are identified and selected
		5.3	Monitoring tools for an organisation's IoT and ICS infrastructure are implemented
		5.4	Effectiveness of the monitoring tools implemented for an organisation's IoT and ICS systems is reviewed and updated where necessary
		5.5	Changes to organisational processes and procedures to deal with IoT and ICS infrastructure incident responses are reviewed for their effectiveness and updated where necessary

Range of Conditions

Resources and tools are constantly being updated or replaced in this technology space. Where a resource or tool is no longer relevant or supported an updated resource or tool may be selected in its place. Those listed are examples at the time this unit was written.

- security frameworks and cyber security mitigation strategies. Examples include:
  - key aspects of the National Institute of Standards and Technology (NIST) Cybersecurity Framework (https://www.nist.gov/cyberframework)
  - Framework for improving Critical Infrastructure Cybersecurity (https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf)
  - key strategies from the European Union Agency for Network and Information Security (ENISA) (https://www.enisa.europa.eu)

Foundation Skills

Foundation skills essential to performance in this unit, but are *not explicit* in the performance criteria are listed here.

Skill	Description
Reading skills to:	accurately interpret documents and reports relating to organisational infrastructure
Writing skills to:	prepare documents with the appropriate technical detail to coordinate information on organisational critical infrastructure
Oral communication skills to:	make presentations and deliver training to staff using the appropriate language and detail for the intended audience

Unit Mapping information	Code and Title Current Version	Code and Title Previous Version	Comments
	VU23304 - Protect industrial networks and operational technology infrastructure for an organisation	VU22256 - Protect critical infrastructure for an organisation	Not equivalent

Assessment Requirements	
TITLE	Assessment Requirements for: **VU23304 - Protect industrial networks and operational technology infrastructure for an organisation**
PERFORMANCE EVIDENCE	The candidate must demonstrate the ability to complete the tasks outlined in the elements, performance criteria and foundation skills of this unit, including evidence of the ability to: • develop, implement, monitor and assess the effectiveness of mitigation strategies to protect both IoT and ICS infrastructure for an organisation.

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:
	• industrial Control System (ICS) architectures
	• IoT architectures
	• ICSs infrastructure include:
	  ○ heating, ventilation and air conditioning (HVAC)
	  ○ building management
	  ○ lighting
	  ○ security
	  ○ Programmable Logic Controllers (PLC's)
	  ○ Supervisory Control and Data Acquisition (SCADA) Systems
	• security frameworks and cyber security mitigation strategies. (Refer Range of Conditions for examples).
	• strategies to defend ICS's include:
	  ○ application whitelisting
	  ○ configuration & patch management
	  ○ reduce attack surface area
	  ○ defendable environment
	  ○ manage authentication
	  ○ monitor and respond
	  ○ implement secure remote access
	• key strategies from ISO/IEC 2700X
	• risk assessment of IoT and ICS systems
	• IoT and ICS vulnerabilities
	• differences between security frameworks, policies, standards, procedures and guidelines
	• mitigation strategies to security critical infrastructure
	• tools to monitor IoT and ICS systems

ASSESSMENT CONDITIONS	Knowledge and skills assessment must be in a real or simulated workplace environment. If simulated it must reflect real workplace conditions with suitable facilities and equipment. Assessment must ensure access to: • real or simulated organisation's IoT and ICS infrastructure

	• computer equipment • networking equipment • 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	**VU23305**
Unit title	**Select and configure security devices for an organisation**
Application	This unit describes the performance outcomes, skills and knowledge required to select and configure an organisation's security devices. It also includes monitoring and assessing the effectiveness of the implementation. It requires the ability to research and evaluate new security devices and technologies as they become available in order to improve the security performance of the organisation. The unit applies to cyber security practitioners who are responsible for an organisation's security infrastructure. No licensing or certification requirements apply to this unit at the time of accreditation
Pre-requisite Units	Nil

Element		**Performance Criteria**	
Elements describe the essential outcomes of a unit of competency.		Performance criteria describe the required performance needed to demonstrate achievement of the element. Assessment of performance is to be consistent with the assessment requirements.	
1	Collate the current network security diagram, security infrastructure functional operation and security device documentation	1.1	Existing security infrastructure diagram for the organisation is sourced
		1.2	In consultation with appropriate personnel the function and operation of the existing network security infrastructure is evaluated
		1.3	Network security devices, systems and tools are identified
2	Configure security devices according to their functional specification	2.1	Resources to configure the network security devices for the organisation are gathered
		2.2	Organisations security policy document is sourced
		2.3	Network security devices, systems and tools are configured according to the functionality described in the network security policy
3	Verify operation of security devices	3.1	Baseline performance of the network security devices for the organisation is determined
		3.2	In accordance with baseline functionality and utilising software or hardware tools the network security device performance is monitored
		3.3	With appropriate personnel the effectiveness of the security device operation is evaluated
4		4.1	New network security devices and technologies are researched and examined

	Investigate and implement new network security architectures and devices	4.2	Higher level packet inspection technology for a network security devise is reviewed and implemented
		4.3	Holistic approaches to traffic inspection technologies for a network security device is examined
		4.4	Concept of dynamic update technology to defend against new cyber-attacks for a network security device is described then implemented
		4.5	Virtual network security technologies are investigated and selected
		4.6	Virtual network security technology solution is configured and implemented

Range of Conditions

Resources and tools are constantly being updated or replaced in this technology space. Where a resource or tool is no longer relevant or supported an updated resource or tool may be selected in its place. Those listed are examples at the time this unit was written.

- Overview of network security devices that provide network security functionality include:
    - Access Control Lists (ACLs)
    - firewalls including Zone based policy firewalls
    - packet filtering
    - inspection rules
    - Intrusion Detection Systems (IDS)
    - intrusion Prevention Systems (IPS)
    - Virtual Private Networks (VPNs)
    - Network Access Control (NAC)
    - Web Application Firewalls (WAF)
    - honeypots
    - packet Shapers
    - proxies
    - reverse Proxies

Foundation Skills

Foundation skills essential to performance in this unit, but are *not explicit* in the performance criteria are listed here.

Skill	Description
Reading skills to:	accurately interpret technical documents and reports relating to organisation security devices
Writing skills to:	prepare documentation with the appropriate technical detail for the intended audience

	Code and Title Current Version	Code and Title Previous Version	Comments

Unit Mapping information	VU23305 - Select and configure security devices for an organisation	VU22257 - Configure security devices for an organisation	Equivalent

Assessment Requirements	
TITLE	Assessment Requirements for: **VU23305 - Select and configure security devices for an organisation**

PERFORMANCE EVIDENCE	The candidate must demonstrate the ability to complete the tasks outlined in the elements, performance criteria and foundation skills of this unit, including evidence of the ability to:
	• configure and modify where required at least two (2) separate organisational existing security devices. In doing so the learner must:
	  ○ assess the current network security diagram, security infrastructure functional operation and security device documentation
	  ○ configure and verify security devices according to the functional specification
	  ○ evaluate the performance of the network security device

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: • Network security technologies • Overview of network security devices that provide network security functionality: (Refer Range of Conditions for examples). • Patch management of security network devices • Testing of network security device configuration
ASSESSMENT CONDITIONS	Knowledge and skills assessment must be in a real or simulated workplace environment. If simulated it must reflect real workplace conditions with suitable facilities and equipment. Assessment must ensure access to: • networking security technologies for two separate organisations • 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	**VU23306**
Unit title	**Design security architecture for an organisation**
Application	This unit describes the performance outcomes, skills and knowledge required to utilise tools and methodologies to design the security architecture for an organisation that addresses it's business requirements, IT applications and end user expectations. It requires the ability to implement a process for reviewing the existing security architecture, conduct of a security design audit and recommend improvements. The unit applies to cyber security practitioners responsible for an organisation's security infrastructure. No licensing or certification requirements apply to this unit at the time of accreditation
Pre-requisite Units	Nil

Element		**Performance Criteria**	
Elements describe the essential outcomes of a unit of competency.		Performance criteria describe the required performance needed to demonstrate achievement of the element. Assessment of performance is to be consistent with the assessment requirements.	
1	Evaluate current security architecture frameworks and methodologies	1.1	Existing security architecture frameworks and methodologies are identified and evaluated
		1.2	In consultation with appropriate personnel the outcomes of the standards and frameworks evaluation are examined for suitability and implementation
		1.3	Business goals and objectives are identified and translated to security goals and objectives
2	Collate network security design documentation	2.1	Existing network security logical architecture is reviewed and updated as required
		2.2	Existing network security physical architecture is reviewed and updated as required
3	Conduct a security assessment on the security devices and components	3.1	Network trust security assessment to reflect zero trust network architectures as the benchmark for secure networks is conducted
		3.2	Existing security infrastructure diagram for the organisation is sourced
		3.3	Template for security assessments including business impact is developed or sourced
		3.4	Risk and threat modelling for the organisation is developed
		3.5	Security metrics covering control objectives, warning thresholds and control thresholds is developed

4	Collate and review security policies for the organisation	4.1	Current security policy documents for the organisation are collated
		4.2	In consultation with appropriate personnel, security policies are reviewed and updated where appropriate
		4.3	Change management process strategies to improve cyber security working practices within the organisation are developed
5	Evaluate methodologies for security architecture	5.1	In consultation with appropriate personnel a layered model of security architecture is evaluated and selected
		5.2	Issues around implementing a layered model of security architecture are prioritised
		5.3	Different types of security technical designs are defined
		5.4	Key development principles of a sound security architecture are investigated
		5.5	Process to address special security architecture challenges are investigated
6	Determine existing security architecture vulnerabilities	6.1	Models and methodologies to identify security architecture vulnerabilities are collated, evaluated and selected
		6.2	An audit to detect vulnerabilities for the security architecture is performed
		6.3	In consultation with appropriate personnel, strategies to mitigate detected security architecture vulnerabilities are developed and deployed
7	Communicate design options for security architecture to the organisation	7.1	Engaging strategies for different stakeholder groups are developed
		7.2	Communication strategies for different stakeholder groups are developed
		7.3	Reports to different stakeholder groups are written and presented utilising developed strategies
		7.4	Tools to develop security architecture documentation are selected and sourced

Range of Conditions

Resources and tools are constantly being updated or replaced in this technology space. Where a resource or tool is no longer relevant or supported an updated resource or tool may be selected in its place. Those listed are examples at the time this unit was written.

- Security architecture frameworks and tools. Examples include:
    - Sherwood Applied Business Security Architecture **(**SASBA) Frameworks for security architecture design
    - Control Objectives for Information and Related Technologies (COBIT)
    - Information Technology Infrastructure Library (ITIL)
    - National Institute of Standards and Technology (NIST) cyber security framework
    - Enterprise Architecture Framework - Zachman Institute for Framework Advancement

Foundation Skills

Foundation skills essential to performance in this unit, but are *not explicit* in the performance criteria are listed here.

Skill	**Description**
Reading skills to:	accurately interpret documents and reports regarding security architecture
Writing skills to:	prepare technical documents with appropriate language and detail for the intended readers
Oral communication skills to:	present security designs to various stakeholder groups and articulate relevant issues encountered in the work environment
Technology skills to:	connect cyber security equipment and networked devices

Unit Mapping information	Code and Title Current Version	Code and Title Previous Version	Comments
	VU23306 Design security architecture for an organisation	VU22259 Utilise design methodologies for security architecture	Equivalent

Assessment Requirements	
TITLE	Assessment Requirements for: **VU23306 - Design security architecture for an organisation**
PERFORMANCE EVIDENCE	The candidate must demonstrate the ability to complete the tasks outlined in the elements, performance criteria and foundation skills of this unit, including evidence of the ability to: • utilise models and methodologies to design the security architecture for an organisation that addresses the business goals and objectives, IT applications and end user requirements.
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: • security architecture designs to suit various stakeholder requirements • security architecture documentation • security network devices • business requirements of the organisation • communication strategies • security architecture frameworks and tools. (Refer Range of Conditions for examples).
ASSESSMENT CONDITIONS	Knowledge and skills assessment must be in a real or simulated workplace environment. If simulated it must reflect real workplace conditions with suitable facilities and equipment. Assessment must ensure access to: • current security infrastructure for two different organisations • computer equipment • networking equipment • relevant 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	**VU23307**
Unit title	**Identify the implications of cloud-based security services**
Application	This unit describes the performance outcomes, skills and knowledge required to identify cyber security implications of using cloud-based services and develop a working knowledge 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. The unit applies to cyber security practitioners 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 Units	Nil

Element		**Performance Criteria**	
Elements describe the essential outcomes of a unit of competency.		Performance criteria describe the required performance needed to demonstrate achievement of the element. Assessment of performance is to be consistent with the assessment requirements.	
1	Identify key features, design and consequences of cloud-based environments.	1.1	Different cloud architectures and models are compared and contrasts identified
		1.2	Implications, limitations and consequences of high availability and scaling in cloud environments are explained
		1.3	Testing techniques for cloud environments are identified
		1.4	Limitations of testing techniques across different cloud environments are defined
		1.5	Sandboxes for cloud infrastructure using cloud services are created
2	Determine the best mechanism and techniques to secure cloud networks	2.1	Mechanisms used for securing cloud networks are identified
		2.2	Appropriate application security and Operating System (OS) controls in cloud environments are applied
		2.3	Appropriate compliance controls in cloud environments to protect data are applied
		2.4	Cloud security services required to meet business needs are identified
3	Identify mechanism and techniques used to operate and support cloud environments	3.1	Logging, monitoring and alerting to protect cloud environments are identified and configured
		3.2	Policies, procedures and techniques to maintain cloud environment security are determined

		3.3	Mechanisms and business requirements to performing disaster recovery tasks in a cloud environment are identified
		3.4	Ways to perform cloud migrations and their limitations are identified
		3.5	Security monitoring services and tools that align with business needs are investigated and documented
4	Determine the best way to troubleshoot cloud-related issues	4.1	Methods to troubleshoot common security issues in cloud environments are defined
		4.2	Methods to troubleshoot common deployment issues in cloud environments are identified

Range of Conditions

Resources and tools are constantly being updated or replaced in this technology space. Where a resource or tool is no longer relevant or supported an updated resource or tool may be selected in its place. Those listed are examples at the time this unit was written.

- 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 Hypertext Transfer Protocol Secure (HTTPS)=(DoH)
    - DNS over Transport Layer Security (TLS)=(DoT)
    - Domain Name System Security Extensions (DNSSEC)
    - Distributed denial-of-service (DDoS) tunnelling techniques
    - network segmentation types such as: micro, tiering, generic network virtualization encapsulation

Foundation Skills

Foundation skills essential to performance in this unit, but are *not explicit* in the performance criteria are listed here.

Skill	Description
Reading skills to:	interpret documented materials and procedures
Writing skills to:	prepare technical documents with appropriate language and detail for the intended readers
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: **VU23307 - Identify the implications of cloud-based security services**
PERFORMANCE EVIDENCE	The candidate must demonstrate the ability to complete the tasks outlined in the elements, performance criteria and foundation skills of this unit, including evidence of the ability to: • manage the security infrastructure for a cloud environment. To complete this, appropriate security controls for managing risk are implemented and troubleshoot techniques to identify common cloud-based security problems are demonstrated.
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 including: o public o private o hybrid o Platform as a Service (PaaS) o Software as a Service (SaaS) o Infrastructure as a Service (IaaS) • Cloud environment limitations including: 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 including: o vulnerability o penetration o performance regression o usability o functional • Limitations of testing techniques across different cloud environments including : o staging o production o Disaster Recovery (DR) o Quality Assurance (QA)

	○ Blue/green deployment strategy • Mechanisms to secure cloud services. (Refer Range of Conditions for examples). • application security and Operating System (OS) controls. • Compliance controls to protect data including: ○ Cloud Access Security Broker (CASB) ○ Data Loss Protection (DLP) ○ segmentation ○ data management ○ access controls ○ classification and encryption • Logging, alerting and monitoring tools including: ○ collectors ○ analysis ○ categorization ○ audits ○ automation ○ baselines ○ tagging ○ scrubbing • Cloud environment policies and procedures including: ○ vulnerability and patch management ○ hypervisors ○ virtual appliances ○ life-cycle management ○ backups and reporting • Disaster recovery in cloud environments including: ○ restoration ○ replication ○ Recovery Point Objective (RPO) ○ Recovery Time Objective (RTO) ○ Service Level Agreement (SLA) ○ playbook ○ failback and failover • Cloud migration strategies including: ○ physical to virtual ○ virtual to virtual ○ cloud to cloud • Cloud environment troubleshooting issues including: ○ privilege ○ authentication

	○ authorisation ○ Public Key Infrastructure (PKI) policy misconfigurations ○ failed security appliances • Cloud deployment troubleshooting issues including: ○ 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	Knowledge and skills assessment must be in a real or simulated workplace environment. If simulated it must reflect real workplace conditions with suitable facilities and equipment. Assessment must ensure access to: • cloud based environment • computer equipment • networking equipment • 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	**VU23308**
Unit title	**Identify Active Directory security concepts**
Application	This unit describes the performance outcomes, skills and knowledge required to enable participants to firstly, become familiar with the architecture of Active Directory (AD) then to identify areas of security vulnerability. It requires the ability to define AD physical structure together with the roles of the protocols used. The unit also includes the tactics, techniques, and procedures (TTP's) used to compromise AD accounts as well as methods of securing and defending AD including developing safe AD working practices. The unit applies to cyber security practitioners who, as part of a team responds to cyber security incidents in an organisation. No licensing or certification requirements apply to this unit at the time of accreditation
Pre-requisite Units	Nil

Element		**Performance Criteria**	
Elements describe the essential outcomes of a unit of competency.		Performance criteria describe the required performance needed to demonstrate achievement of the element. Assessment of performance is to be consistent with the assessment requirements.	
1	Identity Access Management (AM) fundamentals	1.1	Differences between identities, accounts, access, authorisation and authentication are identified
		1.2	Identity lifecycle management process is defined
		1.3	Function and operation of common authentication services are compared
		1.4	Types of authorisation processes are identified
		1.5	Accountability and audit concepts, such as access logging and audit trails are identified
		1.6	Current trends in identity determination such as Multi Factor Authentication (MFA) are investigated
2	Investigate AD architecture	2.1	Logical structure of an AD is identified
		2.2	AD physical structure is defined
		2.3	Roles of the protocols used in AD are defined
		2.4	Mechanics of AD are described
		2.5	Structure of privileged accounts and groups in AD are examined
		2.6	Group Policy Objects (GPO's) configuration issues especially if applying to the domain root or domain controller are identified

		2.7	Cloud connectivity using Active Directory Federation Services (ADFS) is identified
		2.8	Cloud connectivity of AD to Azure Active Directory (AAD) connect is performed
3	Define the basic structure of Windows security	3.1	Windows services and scheduled tasks are identified
		3.2	Differences between Local user and Local Administrator accounts is defined
		3.3	Function and role of Local Security the Authority Server Service (LSASS) in a Windows environment is identified
4	Investigate attack techniques on Microsoft end-points (workstations and servers)	4.1	Common end point attack techniques on end points are identified
		4.2	Privilege escalation using credential dumping tools are examined
		4.3	Common lateral movement techniques are identified
		4.4	Fileless attack tools and techniques on AD are defined
5	Investigate attack techniques on AD	5.1	Compromising methods for AD accounts are defined
		5.2	AD accounts that are attractive to compromise are identified
		5.3	Systems and processes to minimise compromising AD accounts are defined
		5.4	Tactics, techniques, and procedures (TTP's) used to compromise AD accounts are identified
		5.5	Insecure Windows protocols are identified
6	Investigate securing and defending AD from cyber attacks	6.1	Methods of securing AD are investigated
		6.2	AD monitoring tools and techniques for signs of compromise are investigated
		6.3	AD attack patterns determined from logs are identified
		6.4	Role of User and Entity Behaviour Analytics (UEBA) and Endpoint Detection and Response (EDR) tools are identified
7	Develop safe AD working practices	7.1	Methods to protect keyboard entries are investigated
		7.2	Clean source code build strategies are investigated
		7.3	Zero Trust mechanics processes are investigated
		7.4	Privileged access management principles are investigated
		7.5	Methods to harden the environment against compromise are examined
		7.6	Use of Credential Guard and how it protects LSASS memory is examined

Range of Conditions

Resources and tools are constantly being updated or replaced in this technology space. Where a resource or tool is no longer relevant or supported an updated resource or tool may be selected in its place. Those listed are examples at the time this unit was written.

- Logical structure of Active Directory (AD). Examples are:
    - Forests
    - Domains
    - DNS
    - Organisational Units (OUs)
- Physical structure of AD. Examples are:
    - domain controllers
    - AD sites
    - domain members (servers and workstations)
- Mechanics of AD. Examples are:
    - user and computer accounts
    - AD's Schema
    - FSMO roles
    - replication and ACLs on objects and OUs
- End point attack techniques. Examples are:
    - phishing
    - drive-by downloads
    - malicious Office Macros
    - reverse shells
    - Command and Control (C2) channels
- Privileged escalation tools. Example is:
    - Mimikatz and how they attack Local Security Authority Server Service (LSASS)
- Lateral movement techniques. Examples are:
    - Pass-the-hash attacks
    - Pass-the-ticket attacks
- Compromising Active Directory Accounts. Examples are:
    - abusing missing security updates
    - abusing Security Identifier (SID) history
    - Golden Ticket attack
    - stealing the ntds.dit database
    - offline cracking passwords
- Insecure Windows protocols. Examples are:
    - Server Message Block (SMBv1)
    - New technology LAN Manager (NTLMv1)
    - Windows Digest

- unsigned Lightweight Directory Access (LDAP) binds
- weak ciphers

- Securing Active Directory. Examples are:
  - reducing the attack surface
  - allocating least privilege
  - use secure administration workstations
- Monitoring Active Directory for signs of compromise. Review the following 1 article. (Monitoring Active Directory for Signs of Compromise | Microsoft Docs)
- Active Directory Attack patterns. Examples are:
  - suspicious logons
  - group membership updates
- Other References for Knowledge evidence include:
  - Zero trust mechanism (Zero Trust Security Implementation - Essentials Series - Episode 1 - YouTube)
  - Compromising techniques for AD (Monitoring Active Directory for Signs of Compromise | Microsoft Docs)
  - Privileged access management (Developing a privileged access strategy | Microsoft Docs)
  - Hardening your environment (ways to harden your environment against compromise - Microsoft Security Blog

Foundation Skills

Foundation skills essential to performance in this unit, but are *not explicit* in the performance criteria are listed here.

Skill	Description
Reading skills to:	Accurately interpret AD documents and other related information
Writing skills to:	prepare technical documents with appropriate language and detail for the intended readers

Unit Mapping information	New unit, no equivalent unit.

Assessment Requirements	
TITLE	Assessment Requirements for: **VU23308 - Identify Active Directory security concepts**
PERFORMANCE EVIDENCE	The candidate must demonstrate the ability to complete the tasks outlined in the elements, performance criteria and foundation skills of this unit, including evidence of the ability to: • set up and access Active Directory securely and implement security concepts to minimise vulnerabilities for two (2) common exploits.
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: • Logical structure of Active Directory (AD). (Refer Range of Conditions for examples). • Physical structure of AD. (Refer Range of Conditions for examples). • Mechanics of AD. (Refer Range of Conditions for examples). • End point attack techniques. (Refer Range of Conditions for examples). • Privileged escalation tools. (Refer Range of Conditions for examples). • Lateral movement techniques. (Refer Range of Conditions for examples). • Compromising Active Directory Accounts. (Refer Range of Conditions for examples). • Insecure Windows protocols. (Refer Range of Conditions for examples). • Securing Active Directory. (Refer Range of Conditions for examples). • Monitoring Active Directory for signs of compromise.(Refer article in Range of Conditions) • Active Directory Attack patterns. (Refer Range of Conditions for examples). • Zero Trust mechanics. • Privileged access management principles. • Methods to harden your environment.
ASSESSMENT CONDITIONS	Knowledge and skills assessment must be in a real or simulated workplace environment. If simulated it must reflect real workplace conditions with suitable facilities and equipment. Assessment must ensure access to: • computer equipment • networking equipment • relevant documentation • tools and equipment • Virtual software testing environment **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		**VU23309**	
UNIT TITLE		**Undertake vulnerability and penetration testing for information technology infrastructure**	
APPLICATION		This unit describes the performance outcomes, skills and knowledge to expand the testing capability for information technology (IT) infrastructure vulnerabilities. Skills in using advanced features of current toolsets in order to identify weaknesses in the security of an organisation's infrastructure are included. It requires the ability to utilise the Kali security testing platform and open source tools to provide a sound foundation to develop these skills. The unit applies to persons working as cyber security practitioners who use advanced testing tools to determine vulnerabilities in an organisation's web site. No licensing or certification requirements apply to this unit at the time of accreditation.	
PRE-REQUISITE UNIT		VU23301 - Manage penetration testing processes for an organisation	
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	Prepare for testing IT infrastructure	1.1	Processes and scope for conducting infrastructure vulnerability scanning and penetration testing are examined
		1.2	Processes for conducting infrastructure vulnerability scanning and penetration testing are developed
		1.3	Advantages, disadvantages, and dangers of penetration testing are identified
		1.4	Process of note taking during a penetration test is examined
2	Perform vulnerability scanning of the infrastructure	2.1	Features of the selected vulnerability scanning tool are examined
		2.2	Use of the selected vulnerability scanning tool is demonstrated
		2.3	Results for the vulnerability scan report are interpreted

		2.4	Identification of vulnerability remediation through patching or compensating controls is examined
3	Gather information using the testing tool	3.1	Information gathering using the Kali tools is demonstrated
		3.2	Open Source intelligence (OSINT) using Kali's tools is demonstrated
		3.3	Information gathering using Kali's testing tools is demonstrated
		3.4	Vulnerability intelligence value of gathered information is assessed
4	Identify misconfigurations and weaknesses in the infrastructure	4.1	Common areas of infrastructure misconfiguration and weaknesses are identified and examined
		4.2	Methods of exploiting misconfiguration and weaknesses are demonstrated
		4.3	Use of Kali's Database Assessment tools is demonstrated
		4.4	Use of rootkits and trojan backdoors are examined
5	Exploit infrastructure vulnerabilities	5.1	Auxiliary scanning to identify additional vulnerabilities using Kali's Metasploit tool is demonstrated
		5.2	Exploitation of identified vulnerabilities using Kali's Metasploit tool is demonstrated
		5.3	Range of Kali's Metasploit exploit payloads is examined
		5.4	Use of Kali's Metasploit encoders to hide payloads is demonstrated
		5.5	Creation of shell payloads using Kali is demonstrated
6	Escalate privileges	6.1	Access and privilege models in Windows and Linux systems are examined
		6.2	Use of Kali's Metasploit exploits to escalate privileges is demonstrated
		6.3	Use of open source proof of concept privilege escalation exploits is demonstrated
7		7.1	Remediation strategies to mitigate identified exploitable vulnerabilities are formulated

	Exploitable vulnerabilities are mitigated	7.2	Hardening guides for key technologies are examined

RANGE OF CONDITIONS:

Resources and tools are constantly being updated or replaced in this technology space. Where a resource or tool is no longer relevant or supported an updated resource or tool may be selected in its place. Those listed are examples at the time this unit was written.

- Kali's password cracking tools. Examples are:
    - Hydra
    - John-the-ripper
- Kali's database assessment tools. Example is:
    - Sqlmap

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:	accurately interpret documents and reports regarding features of current toolsets in order identify weaknesses in the security of an organisation's infrastructure
Writing skills to:	prepare technical documentation with appropriate language and detail for the intended audience
Oral communication skills to:	articulating relevant issues encountered in the work environment with other personnel

UNIT MAPPING INFORMATION	New unit, no equivalent unit.

Assessment Requirements	
TITLE	Assessment Requirements for: **VU23309 - Undertake vulnerability and penetration testing for information technology infrastructure of an organisation**
PERFORMANCE EVIDENCE	The candidate must demonstrate the ability to complete the tasks outlined in the elements, performance criteria and foundation skills of this unit, including evidence of the ability to: • undertake advanced penetration testing for vulnerabilities on at least two (2) different IT infrastructure. In doing so, the candidate must, interpret and apply the penetration testing process and use the Kali testing framework to determine exploitability of identified vulnerabilities

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:
	• Kali's information gathering tools
	• Kali's Metasploit exploitation tool
	• Kali's password cracking tools. (Refer Range of Conditions for examples).
	• Kali's database assessment tools. (Refer Range of Conditions for examples).
	• Common infrastructure vulnerabilities including:
	  ○ weak passwords
	  ○ excessive file and directory access
	  ○ credentials stored on disk
	  ○ open services.

ASSESSMENT CONDITIONS	Knowledge and skills assessment must be in a real or simulated workplace environment. If simulated it must reflect real workplace conditions with suitable facilities and equipment. Assessment must ensure access to: • organisation's IT infrastructures • Kali's tools • 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.