22334VIC

Certificate IV in Cyber Security

(Version 2)

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

Accredited for the period 1st July 2017 to 31st December 2022

VICTORIA State Government | Education and Training

Version	Date	Comment
Version 1	I July 2017	Initial accreditation (1st July 2017 to 30th June 2022)
Version 2	9 May 2022	VRQA approved short term (6 months) extension to the course accreditation period. (1st July 2017 to 31st December 2022)

No new students may be enrolled after 31 December 2022. Continuing students may complete their studies and receive the qualification for successful completion according to the transition arrangements specified by the relevant VET regulator.

Disclaimer

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

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

Third party sites

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

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

Contents

Section A: Copyright and Course Classification Information

1. Copyright owner of the course

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

2. Address

Executive Director
Higher Education and Workforce Development
Higher Education and Skills
Department of Education and Training (DET)
GPO Box 4367
MELBOURNE Vic 3001

Organisational Contact:

Manager, Training and Learning Products Unit
Higher Education and Workforce Development
Higher Education and Skills
Telephone: 131823
Email: course.enquiries@edumail.vic.gov.au

Day-to-Day Contact:

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

3. Type of submission

Accreditation

4. Copyright acknowledgement

The units of competency:

BSBWHS401	Implement and monitor WHS policies, procedures and programs to meet legislative requirements
BSBRES401	Analyse and present research information

are from the BSB Business Services Training Package administered by the Commonwealth of Australia.

The units of competency:

ICTICT418	Contribute to copyright, ethics and privacy in an ICT environment
ICTNWK401	Install and manage a server
ICTNWK416	Build security into virtual private networks
ICTNWK502	Implement secure encryption technologies
ICTNWK503	Install and maintain valid authentication processes
ICTNWK509	Design and implement a security perimeter for ICT networks
ICTNWK511	Manage network security
ICTNWK531	Configure an internet gateway
ICTPRG405	Automate processes
ICTPRG407	Write script for software applications
ICTSAS409	Manage risks involving ICT systems and technology
ICTSAS418	Monitor and administer security of an ICT system
ICTSAS505	Review and update disaster recovery and contingency plans

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

© Commonwealth of Australia

The unit of competency:

RIICOM301D Communicate information

is from the RII Resources and Infrastructure Industry Training Package administered by the Commonwealth of Australia.

© Commonwealth of Australia

5. Licensing and franchise

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

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

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

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

Request for other use should be addressed to:

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

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

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

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

6. Course accrediting body

Victorian Registration and Qualifications Authority (VRQA)

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

7. AVETMISS information

ANZSCO code:	313199	ICT Support Technicians
ASCED code:	0299	Other Information Technology
National course code:		22334VIC

8. Accreditation period

1st July 2017 to 31st December 2022

Section B: Course Information

1. Nomenclature	***Standard 1 AQTF Standards for Accredited Courses***
1.1 Name of the qualification	Certificate IV in Cyber Security
1.2 Nominal duration of the course	735 - 960 hours
2. Vocational or educational outcomes	***Standard 1 AQTF Standards for Accredited Courses***
2.1 Purpose of the course	The Certificate IV in Cyber Security is a technician level qualification that will provide graduates with the knowledge and a comprehensive set of technical skills that enables them to: - monitor the risk of cyber security attacks - implement appropriate software - use a range of tools and procedures to mitigate cyber security threats - protect an organisation from insider security breaches - develop systems to minimise network vulnerabilities and risks. Graduates of the course will be able to seek employment as cyber security practitioners in a range of commercial enterprises/organisations and government bodies**.**
3. Development of the course	***Standards 1 and 2 AQTF Standards for Accredited Courses***
3.1 Industry / enterprise/ community needs	The recent Australian cyber security strategy paper released May 2016; *Australia's Cyber Security Strategy – enabling innovation, growth & prosperity,* states the following: *"Like many nations Australia is suffering from a cyber security skill shortage. These particular skills are essential in our connected technology – enabled world and they are fundamental to this nation's success. At the global level in the information security sector it is expected to see a deficit of 1.5 million professionals by 2020".*[1] *For Australia to have the cyber security skills and knowledge to thrive in the digital age the Federal Government is:* - *addressing the shortage of cyber security professionals in the workforce through targeted actions at all levels of Australia's education system, starting with academic centres of cyber security excellence in universities and by increasing diversity in the workforce* - *working with the private sector and international partners to raise awareness of the importance of cyber security across the community".*[2]

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

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

Many Australian organisations are unaware of the risks they face in cyberspace. The government is committed to equipping Australians with the right cyber security skills and raising levels of cyber security awareness so all Australian can benefit from the opportunities presented in cyber space.

> "*Demand in Australia for cyber security services and related jobs such as legal services, insurance and risk management is expected to grow by at least 21 per cent over the next five years. There will be significant employment and career opportunities for those with appropriate skills. Currently there is a short fall in the number of people with the appropriate skills and a number of job vacancies in the private and public sectors are not being filled. The take up of ICT- related university degrees (often a precursor for cyber security professionals), has halved over the last decade and graduation rates have dropped*".[3]

The above statement, also from *Australia's Cyber Security Strategy – enabling innovation, growth & prosperity,* highlights there is insufficient awareness of the employment opportunities as well as the types of courses currently available to obtain the appropriate skills.

The shortfall in appropriate skills is further emphasised by the *Telstra Cyber Security Report - 2016* with the following quote:

> *"This year's survey highlighted the growing shortage of skilled security staff required to perform increasingly complex security tasks as one of the major challenges for organisations. 62% of organisations stated that they have too few information security professionals to implement security activities within their organisations. Skills that entailed security risk assessments and conducting forensic investigations were among the most lacking across all verticals with an average of 54.3% organisations indicating a shortage of skills in these areas. Asian organisations lacked more than their Australian counterparts across all areas on average.*
>
> *Our research reveals that the reasons for the hiring shortfall are less about funding, than an insufficient pool of suitable candidates. While the sophistication of cyber-threats and a broadening landscape that requires security oversight e.g. mobile devices, cloud-based services, and the Internet of Things and the skills to identify, analyse, manage and prevent cyber-related attacks are becoming more demanding.*
>
> *Despite increased industry demand for specific ICT skills, the take-up of ICT-related tertiary courses in Australia over the last decade has halved. A 2014 analysis by the Australian Financial Review of university course take-up by domestic undergraduate students since 2001 shows a 36% decline in students. While the mismatch between the needs of industry and tertiary graduate qualifications is a general one impacting the whole of the ICT industry, it particularly affects dynamic and rapidly changing areas of technologies which is specifically relevant for cyber security"*[4]

To address the skill shortage the government's Australian cyber security strategy paper states:

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

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

> *"To build tomorrow's workforce, the Federal Government will work in partnership with the private sector and academic institutions to improve cyber security education at all levels of the education system. This will help to ensure Australia develops a workforce with the right skills and expertise that can help all Australian take full advantage of the opportunities in cyber space. The most urgent need is for highly skilled cyber security professionals. Academic centres of excellence will enhance the quality of cyber security courses, teachers and professionals in Australia. The centres will deliver undergraduate and postgraduate cyber security education through a consistent curriculum and quality teaching. The profile of these centres will also help to inspire students to think about careers in cyber security and study STEM subjects (science, technology, engineering and mathematics) at school. In addition, the Government will work with the private sector, the States and Territories and Skill Service Organisations to support the expansion of cyber security training in Registered Training Organisations (RTOs) including TAFEs and potentially include the development of a cyber security apprenticeship.'*[6]

As part of the Government initiatives, Box Hill Institute received a substantial funding grant to develop, promote and enhance delivery of cyber security training and increase the placement of graduates into cyber security jobs. The current Certificate IV in IT course (ICT40115) was customized to strengthen its' cyber security focus. An extensive training needs analysis was undertaken in conjunction with industry organisations, which provided list of duties considered to be appropriate for a person working at entry level in cyber security. (See Appendix 1)

It was acknowledged that job titles use by the industry for the role vary considerable but for the purpose of creating a duties list the title of junior cyber security analyst was selected.

The duties identified for this role are:

- maintaining security control
- providing information on security implications
- monitoring and responding to security events
- reporting on security issues
- responding to security events
- working within teams
- communicating clearly
- applying security concepts
- identifying security weaknesses proactively
- maintaining business relationships.

Following on from the initial DACUM session a mapping exercise was undertaken to identify existing training package units available and to determine the gaps were new units were to be developed to cover all components of the

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

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

duties identified. In total 10 new units were developed to address the following knowledge and skills areas:

- networking basics required for cyber security
- IT skills required for cyber security
- system testing procedures
- introduction to data collection and analysis
- securing a web site
- introduction to cyber security
- implementing network security
- managing a cyber security system
- incident response plans
- cyber security project.

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

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

Membership of the Steering Committee comprised:

- Grant McKechnie (Chair) - NBN Co
- Craig Templeton - ANZ
- Matt Carling - Cisco
- Andreas Dannert – Information Systems, Audit and Control Association (ISACA)
- Pamela O’Shea – BAE Systems
- Helaine Leggat – Australian Information Security Association (AISA)
- Dominic Schipano – Communication, Information and Technology Training (CITT)
- Jamie Rossato – NAB

In attendance:

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

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

3.2 Review for re-accreditation	Not applicable
4. Course outcomes	***Standards 1, 2, 3 and 4 AQTF Standards for Accredited Courses***
4.1 Qualification level	*Standards 1, 2 and 3 AQTF Standards for Accredited Courses* This course is aligned with Level 4 of the Australian Qualifications Framework (AQF) in that graduates will have: • cognitive skills to identify and analyse risk of security attacks and recommend appropriate strategies to mitigate the attacks • cognitive, technical and communication skills to implement and use a range of tools and procedures to mitigate cyber security threats in a wide variety of contexts • specialist technical skills to apply solutions to a defined range of unpredictable problems by methodically verifying compliance of all aspects associated with network security • broad knowledge base of relevant Australian standards, codes of practice and industry guidelines on network security • ability to evaluate information from a variety of sources and analyse the data gathered on the network security to assess compliance • ability to take responsibility for own outputs and contributions as part of a team to maintaining an organisation's cyber security system and incident response plan. The Volume of Learning for the Certificate IV in Cyber Security is typically 0.5 - 2 years. This incorporates structured training delivery and opportunities for practice and reinforcement of skills including, self-directed study, research, project work and written assignments.
4.2 Employability skills	*Standard 4 AQTF Standards for Accredited Courses* The Employability Skills for the Certificate IV in Cyber Security are summarised in Table 1.

Table 1: Summary of the Employability Skills for the Certificate IV in Cyber Security

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

Employability Skills	**Industry/enterprise requirements for this qualification include the following facets. On successful completion of the course a graduate should be able to:**

Communication	• Listen to and interpret verbal information • Read and interpret relevant regulations, signs, labels and other relevant workplace documents associated with cyber security • Write reports as part of the inspection and testing requirements and investigations in network security • Negotiate complex issues with others • Speak clearly and directly on complex matters, when sharing data, requirements or other information relevant to inspection and testing outcomes in network security
Teamwork	• Provide leadership during activities as appropriate • Collaborate with others • Work with diverse range of people and as part of a team
Problem solving	• Identify and solve or report complex problems • 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 complex issues • Monitor and anticipate problems that may occur in the course of cyber security vulnerability inspection and testing activities
Initiative and enterprise	• Modify activities dependent on different situations • Respond appropriately to changes in equipment, standard operation procedures and the working environment • Take appropriate actions in a diverse range of cyber security incidents
Planning and organising	• Implement emergency plans, systems and procedures • Implement procedures for maintaining compliance with relevant work requirements • Collect and interpret information needed when undertaking inspection and testing of the network security • Organise and plan own activities • Manage time priorities
Self-management	• Interpret and apply relevant enterprise procedures • Establish and follow own work plans and schedules • Evaluate and monitor own work performance
Learning	• Adapt own competence in response to change • Update own knowledge and skills required for network security
Technology	• Use testing equipment and systems as required • Use computers and printers to prepare reports • Implement and monitor the application of OH&S procedures

4.3 Recognition given to the course	*Standard 5 AQTF Standards for Accredited Courses* This course is currently being independently assessed by the Australian Information Security Association (AISA) for endorsement on behalf of its' membershi
4.4 Licensing/ regulatory requirements	*Standard 5 AQTF Standards for Accredited Courses* There are no licensing or regulatory requirements relating to this course.

5. Course rules

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

5.1 Course structure

To be awarded the Certificate IV in Cyber Security participants must complete sixteen (16) units consisting of:

- ten (10) core units, plus
- six (6) elective units

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

Table 2: Course structure

Unit code	Field of Education code (six-digit)	Unit Title	Pre-requisite	Nominal hours
Core units:				
BSBWHS401	061301	Implement and monitor WHS policies, procedures and programs to meet legislative requirements	Nil	50
BSBRES401	080399	Analyse and present research information	Nil	40
RIICOM301D	080399	Communicate information	Nil	30
ICTICT418	029999	Contribute to copyright, ethics and privacy in an ICT environment	Nil	40
ICTPRG407	029999	Write script for software applications	Nil	40
VU21988	029901	Utilise basic network concepts and protocols required in cyber	Nil	80

		security		
VU21989	029901	Test concepts and procedures for cyber security	Nil	60
VU21990	029901	Recognise the need for cyber security in an organisation	Nil	60
VU21991	029901	Implement network security infrastructure for an organisation	VU21988 VU21990	80
VU21992	029901	Develop a cyber security industry project	ICTPRG407 VU21988 VU21989 VU21990	120
Total core unit hours				**600**
Elective units: Select 6 Units of Competency				
VU21989	029901	Secure a networked personal computer	Nil	60
VU21990	029901	Perform basic cyber security data analysis	Nil	20
VU21991	029901	Manage the security infrastructure for the organisation	Nil	80
VU21992	029901	Evaluate and test an incident response plan for an enterprise	Nil	40
VU21989	029901	Expose website security vulnerabilities	Nil	40
ICTNWK401	020113	Install and manage a server	Nil	40
ICTNWK416	020113	Build security into virtual private networks	Nil	20
ICTNWK502	020113	Implement secure encryption technologies	Nil	20
ICTNWK503	020113	Install and maintain valid authentication processes	Nil	25
ICTNWK509	020113	Design and implement a security perimeter for ICT networks	Nil	60

ICTNWK511	020113	Manage network security	Nil	80
ICTNWK531	020113	Configure an internet gateway	Nil	40
ICTPRG405	020117	Automate processes	Nil	40
ICTSAS409	029901	Manage risks involving ICT systems and technology	Nil	20
ICTSAS418	029901	Monitor and administer security of an ICT system	Nil	30
ICTSAS505	029901	Review and update disaster recovery and contingency plans	Nil	30
			Range of elective nominal hours	**135 - 360**
			Total nominal hours for the course	**735 - 960**

5.2 Entry requirements

Standard 9 AQTF Standards for Accredited Courses

There are no formal entry requirements for this course, although participants would be best equipped to achieve the course outcomes if they have the learning, reading, writing and literacy, and numeracy competencies to Level 3 of the Australian Core Skills Framework (ACSF). See http://education.gov.au/search/site/ACSF

Applicants who have a lower level of language, literacy and numeracy skills may require additional support to successfully complete the course.

6. Assessment Standards 10 and 12 AQTF Standards for Accredited Courses

6.1 Assessment strategy

All assessment, including Recognition of Prior Learning (RPL) must be compliant with:

- Standard 1, Element 1.5 of the Australian Quality Training Framework (AQTF): *Essential Conditions and Standards for Continuing Registration* or
- Standard 1, Clauses 1.1 and 1.8 of the *Standards for Registered Training Organisations (RTOs) 2015,* or
- The relevant Standards for Registered Training Organisations in effect at the time of assessment.

Assessment strategies must therefore ensure that:

- all assessments are valid, reliable, flexible and fair
- learners are informed of the context and purpose of the assessment and the assessment process
- feedback is provided to learners about the outcomes of the assessment process and guidance given for future options

	• time allowance to complete a task is reasonable and specified to reflect the industry context in which the task takes place. Assessment strategies should be designed to: • cover a range of skills and knowledge required to demonstrate achievement of the course aim; • collect evidence on a number of occasions to suit a variety of contexts and situations; • be appropriate to the knowledge, skills, methods of delivery and needs and characteristics of learners; • assist assessors to interpret evidence consistently; • recognise prior learning. • be equitable to all groups of learners. Assessment methods are included in each unit and include: • oral and/or written questioning • inspection of final process outcomes • portfolio of documentary on-site work evidence • practical demonstration of required physical tasks • Investigative research and case study analysis. Questioning techniques should not require language, literacy and numeracy skills beyond those required in this unit of competency. A holistic approach to assessment is encouraged. This may be achieved by combining the assessment of more than one unit where it better replicates working practice. Assessment of the imported unit must reflect the Assessment Requirements for the relevant Training Package.
6.2 Assessor competencies	*Standard 12 AQTF Standards for Accredited Courses* Assessment must be undertaken by a person or persons with competencies compliant with: • Standard 1.4 of the AQTF: *Essential Conditions and Standards for Continuing Registration,* and/or • Standard 1, Clauses 1.13, 1.14, 1.15, 1.16 and 1.17 of the *Standards for Registered Training Organisations 2015 (RTOs),* and/or • The relevant Standards for Registered Training Organisations in effect at the time of assessment. Assessors of the endorsed units of competence must meet the requirements for assessors specified in the relevant Training Package.

7. Delivery	***Standards 11 and 12 AQTF Standards for Accredited Courses***
7.1 Delivery modes	*Standard 11 AQTF Standards for Accredited Courses* The following range of delivery methods may be considered: • work-based training and assessment • RTO-based training and assessment • part RTO and part work based training and assessment • recognition of prior learning combined with further training as required. There are no restrictions on offering the program on either a full-time or part-time basis. Delivery methods should encourage collaborative problem solving incorporating practical applications and outcomes and include team based exercises where possible. Some areas of content may be common to more than one element/performance criteria and therefore some integration of delivery may be appropriate.
7.2 Resources	*Standard 12 AQTF Standards for Accredited Courses* General facilities, equipment and other resources required to deliver the proposed Certificate IV in Cyber Security include: • training facilities and equipment • access to computers and internet • relevant standards, texts and references • appropriate environmental safeguards • health and safety facilities and equipment • workplace or a simulated workplace environment, appropriate to the assessment tasks.

	Training must be undertaken by a person or persons with competencies compliant with: • Standard 1.4 of the *AQTF: Essential Conditions and Standards for Continuing Registration* and/or • Standard 1, Clauses 1.13, 1.14, 1.15, 1.16 and 1.17 of the *Standards for Registered Training Organisations 2015* (SRTOs) and/or • The relevant Standards for Registered Training Organisations in effect at the time of assessment.

8. Pathways and articulation	*Standard 8 AQTF Standards for Accredited Courses* At this stage there are no formal arrangements for articulation to other accredited courses or the higher education sector. It should be noted that an Advanced Diploma of Cyber Security is currently being developed and it is anticipated that graduates of the Certificate IV will be able to articulate into the higher level qualification with a number of credits. When arranging articulation providers should refer to the: *AQF Second Edition 2013 Pathways Policy* This course contains nationally endorsed units of competence. Participants who successfully complete any of these units will be able to gain credit into other qualifications containing these units in any future studies.
9. Ongoing monitoring and evaluation	*Standard 13 AQTF Standards for Accredited Courses* The Certificate IV in Cyber Security will be maintained and monitored by the Curriculum Maintenance Manager (CMM) - Engineering Industries. A formal review of the course will take place at least once during the period of accreditation and will be informed by feedback from: • course participants and graduates • teaching and assessing staff • industry representatives and associations. Any significant changes to the course resulting from course monitoring and evaluation procedures will be reported to the VRQA. Course maintenance and review procedures may also indicate that the course in total should be expired if a suitable qualification becomes available through the development, review or continuous improvement process of a Training Package.

Section C: Units of competency

Imported units of competency from Training Packages:

BSBWHS401	Implement and monitor WHS policies, procedures and programs to meet legislative requirements
BSBRES401	Analyse and present research information
ICTICT418	Contribute to copyright, ethics and privacy in an ICT environment
ICTPRG405	Automate processes
ICTPRG407	Write script for software applications
ICTNWK401	Install and manage a server
ICTNWK416	Build security into virtual private networks
ICTNWK502	Implement secure encryption technologies
ICTNWK503	Install and maintain valid authentication processes
ICTNWK509	Design and implement a security perimeter for ICT networks
ICTNWK511	Manage network security
ICTNWK531	Configure an internet gateway
ICTSAS409	Manage risks involving ICT systems and technology
ICTSAS418	Monitor and administer security of an ICT system
ICTSAS505	Review and update disaster recovery and contingency plans
RIICOM301D	Communicate information

Units of Competency:

VU21988	Utilise basic network concepts and protocols required in cyber security
VU21993	Secure a networked personal computer
VU21989	Test concepts and procedures for cyber security
VU21994	Perform basic cyber security data analysis
VU21990	Recognise the need for cyber security in an organisation
VU21991	Implement network security infrastructure for an organisation
VU21995	Manage the security infrastructure for the organisation
VU21992	Develop a cyber security industry project
VU21996	Evaluate and test an incident response plan for an enterprise
VU21997	Expose website security vulnerabilities

VU21988 - Utilise basic network concepts and protocols required in cyber security

Unit Descriptor

This unit provides a cyber security practitioner with an introduction to the skills and knowledge required to comprehend how data travels around the internet and the function and operation of protocols such as the Transmission Control Protocol/Internet Protocol (TCP/IP) suite and devices that facilitate this data transfer. The exposure to these protocols is at an introductory level in this unit.

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

Employability skills

This unit contains employability skills

Application of the Unit

This unit is applicable to individuals working as a cyber security practitioners and will support their ability to detect breaches in security infrastructure

ELEMENT	PERFORMANCE CRITERIA
1. Outline key network security concepts	1.1 ***Networking concepts*** that affect cyber security in a data network are defined 1.2 Differences between ***network security*** and ***cyber security*** are clarified 1.3 Open System Interconnection (OSI) and the Transmission Control Protocol (TCP)/***Internet Protocol (IP)*** models of data communication are defined**.** 1.4 Function and basic operation of protocols in the TCP/IP are defined 1.5 Organisation's security policy is reviewed 1.6 ***Business implications*** of cyber security breaches are introduced
2. Define key features of the TCP/IP and OSI models	2.1 Key protocols of the TCP/IP suite and OSI layered models are identified and demonstrated. 2.2 Binary number system and hexadecimal number systems are defined. 2.3 Conversions between number systems are demonstrated 2.4 Differences and commonalities between the OSI and TCP/IP Internet Protocol models are described and demonstrated 2.5 IPv4 and IPv6 (internet protocol versions 4 & 6) addressing schemes are demonstrated

	2.6	OSI Layer 1 standards are identified
	2.7	OSI Layer 2 Protocols, standards and addressing media access control addresses (MAC) for both local area networks (LANs) and wide area networks (WANs) are described and demonstrated
	2.8	OSI Layer 3 Routed and Routing addressing protocols are describes and demonstrated
	2.9	OSI Layer 4 Protocols and Real Time Protocols (RTP) with particular emphasis on security vulnerabilities are defined and demonstrated.
	2.10	OSI Layer 5 to 7 protocols and networking applications are defined and demonstrated
3. Implement and demonstrate the function and operation of key networking devices	3.1	Physical and logical network representations of a local area network are implemented
	3.2	Function and operation of network switches are described and implemented
	3.3	Function and operation of network routers are described, and implemented
	3.4	Function and operation of a firewall is described and demonstrated
	3.5	Function and operation of a wireless access point (WAP) is described, and implemented
	3.6	End to end network ***troubleshooting methodologies and commands*** are implemented and demonstrated.
4 Implement the components of a network security laboratory and testing environment	4.1	***Software tools*** for the testing environment are identified
	4.2	Use of virtualisation is described and demonstrated in the testing environment
	4.3	Interconnectivity of the virtualised tools is described and demonstrated
	4.4	Basic use of the ***testing environment*** is demonstrated
5 Present current examples of cyber network attacks and resources	5.1	Example of a current distributed denial of service (DDoS) attack is presented
	5.2	Example of a current ransomware breach is presented
	5.3	***Useful resources*** that increase industry's awareness of cyber security awareness are identified.

REQUIRED SKILLS AND KNOWLEDGE

Required skills

- Articulating issues arising from the operation of a network
- Applying numeracy skills to perform calculations in binary and hexadecimal number systems
- Base level problem solving to implement provided scripts for a switch and a router
- Reading and accurately interpreting documents and reports
- Operating a personal computer
- Basic level ability in network cabling
- Communicating with others to address cyber security network concepts and protocols

Required knowledge:

- OSI layered communication model
- TCP/IP layered communication model
- Media Access Layer (MAC) addresses
- Binary number system
- Hexadecimal number system
- Transmission Control Protocol (TCP) protocol
- User Datagram Protocol (UDP)
- IPV4 addressing
- Basics of IPV6 addressing
- Routers, switches, firewall fundamentals & wireless access points
- End to end test commands eg Ping, Traceroute
- Fundamentals of Cyber Security tools Wireshark, Kali, Netstumbler & Netstat
- Fundamental DOS & DDOS attack mechanisms
- Fundamental ransomware attack mechanisms
- Wireless LANs and their use and vulnerabilities
- Virtual images and their construction
- Fundamentals of a Scripting language eg Python

Range Statement

Networking concepts may include but not limited to:

- Topology in which local area networks (LAN) and a wide area network (WAN) are connected
- Connections involving equipment such as routers, switches, bridges and hubs using cables or wireless technology (Wi-Fi)
- Devices used in the computer network etc

Network security may include but not limited to:

- Components that constitute the security of the computer network such as:
    - network architecture
    - firewalls
    - malware detecting software etc

Cyber security may include but not limited to:

- Components that constitute the cyber security features of a business such as:
    - security hardware
    - data collecting software
    - malware detecting tools
    - incident response plans etc.

Internet Protocol (IP) may include but not limited to:	• TCP • PPP • Ethernet • ARP • RARP • IP • FTP • HTTP • DHCP
Business Implications may include but not limited to:	• Financial • Organisation processes and policies • Human resources • Work practises • Communication structures etc.
Troubleshooting methodologies and commands may include but not limited to:	• Common testing commands used in end to end troubleshooting such as: ○ Ping ○ Traceroute
Software tools used for the testing environment may include but not limited to:	• Wireshark • Metasploit • Kali • Netstumbler • Netstat etc.
Useful resources may include but not limited to:	• Current articles • Newspaper items • TV documentaries • TV series • Useful URL sites • Visiting industry practitioner etc.

EVIDENCE GUIDE

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

Critical aspects for assessment and evidence required to assess competency in this unit	Assessors must be satisfied that the candidate can: • demonstrate a working knowledge of network concepts and protocols required in cyber security • define key features of the TCP/IP and OSI models • demonstrate the interconnection and operation of key networking devices • implement the components of a network security laboratory and testing environment • identify current examples of cyber network attacks and resources available to increase awareness of cyber security.

Context of and specific resources for assessment

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

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

Method of assessment

Evidence can be gathered in a combination of ways including:

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

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

VU21993 - Secure a networked personal computer

Unit Descriptor	This unit provides base level skills and knowledge to configure an operating system on a personal computer, adding security, setting user level passwords and privileges to limit and identify user access – all required to increase protection of the end point from cyber security attacks. The unit also provides an overview of internet of things (IOT) devices, an introduction to computer networking virtualisation and base level Linux commands – deemed to be invaluable in using cyber security tools. No licensing or certification requirements apply to this unit at the time of accreditation.
Employability skills	This unit contains employability skills.
Application of the Unit	This unit is applicable to individuals intending to work as a cyber security practitioner.

ELEMENT	**PERFORMANCE CRITERIA**
1. Identify the role of personal computers and other computing devices in cyber security	1.1 Computer system components are identified and how they work together is explained. 1.2 Identification and selection of appropriate components for a computer system are selected 1.3 Configuration of specialised computer systems is described and demonstrated 1.4 Role of security relevant peripherals is defined 1.5 Common computer input output devices are identified 1.6 Emerging Internet of Things (IOT) devices are identified and demonstrated
2. Undertake preventative maintenance and base level troubleshooting procedures for a computer	2.1 ***Preventative maintenance*** procedures for a personal computer are described and demonstrated 2.2 Base level troubleshooting procedures are demonstrated
3 Configure and use a computer operating system and relevant applications	3.1 Operating system (OS) installation is performed 3.2 Operating system structure is examined 3.3 Appropriate security applications are installed and configured 3.4 Routine system management tasks with appropriate operating system tools are demonstrated

	3.5	Common preventative maintenance techniques for operating systems are described and demonstrated
	3.6	***Configuring access controls for the workstation*** is described and implemented
	3.7	Setting passwords and allocating privileges are described and implemented
	3.8	Basic operating system troubleshooting processes are explained and demonstrated
4. Configure and use virtualised images	4.1	Environmental requirements for installing the virtualisation software are reviewed
	4.2	Required services and ports, according to virtualisation software vendors are installed
	4.3	Environmental requirements to ensure virtual machines function are configured
	4.4	Remote client access to virtual machines is configured
5. Identify key concepts in networking	5.1	Key components of a computer network are identified
	5.2	Purpose and characteristics of networking standards are explained
	5.3	Changing the IP address in an operating system is performed
	5.4	Network connectivity between computers is configured and tested
6. Connect devices to networks	6.1	Process of connecting a computer to a wired and wireless network is demonstrated
	6.2	Purpose and characteristics of internet service provider (ISP) connection technologies are defined
	6.3	Cloud concepts and network host services are examined
	6.4	Preventative maintenance procedures for networks are demonstrated
	6.5	Base level troubleshooting methods for networks are described and demonstrated
7. Demonstrate base level Linux commands	7.1	Structure and characteristics of the Linux operating system environment are defined
	7.2	Use of ***base level Linux commands*** is defined and demonstrated

REQUIRED SKILLS AND KNOWLEDGE

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

Required skills

- Identifying the components and explain the operation of a personal computer
- Operating a personal computer
- Performing preventive maintenance and troubleshooting on personal computers.
- Installing Windows operation systems
- Performing management and maintenance of Windows operating systems
- Programing networking devices from provided scripts
- Reading and comprehending computer technology reports
- Securing user level access for a personal computer
- Identifying and using networking devices

Required knowledge:

- Hardware components of a personal computer
- Virtulisation concepts
- PC peripherals
- PC input output devices
- Internet of Things (IOT) devices
- Communication protocols for IOT devices
- Security issues relating to IOT devices
- Operating systems (Windows or Linux)
- Virtualization operation and structure
- Creating and configuring virtualised images
- Linux base level commands
- Networked device connections

Range Statement

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

Preventative maintenance may include but not limited to:

- Hardware tasks such as:
  - remove dust from fans, power supply, internal components and peripherals
  - clean the mouse, keyboard & display
  - check for loose cables.
- Software tasks such as:
  - review and install appropriate OS, security and driver updates
  - regularly scan for viruses
  - remove unwanted programs
  - scan for hard drive errors.

Configuring access controls for the workstation may include but not limited to:

- Regular password changes which define minimum password length and strength,
- Protecting key files with operating system features like group policies

Base level Linux commands may include but not limited to:

- Pwd (print current directory)
- Cd (change directory)
- Mkdir (make directory)
- Rmdir (remove directory)
- ls (list files)
- Rm file (removes file)
- lsblk (list block devices)
- Chmod (change file mode bits)

EVIDENCE GUIDE

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

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

Assessors must be satisfied that the candidate can:

- demonstrate preventative maintenance and base level troubleshooting procedures for a computer
- demonstrate the ability to configure and use a computer operating system and relevant applications
- demonstrate the ability to configure and use virtualised images for a computer
- identify key concepts in networking
- connect devices to networks
- demonstrate base level Linux commands.

Context of and specific resources for assessment

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

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

Method of assessment

Evidence can be gathered in a combination of ways including:

- observation of processes and procedures
- oral and/or written questioning on required knowledge and skills
- testimony from supervisors, colleagues, clients and/or other appropriate persons

- inspection of the final product or outcome
- portfolio of documented evidence.

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

VU21989 - Test concepts and procedures for cyber security

Unit Descriptor

This unit provides introductory skills and knowledge required to implement testing procedures for systems in an organisation. These involve application layer testing tools as defined by the Open Web Application Security Project (OWASP), network testing and monitoring tools. The unit examines common threats, ethical hacking principles and introduction to penetration testing, social engineering security issues, enumeration, port scanning, sniffers, footprinting, traffic sniffers and wireless LAN vulnerabilities and contains a solid treatment of intrusions.

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

Employability skills

This unit contains employability skills.

Application of the Unit

This unit is applicable to individuals intending or working as cyber security practitioners.

ELEMENT		PERFORMANCE CRITERIA
1. Identify typical cyber security application layer testing methodologies and tools	1.1	***Existing frameworks that identify common application layer vulnerabilities*** are investigated
	1.2	Most common application layer security vulnerabilities are identified
	1.3	Current policies to minimize the identified application layer vulnerabilities are enhanced.
2. Use networking security testing methodologies, tools and commands	1.1	***End to end testing commands*** for network continuity are demonstrated
	1.2	Systematic troubleshooting procedures for network connectivity are demonstrated
	1.3	Use of ***networking monitoring tools*** are demonstrated
3. Implement the lab testing environment	3.1	***Lab testing environment*** is configured
	3.2	Using end to end testing commands, the lab environment is tested for functionality
4. Identify common threats and mitigation strategies	4.1	Current Trojans, Virus's and Worms are identified
	4.2	Methods of Denial of Service (DOS) and Distributed Denial of Service (DDOS) attacks and corresponding mitigation strategies are investigated
	4.3	Methods of Domain Name Server (DNS) attacks and corresponding mitigation strategies are identified
	4.4	Zero day vulnerabilities are identified

	4.5	Common vulnerabilities and exposures (CVE’s) are defined
	4.6	***Heuristics as a methodology for string analysis*** and their corresponding toolset are identified
5. Demonstrate ethical hacking principles and procedures	5.1	Ethical hacking process and procedures are described
	5.2	Base level troubleshooting procedures are demonstrated
	5.3	Fundamentals of penetration testing are described
	5.4	Legal implications of hacking are explained
	5.5	Process of ***footprinting*** the computer systems of a company is examined
	5.6	Methodologies of ***Enumeration*** to gather system usernames are described
	5.7	Tools to ***port scan*** a computer system are demonstrated
	5.8	Methodologies of system hacking are described then demonstrated
	5.9	Common ***sniffing tools*** are describes and demonstrated
6. Identify security vulnerabilities of Wireless LANs (WLANs)	6.1	WLAN hardware vulnerabilities are identified
	6.2	WLAN software issues and vulnerabilities are determined
7. Demonstrate basic scripting for a cyber security environment	7.1	Introduction to ***scripting languages*** is demonstrated
	7.2	Scripts for testing tools are described and demonstrated
	7.3	Programming environment for compilation and libraries are identified
	7.4	Introduction to scripting basic programming language is described and demonstrated

REQUIRED SKILLS AND KNOWLEDGE

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

Required skills

- Using networking security testing methodologies, tools and commands
- Configuring lab testing environment
- Installing and configuring software packages for an outcome
- Interpreting results from software packages
- Communicating and contributing as a team member to solve networking problems

Required knowledge:

- Layer 3 test command
    - Ping
    - Traceroute
- Testing tools include (but not exhaustive). Other tools will be utilised to adapt to new technologies as required:
    - Wireshark
    - Kali
    - Netstumbler
    - Netstat
- Ethical Hacking
- Penetration testing
- Footprinting
- Enumeration
- Port Scanning
- System Hacking
- Trojans, Virus's and Worms
- Sniffing tools
- DOS & DDOS attacks methodology
- DNS attack methodologies
- Wireless LANs
- Scripting languages eg Pytho

Range Statement

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

Frameworks that identify common software vulnerabilities may include but not limited to:	• The Open Web Application Security Project (OWASP) • The Open Source Intelligence (OSINT)
End to end testing commands may include but not limited to:	• Ping and Traceroute
Networking monitoring tools may include but not limited to:	• Wireshark • Languard • Microsoft network monitor • Nagios • OpenNMS • Advanced IP Scanner
Lab testing environment may include but not limited to:	• A network • Wireshark • Kali • Netstumbler • Netstat

Heuristics as a methodology for string analysis may include but not limited to:

- Examples of modern scanning programs that include Heuristic methodology include:
    - Kapernsky
    - Norton,
    - Trend
    - McAfee

Footprinting may include but not limited to:

- Software examples that can be used for footprinting include:
    - advanced google
    - whois
    - netcraft
    - nslookup
    - dig
    - metagoofil
- Note: that these tools may change with new technology developments

Enumeration may include but not limited to:

- Examples include:
    - NBTscan
    - DumpSec
    - Legion
    - Nat
    - SMBScanner
    - NBTEnum
    - Netcat etc.

  Note: These tools may change with new technology developments

Port scan may include but not limited to:

- Hardware and software tools to scan the ports on a computer The most popular example is nmap

  Note: that these tools may change with new technology developments

Sniffing tools may include but not limited to:

- Examples are
    - Wireshark
    - Ethereal
    - Ettercap
    - tcpdump

  Note: that these examples may change with the development of new technology

Scripting languages may include but not limited to:

- Examples include:
    - JavaScript
    - ASP
    - JSP
    - PHP
    - Perl
    - Tcl
    - Python

  Python is the language of choice in Cyber security

EVIDENCE GUIDE

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

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

Assessors must be satisfied that the candidate can:

- demonstrate the ability to utilise networking security testing methodologies, tools and commands
- implement a lab testing environment
- identify common threats and mitigation strategies
- demonstrate ethical hacking principles and procedures
- identify security vulnerabilities of Wireless LANs (WLANs))
- demonstrate basic scripting for a cyber security environment.

Context of and specific resources for assessment

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

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

Method of assessment

Evidence can be gathered in a combination of ways including:

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

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

VU21994 - Perform basic cyber security data analysis

Unit Descriptor

This unit provides the knowledge and skills necessary for a cyber security practitioner to detect and recognize discrepancies in data by performing analysis. The unit covers the collection of data on a scenario and performing basic analysis and includes the process of breaking down the scenario to a set of subtasks which are examined for their effectiveness. The unit includes an introduction of databases as a repository for data and the vulnerabilities that exist and an introduction to software tools to supporting pattern recognition

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

Employability skills

This unit contains employability skills.

Application of the Unit

This unit is applicable to individuals intending to work as a cyber security practitioners and is deemed an essential foundation skill for managing live data threats.

ELEMENT	**PERFORMANCE CRITERIA**
1. Demonstrate the process of basic cyber security data analysis	1.1 Information for a provided scenario from ***alerts, logs or reported events*** is collected
	1.2 Strategy to process this data is developed
	1.3 Data to be processed is broken down into subtasks and a range of strategies are developed to analyse these subtasks.
	1.4 Options are evaluated and the most appropriate subtask selected
	1.5 Selected subtasks are implemented
	1.6 Effectiveness of the subtasks implementation is evaluated and modified as required
2. Examine the use of data bases as a repository for data	2.1 Use of a data bases is described and demonstrated
	2.2 Access to data in a database is demonstrated
	2.3 Database security vulnerabilities are identified
	2.4 Strategies for mitigating database vulnerabilities are investigated
	2.5 Concept of Big Data is explained and demonstrated
3. Identify discrepancies and anomalies in data sets	3.1 Detecting discrepancies in data is described and performed
	3.2 Pattern recognition is demonstrated

3.3 Detecting anomalies in data is identified

3.4 Software tools to support the detection of anomalies and discrepancies are demonstrated

3.5 Use of automation in data collection and analysis is explained

3.6 ***Common software tools to identify data patterns*** are identified and demonstrated

REQUIRED SKILLS AND KNOWLEDGE

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

Required skills

- Recognising patterns of data
- Using data recognition software tools
- Working as a team member to problem solve database vulnerabilities
- Reading and comprehending documented material and procedures
- Using a laptop or a workstation
- Installing and using software packages
- Foundational troubleshooting
- Planning and organizing tasks and subtasks
- Evaluating effectiveness of processes
- Affecting change to processes

Required knowledge:

- Sources of data:
  - Firewalls
  - Intrusion Detection systems (IDS)
  - Access Control Systems
  - Security and Event Management systems (SIEM)
- Database concepts
- Inputting data to a database
- Accessing data from a database
- Database security vulnerabilities
- Mitigation strategies to minimise database security vulnerabilities
- Big data concepts only
- Splunk as an example of software used in data analysis

Range Statement

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

Alerts, logs or reported events. may include but not limited to:	• Firewalls • Intrusion detection systems (IDS) • access control systems • Security and Event Management Systems (SIEM)
Common software tools to identify data patterns may include but not limited to:	• Mine • Splunk • Data Recon

EVIDENCE GUIDE

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

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

Assessors must be satisfied that the candidate can:

- collect data on a scenario and perform basic data analysis
- recognise discrepancies and anomalies in data sets
- examine the use of data bases as a repository for data
- use software tools to support the detection of anomalies and discrepancies.

Context of and specific resources for assessment

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

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

Method of assessment

Evidence can be gathered in a combination of ways including:

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

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

VU21990 - Recognise the need for cyber security in an organisation

Unit Descriptor

This unit provides introductory knowledge and skills to recognize threats, risks and vulnerabilities to cyber security in an organisation. It includes the threats an organisation encompasses such as networks, machines, applications, data, users and infrastructure. The unit also covers an introduction to common cyber security attack mechanisms and an introduction to identity and threat management as well as security issues surrounding Internet of Things (IOT) devices. Finally, the unit introduces the implementation of tools and systems an organisation can use to protect from cyber-attacks.

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

Employability skills

This unit contains employability skills

Application of the Unit

This unit is applicable to individuals intending to work as a cyber security practitioner

ELEMENT	PERFORMANCE CRITERIA
1 Define a cyber security framework for an organisation	1.1 Definition of information security is developed
	1.2 ***Threat sources*** for an organisation are identified
	1.3 Relationship between data, networks, machines, users and applications in an enterprise is defined
	1.4 Introduction to identity and access management (IAM) is clarified
	1.5 Security of physical infrastructure of the enterprise is identified and evaluated
2 Identify the need for cyber security	2.1 Reasons to protect online identity and personal data are clarified
	2.2 Reasons to protect an organisation’s data are explained
	2.3 Concept of ***cyber threat*** is defined
	2.4 Reasons for the need of cyber security professionals are explained

3 Identify common and emerging cyber security attacks, and techniques	3.1	Security vulnerabilities and malware are identified and demonstrated
	3.2	***Threat actors, threat vectors and threat goals*** are defined
	3.3	Techniques used by attackers to infiltrate a system are described and demonstrated
	3.4	Characteristics and operation of a cyber-attack are explained
	3.5	Trends of cyber threats are investigated
	3.6	Cyber-attacks on ***enterprise infrastructure*** are identified
	3.7	Examples of IOT devices are described and demonstrated
	3.8	Security vulnerabilities for IOT devices are defined
4 Implement methods to protect your data and privacy	4.1	Techniques to protect personal devices and data are described and implemented
	4.2	***Authentication techniques*** are identified and demonstrated
	4.3	Methods to protect personal devices from threats are implemented
	4.4	Methods and tools to safeguard personal privacy are defined
	4.5	Logical and physical access controls are defined and implemented
5 Implement methods to protect an organisation's data	5.1	Common equipment used to protect an organisation from cyber security attacks is identified
	5.2	Terms such as botnets, the cyber kill chain process and behavior based security in the context of cyber security protection methodologies are explained.
	5.3	Methods for protecting an organisation from cyber-attacks are developed and evaluated
	5.4	Introduction to behavior based approach to cyber security is presented
	5.5	***Incident response standards*** are defined

REQUIRED SKILLS AND KNOWLEDGE

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

Required skills

- Using a PC or Laptop computer and software tools
- Implementing methods to protect personal data and privacy
- Communicating and working in a team environment
- Problem solving threats and vulnerabilities
- Interpreting and following documented material and procedures
- Evaluating an organisation’s security policy document

Required knowledge:

- An enterprise security framework
- Current types of security vulnerabilities and malware
- Methods of cyber security attacks
- Methods to protect your own data and privacy
- Methods and tools used to protect an organisation’s data
- Internet of Things (IOT) devices
- Access management techniques
- Access controls
- Overview of the responsibilities and resources that standards and organisation bodies provide for an enterprise
- Cyber security risk

Range Statement

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

Threat sources may include but not limited to:	• network • data • applications • users • machines
Cyber threat may include but not limited to:	• Phishing • malicious coding • passwords attacks • outdated software vulnerabilities • removable media
Threat actors, threat vectors and threat goals may include but not limited to:	• *Threat actors* examples: o Criminals o Nation State o Hactivist o Insider etc. • *Threat vectors* examples: o Malware o Phishing o DOS attacks etc. • *Threat goals* examples: o Data steal

  - Data disrupt
  - Embarrass organisation etc.

Enterprise infrastructure may include but not limited to:

- Lighting
- HVAC
- programmable logic controllers (PLC's)
- IOT devices

Authentication techniques may include but not limited to:

- Authentication, Authorizing and Accounting (AAA)
- RADIUS

Incident response standards may include but not limited to:

- Standard ISO27035
- National Institute of Standards and Technology (NIST)
- European Union Agency for Network and Information Security (ENSISA)
- Information Security Forum (ISF)
- Standards for Information Assurance for Small to Medium Enterprises Consortium (IASME)
- National Cyber Security Centre - Australia (NCSC)

EVIDENCE GUIDE

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

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

Assessors must be satisfied that the candidate can:

- define a cyber security framework for an organisation
- explain the need for cyber security for an enterprise
- recognise current and emerging cyber security attack methods and techniques
- implement methods to protect personal data and privacy
- implement methods to protect an organisation's data.

Context of and specific resources for assessment

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

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

Method of assessment

Evidence can be gathered in a combination of ways including:

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

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

VU21991 - Implement network security infrastructure for an organisation

Unit Descriptor

This unit provides a sound working knowledge of the key features which make up the network security for an organisation.

The unit includes a detailed investigation of threats and mitigation techniques, network security architectures, introduction to firewall setup and configuration, intrusion prevention system (IPS) setup and operation as well as internetworking operating system (IOS) software features to harden routers and switches. The unit also investigates proxy server vulnerabilities, Wireless Lan (WLAN) security vulnerabilities and the application of Virtual Private Networks (VPN's) and cryptography fundamentals.

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

Pre requisite Unit/s

VU21988 - Utilise basic network concepts and protocols required in cyber security

VU21990 – Recognise the need for cyber security in an organisation

Employability Skills

This unit contains employability skills.

Application of the Unit

This unit is applicable to individuals intending to work as a cyber security practitioners.

ELEMENT		**PERFORMANCE CRITERIA**
1. Examine modern network security threats and attacks	1.1	Network security architectures is identified
	1.2	Select group of modern ***cyber security threats and attacks*** are examined in detail.
	1.3	Tools and procedures to mitigate the effects of malware and common network attacks are identified
2. Configure secure administrative access to network devices	2.1	Network security architectures is described, demonstrated and implemented
	2.2	Process of configuring secure administrative access to network devices is described and implemented
	2.3	Process of allocation user command privileges for network devices is described, demonstrated and implemented
	2.4	Secure management and network monitoring is implemented
	2.5	***Features to enable security on Internet Operating System (IOS) based routers*** are implemented

	2.6	Purpose of Authentication, Authorization and Accounting (AAA) procedures to access to network devices are described
	2.7	AAA authentication from a local server is implemented
3. Implement firewall technologies	3.1	Operation of access lists (ACL's) is described and implemented
	3.2	Function and operation of a firewall to mitigate network attacks is described and implemented
	3.3	Zone based policy firewall is demonstrated and implemented
	3.4	Tools to implement packet filtering are demonstrated and implemented
	3.5	Operation of inspection rules are described and demonstrated
4. Investigate new firewall technologies	4.1	Higher level packet inspection is performed
	4.2	Holistic approaches to traffic inspection are investigated
	4.3	Concept of dynamic updates for defending against new cyber-attacks are examined
	4.4	New firewall technology operation is demonstrated
5. Implement Intrusion prevention systems (IPS)	5.1	Securing a network with network based Intrusion Prevention System (NIPS) is examined
	5.2	Detecting malicious traffic using signatures is demonstrated
	5.3	Intrusion Prevention System (IPS) using an Internetworking Operating System (IOS) is defined and implemented
6. Examine proxy server security issues	6.1	Function and operation of a proxy server is summarized
	6.2	Proxy server vulnerabilities are identified
	6.3	Mitigation strategies for proxy server vulnerabilities are defined and demonstrated
7. Investigate Wireless security vulnerabilities	7.1	Operation of WLANs as a communication media is summarized
	7.2	Overview of the 802.11 WLAN standards is explained
	7.3	Relationship between the Data Layer and the Physical layers for WLANS is defined
	7.4	WLAN architecture of a typical system is defined and demonstrated
	7.5	Authentication and Association methods for wireless clients are described and demonstrated

	7.6 Strengths and weaknesses of WLAN encryption techniques are investigated
	7.7 ***Current tools to discover and interrogate WLANS*** are demonstrated and utilised
	7.8 WLAN security checklist is developed
	7.9 802.1x security authentication standards for WLANS (and wired devices) are summarized
8. Demonstrate the fundamental operation of Cryptographic systems	8.1 Overview of cryptography is provided
	8.2 Process of working with symmetric & asymmetric algorithms is defined
	8.3 Function and operation of encryption, hashes and digital signatures to secure a network is summarized
	8.4 Data integrity and authentication utilizing encryption algorithms are defined
	8.5 Data confidentiality utilizing encryption algorithms are summarized
	8.6 Process of public key encryption to ensure data confidentiality is demonstrated
	8.7 ***Cryptography standards and protocols*** are summarized
	8.8 Common use of ***protocols that utilize cryptography*** are demonstrated
9. Define and demonstrate the fundamentals of Virtual Private Networks (VPN's)	9.1 Advantages and operation of Virtual Private Networks (VPN's) are explained
	9.2 Operation of Internet Protocol Security (*IPSec)* VPN's is summarized
	9.3 Operation of tunneling is described and demonstrated
	9.4 Site to site IPSec VPN with pre shared key authentication is demonstrated

REQUIRED SKILLS AND KNOWLEDGE

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

Required skills

- Communicate and contribute as a member of a team
- Problem solve network security infrastructure
- Interpret and follow documented material and procedures
- Use a laptop or a workstation
- Install and demonstrate the application of software packages
- Perform basic mathematical calculations
- Connecting networked devices
- Configuring a firewall
- Implementing IPS
- Plan and apply foundational troubleshooting of network security infrastructure
- Drive testing software packages

Required knowledge:

- Testing methodologies
- Using networking devices
- New firewall technologies
- CLI to configure a network device
- Handle and use network devices
- WLAN operation and architectures
- WLAN vulnerabilities
- Encryption, hashes and digital signatures
- Encryption algorithms
- Public key encryption
- Basic Cryptography
- VPN's
- IPSec

Range Statement

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

Cyber security threats and attacks may include but not limited to:	• Types of malware • Trojans, • Spoofing • Phishing • Spear phishing Man in the middle • Password attacks • Emerging attacks
Features to enable security on Internet Operating System (IOS) based routers may include but not limited to:	• Configure secure administrative access • Configure command authorization using privilege levels • Implement secure management and monitoring of network devices • Implement automated features to enable security

Current tools to discover and interrogate WLANS may include but not limited to:

- Netstumbler
- Aerosol
- Airsnort

Cryptography standards and protocols may include but not limited to:

- A series of standards that define the function and operation of Cryptography (eg. X.509)

Protocols that utilize cryptography may include but not limited to:

- Secure Sockets Layer (SSL)
- Transport Layer Security (TLS)
- HTTP Secure
- Pretty Good Privacy (PGP)

EVIDENCE GUIDE

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

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

Assessors must be satisfied that the candidate can:

- identify network security threats and attacks
- configure securing network devices
- select and implement firewall technologies
- implement intrusion prevention systems;(IPS)
- identify proxy server security issues
- recognise Wireless security vulnerabilities
- demonstrate the fundamental operation of Cryptographic systems and Virtual Private Networks (VPN's).

Context of and specific resources for assessment

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

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

Method of assessment

Evidence can be gathered in a combination of ways including:

- observation of processes and procedures
- oral and/or written questioning on required knowledge and skills
- testimony from supervisors, colleagues, clients and/or other

appropriate persons

- inspection of the final product or outcome
- portfolio of documented evidence.

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

VU21995 - Manage the security infrastructure for the organisation

Unit Descriptor

The unit provides the basic knowledge and skills required to manage the implementation of the security infrastructure for an organisation. It includes assessing risk, implementing appropriate controls, monitoring their effectiveness, following organisation policy to store relevant data and compiled reports for future audit purposes.

The practitioner will monitor and evaluate the physical security infrastructure of the organisation, and implement a regular security infrastructure maintenance program.

It is likely that the practitioner will need to obtain relevant security clearance to handle this data.

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

Employability skills

This unit contains employability skills.

Application of the Unit

In the context of the unit it is acknowledged that managing, monitoring and evaluating aspects and practises of the organisations security infrastructure will be performed as part of a team. Advice may be provided for other groups within the organisation.

ELEMENT	PERFORMANCE CRITERIA
1. Identify the key features from information and security policies for an organisation	1.1 Information and security policy documents for the organisation are examined
	1.2 Implications of these policies are discussed and evaluated by the team
	1.3 Implications of the organisation’s work habits relating to its security policy are evaluated
	1.4 Implications of the organisation’s configuration and change management are evaluated
2. Determine risk category for the security infrastructure	2.1 Audit of existing tools and security infrastructure for the organisation is conducted
	2.2 Security infrastructure ***baseline*** is determined
	2.3 ***Risk assessment*** on the system is conducted as part of a team and associated risks categorised
	2.4 Risk assessment on human operations is conducted as part of a team and interactions with the system are categorised
	2.5 Risk plans are matched to risk categories

	2.6	Resources required by risk categories to minimise business operation are determined
3. Identify the physical security vulnerabilities of the organisation’s security infrastructure	3.1	Physical infrastructure of the organisation’s security infrastructure is identified
	3.2	Security infrastructure vulnerabilities are documented
	3.3	Security infrastructure vulnerabilities are communicated to appropriate management personnel
4. Implement appropriate security system controls for managing the risk	4.1	Effective controls to manage risk are devised and implemented
	4.2	Policies and procedures to cover user access of the system are developed
	4.3	If required, training in the use of system related policies and procedures is conducted
	4.4	High-risk categories are regularly monitored
	4.5	System breakdowns are categorised and recorded
	4.6	Security plan and procedures to include in management system are developed
	4.7	Security recovery plan is developed
	4.8	System controls to reduce risks in human interaction with the system are implemented
5. Monitor security infrastructure tools and procedures	5.1	Controls that manage risks are reviewed and monitored
	5.2	Risk analysis process based on security benchmarks from vendors is reviewed
6. Implement data and report storage in line with organisation policies	6.1	Data and report storage policies for the organisation are reviewed
	6.2	Incident reporting documentation according to the organisation’s policies is stored
	6.3	Relevant security clearances required by the security practitioner are obtained
7. Promote cyber security awareness in the organisation	7.1	Implications of the enterprise’s security policy for the enterprise are defined and evaluated
	7.2	Strategies to promote security policy awareness amongst the organisation are planned and implemented
	7.3	Security policy awareness strategies are evaluated for their effectiveness within the organisation and if required modified for increased impact
	7.4	Training to implement the organisation’s security policy practices is planned and implemented
8. Implement cyber hygiene principles	8.1	***Best practices in cyber hygiene*** are identified
	8.2	Cyber hygiene process is identified and implemented

REQUIRED SKILLS AND KNOWLEDGE

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

Required skills

- Communicate and contribute as a member of a team
- Problem solve an organisation security system
- interpret and follow documented material and procedures
- Use a laptop or a workstation
- Install and demonstrate the application of software packages
- Contribute to the evaluation of the organisation's security plan
- Contribute to the planning and development of an organisation’s security policy
- Perform risk assessment for cyber security for an organisation
- Interpret risk assessment data from appropriate standards bodies (ISO 27001 or NIST)
- Implement cyber hygiene processes for an organisation
- Document incident processes
- Communicate incident report succinctly and effectively

Required knowledge:

- Methods of cyber security attacks
- Methods and tools used to protect an organisation's data
- Cyber security risk management plans and policies
- Requirements of cyber hygiene processes
- Best practices in cyber hygiene processes
- Maintence procedures
- Malware scanners
- Virus Scanners
- Diagnostic tools eg.
    - MS Baseline Security Analyser (or equivalent)
    - MS Security Compliance Manager (or equivalent)

Range Statement

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

Baseline may include but not limited to:	• List of malware scanners • List of virus scanners • List of security infrastructure equipment • Baseline diagnostic tools ; o MS Baseline Security Analyser(or equivalent) o MS Security Compliance Manager (or equivalent)
Risk assessment may include but not limited to:	• Hardware systems • Laptops • Customer data • Intellectual property
Best practices in cyber hygiene may include but not limited to:	• Identify devices in the organisation • Prioritise, devices on risk sensitivity • Hardening security on devices

- Implementing security patches
- Sound data backup strategies
- Effective security training

EVIDENCE GUIDE

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

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

Assessors must be satisfied that the candidate can:

- undertake cyber security infrastructure risk assessment of an organisation’s system
- implement appropriate security system controls for managing risk
- develop and review an organisation’s security risk plans and policies
- store audit data and reports according to the organisation’s policies
- implement best practice in cyber hygiene.

Context of and specific resources for assessment

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

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

Method of assessment

Evidence can be gathered in a combination of ways including:

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

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

VU21992 - Develop a cyber security industry project

Unit Descriptor

The purpose of this unit is to undertake a project that simulates a real cyber security environment.

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

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

Pre-requisite Units

ICTPRG407 - Write scripts for software applications

VU21988 - Utilise basic network concepts and protocols required in cyber security

VU21989 – Test concepts and procedures for cyber security

VU21990 – Recognise the need for cyber security in an organisation

Employability skills

This unit contains employability skills.

Application of the Unit

This unit is applicable to individuals intending to work as a cyber security practitioner

ELEMENT	PERFORMANCE CRITERIA	
1. Determine context of business need or problem	1.1	Scope and system boundaries of the business problem are determined together with the problem solving methodology
	1.2	Background information is gathered and development of questions appropriate to business problem are prepared
	1.3	Objectives and expected outcomes to be achieved are identified and documented
	1.4	Key elements for project milestones are identified
	1.5	Work plan statement is developed
	1.6	Documentation for substantiation is submitted to relevant person/s
2 Establish project team	2.1	Team members for the project are selected
	2.2	Individual responsibilities for each team member are defined
	2.3	Team performance criteria is established
	2.4	Methodology of team performance measurement is defined

3. Support the project plan development	3.1	Process of identify tasks and resources needed to complete the project plan is determined
	3.2	Schedule of project tasks including realistic timeframes and costs is prepared
	3.3	Specific responsibilities to project team members are allocated
	3.4	Process to manage risks and/or unexpected events that may impact upon the project objectives and/or timelines is developed
4. Evaluate the suitability of the gathered resources	4.1	***Key components*** required from the provided design are identified
	4.2	Resources for the project are allocated
	4.3	Team members familiarise themselves with the operation of the selected resources and investigate in more detail where required, for project implementation
5. Implement the provided project design	5.1	Suitable systematic processes that implement the provided design are identified
	5.2	Each section of the provided design is implemented and tested for functionality according to prescribed test procedures
	5.3	Verification of end to end functionality of the design with ***team members*** input is performed
	5.4	Feedback to the system designer is provided
	5.5	System changes provided by the system designer are implemented
	5.6	Documentation for the process is prepared such as meeting minutes, reports, email trails and presentations

6. Support the development of an implementation plan	6.1	Implementation plan with minimal end user's disruption is developed and implemented
	6.2	Where appropriate, end user training is provider
7. Prepare documentation for publication	7.1	Completed technical documentation covering the scope of work is drafted and checked for accuracy
	7.2	Technical documentation is submitted for approval by appropriate person/s
	7.3	Technical documentation for publication is prepared, printed and distributed
8. Review team activities and performances	8.1	Team performance against objectives is reviewed
	8.2	Matters affecting policies, plans and other related issues are discussed regularly with the team
	8.3	Team members input during the decision making process is sought
	8.4	Proposed workplace changes and improvements to processes are determined with team members input
	8.5	Individual achievement of team members is recognized
	8.6	Team objectives against targets are validated
9. Support project completion and handover	9.1	Project timeframes, scope, cost and quality expectations are evaluated
	9.2	Project risks strategy is reviewed by team members
	9.3	Ability of project deliverables to meet project expectations are verified
	9.4	Support or maintenance documents if applicable are prepared
	9.5	Where appropriate end users are trained
	9.6	Final project sign-off from sponsor and key stakeholders is obtained from the client
	9.7	Project is closed and experience gained and lessons learnt are documented

REQUIRED SKILLS AND KNOWLEDGE

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

Required skills

- Assembling, participating in and coordinating a work team
- Communicating and problem solving within a team environment
- Evaluating the performance of a work team
- Developing a project implementation plan including realistic timelines and allocation of tasks for team members
- Establishing project risk assessment
- Gathering, testing and allocating project resources
- Testing concepts and procedures for cyber security
- Using procedures to identify data traffic anomalies
- Installing and using software packages
- Connecting cyber security equipment and networked devices
- Using basic Linux commands
- Interpret and writing basic scripts
- Preparing technical documentation
- Making presentation to clients

Required knowledge:

- Working in a team
- Testing methodologies
- Implementing provided designs
- Operating software testing packages
- Interconnecting virtual images
- Operating systems (Windows or Linux)
- Virtualisation operation and structure
- Creating and configuring virtualised images
- Using networking devices
- Configuring firewalls
- Implementing Intrusion Detection Systems (IDS) features to examine data for anomalies for a potential security threat
- Implement Intrusion Prevention Systems (IPS) to monitor data traffic
- Introductory red and blue teaming exercises
- Support the development of an implementation plan
- Contribute to the team performance evaluation
- Support the process of risk assessment
- Business implications of cyber security breaches

Range Statement

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

Key components may include but not limited to:

- Firewalls
- Virtual Images
- Software
- Hardware

Team members in this context are:

- *Red Teaming* (detecting network and system vulnerabilities – ethical hacking)
- *Blue Teaming* (defending against both real attackers and Red Team)

EVIDENCE GUIDE

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

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

Assessors must be satisfied that the candidate can:

- develop a network security infrastructure (project) and prepare a implementation plan that leads to a solution
- organise a work team
- function and solve problems in a work team environment
- gather resources for project implementation
- test resources for functionality and operation as required
- implement project according to the provided design
- test the system for functionality
- conduct team activities and evaluate team performance
- prepare project documentation and make a presentation to the client.

Context of and specific resources for assessment

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

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

Method of assessment

Evidence can be gathered in a combination of ways including:

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

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

VU21996 - Evaluate and test an incident response plan for an enterprise

Unit Descriptor

This unit provides the basic knowledge and skills for a cyber security practitioner to examine, as part of a team, an organisation's existing incident response plan (IRP) and expand it as necessary to more thoroughly deal with incidents. The unit includes forming the team, clarifying roles, interpreting an incident response plan (IRP), using red and blue teams to test the IRP, implementing an incident, evaluating the IRP for its effectiveness and developing improvement.

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

Employability skills

This unit contains employability skills.

Application of the Unit

This unit is applicable to individuals intending to work as a cyber security practitioners

ELEMENT		**PERFORMANCE CRITERIA**
1. Identify and gather members to form an incident response team	1.1	Enterprise staff are selected to form an ***incident response team (IRT)***
	1.2	Incident response team member's roles and responsibilities are defined
	1.3	Communication strategies of the IRT within the enterprise are clarified
	1.4	IRT reporting hierarchy is determined
	1.5	Business implications to the enterprise of cyber incidents are articulated
2. Define red, blue and purple team tasks	2.1	***Red teaming*** activities for incident responses are created
	2.2	***Blue teaming*** activities for incident responses are created
	2.3	***Purple teaming*** activities are defined
3 Plan the implementation of the organisation's incident	3.1	The organisation's ***incident management plan*** is evaluated

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

REQUIRED SKILLS AND KNOWLEDGE

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

Required skills

- Communicate and contribute as a member of a team
- Problem solve network security infrastructure
- Interpret and follow documented material and procedures
- Use a laptop or a workstation
- Install and demonstrate the application of software packages
- Perform basic mathematical calculations
- Plan and develop an Incident Response Plan (IRP) for the enterprise
- Plan and develop attack exercises to test a security system for vulnerabilities
- Plan and develop mitigation strategy to defend a security system form attacks
- Evaluating IRP effectiveness and implementing new strategies

Required knowledge:

- methods to protect your own data and privacy
- basic level penetration testing of the security system for an enterprise
- tools used to test a network for vulnerabilities For example: Kali Linux, Metasploit
- methods and tools used to protect an organisation's data
- the concept of red, blue and purple teaming
- discussing better IRP strategies

Range Statement

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

Incident Response Team (IRT) activities include:	• Virus infections • Hacker attempts and break-ins • Improper disclosure of confidential information to others • System service interruptions • Breach of personal information • Other events with serious information security implications
Red-teaming activities include:	• Developing plans and strategies to test the security systems for the enterprise (penetration testing).
Blue-teaming activities include:	• Developing plans and strategies to protect the security systems for the enterprise.
Purple-teaming activities include:	• Maximize the effectiveness of the Red and Blue teams

EVIDENCE GUIDE

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

Critical aspects for assessment and evidence required to assess competency in this unit	Assessors must be satisfied that the candidate can: • assemble an incident response team and allocate roles and responsibilities • plan responses to incidents according to prescribed processes defined in the organisation's incident response policy document • utilise a red team to attack a security system for prescribed incidents • utilise a blue team to implement mitigation strategies for prescribed incidents • evaluate the organisation's incident response plan to the prescribed incidents and recommend changes as determined.

Context of and specific resources for assessment

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

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

Method of assessment

Evidence can be gathered in a combination of ways including:

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

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

VU21997 - Expose website security vulnerabilities

Unit Descriptor

This unit provides the knowledge and skills required to ensure and maintain the security of an organisation's website by utilizing the outcomes of the Open Web Application Security Project (OWASP). Current penetration testing tools are also utilised to determine the vulnerabilities of a web site. Vulnerabilities are assessed and reported to appropriate personnel to minimize risk.

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

Employability skills

This unit contains employability skills.

Application of the Unit

This unit provides a sound introduction to the aspects of managing a cyber security system and is applicable to individuals intending to work as a cyber security practitioner

ELEMENT	PERFORMANCE CRITERIA	
1. Explain the HTTP protocol and web server architectures	1.1	Web application server architecture is explained
	1.2	Structure and operation of the HTTP protocol is described
2. Identify web site content	2.1	Technology stack of a web application and web server are identified
	2.2	***Web server scanner software and Web content scanner software*** are demonstrated and utilised
	2.3	Spidering for web applications and websites are described and demonstrated
3. Install web application proxy testing tools	3.1	Example of web application ***proxy testing tools*** are described and demonstrated
	3.2	Proxy testing tools for a proxy server are configured and installed
	3.3	Web application traffic is intercepted and logged with a ***web application testing tool suite***
4 Use current frameworks that identify common software vulnerabilities	4.1	***Existing frameworks that identify common software vulnerabilities*** are investigated

	4.2 Most common web security vulnerabilities are identified
	4.3 Methods to determine injection weaknesses (SQLi) for web applications are described and demonstrated
	4.4 Methods for basic Broken Authentication and Session Management weaknesses for web applications are described and demonstrated
	4.5 Methods for basic Cross Site Scripting (XSS) weaknesses for web applications are described and demonstrated
	4.6 Methods for Insecure Direct Object Reference weaknesses for web applications are described and demonstrated
5 Report web application vulnerabilities	5.1 Technical issues and assigning risk are identified
	5.2 Detailed reproduction steps are recognised
	5.3 Remediation steps are identified
	5.4 Penetration test report is written and presented to relevant technical persons
	5.5 An executive summary is prepared and provided to appropriate persons.

REQUIRED SKILLS AND KNOWLEDGE

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

Required skills

- Communicate and contribute as a member of a team
- Solve problems related to an organisation's website security vulnerabilities
- Ability to read and comprehend technical procedures and documents
- Use a laptop or a workstation
- Install and interpret software test packages
- Plan and present proposed solutions to a client
- Contribute to writing reports

Required knowledge:

- Website development functionality and operation
- Website vulnerabilities
- Basic level penetration testing of the website for an enterprise
- Website servers
- Server scripting
- Firewall features and operation
- Existing frameworks of reported software vulnerabilities
- HTTP structure
- Testing tools for website vulnerabilities (Penetration testing (PEN testing))
  - Nikto
  - DIRB
  - Burp Suite
- Open Web Application Security Project (OWASP) top 10 Web based vulnerabilities

Range Statement

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

Web server scanner software and Web content scanner software may include but not limited to:	• **Nikto** - an Open Source (GPL) web server scanner which performs comprehensive tests against web servers • **DIRB** - a Web Content Scanner which looks for existing (and/or hidden) Web Objects
Proxy testing tools may include but not limited to:	• Burp Suite • TestRail • Lagado
Web application testing tool suite may include but not limited to:	• The Burp Suite of tools • WebLoad • Apache JMeter • NeoLoad • LoadRunner
Existing frameworks that identify common software vulnerabilities may include but not limited to:	• Open Web Application Security Project (OWASP) • Open Source Intelligence (OSTINT)

EVIDENCE GUIDE

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

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

Assessors must be satisfied that the candidate can:

- describe HTTP Protocol and web server architectures
- identify web site content
- demonstrate web application proxy testing tools
- utilise a current framework to test for common software vulnerabilities and interpret the result
- prepare a written report on web application vulnerabilities.

Context of and specific resources for assessment

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

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

Method of assessment

Evidence can be gathered in a combination of ways including:

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

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

BOX HILL
INSTITUTE
Global Educators

Appendix 1 - Certificate IV in Cyber Security Report on a DACUM

Session held on Thursday 5th May 2016

Present:	Andreas Dannert	Deloitte Australia
	Roger Ward	Securekloud
	Craig Templeton	Head of Security Enablement, ANZ Bank
	Arno Brok	Australian Information Security Association
	Steve Besford	Box Hill Institute of TAFE
	Matt Carling	Cisco (Web ex)
Apologies:	Grant McKechnie	NBNCo
	Brett Winterford	CBA
	Jamie Rossato	NAB
Facilitator:	Sam McCurdy	Dewhurst Consultancy Pty Ltd
In attendance:	Jane Young	Box Hill Institute of TAFE
	Sally Gill	Box Hill Institute of TAFE
	George Adda	Box Hill Institute of TAFE

1. **Welcome:**
   Sam welcomed those present and briefly explained the purpose and procedure of the DACUM session, which was to establish a job profile for a selected cyber security job, from which a suitable training program can be developed.

2. **Establishing the range of relevant cybersecurity job titles:**
   The DACUM began by establishing the range of entry level job titles that exist within the cyber security industry. The following list of job titles was developed:

- Security Analyst (Junior)
- Pen Tester/Social Engineer
- Risk Analyst
- Incident Responder
- Security Operations Manager
- Network Security Analyst
- Security Assessor
- Treat Analyst
- Cyber Intelligence & Response Technologist (CIRT)
- Security Operation Centre Analyst (SOC)
- Business Continuity Analyst
- Security Designer

The group was then asked to select one of the job titles that best represented the work that a graduate of the proposed course might do, so that the duties and tasks for the job could be identified. The group unanimously selected the job of a junior Security Analyst.

3. **Establishing the duties of a junior Security Analyst:**
   The group was asked to identify the duties of the job by competing the sentence, “A junior Security Analyst is responsible for ……………………

   This resulted in the following list of duties being identified.

   - Maintaining security control
   - Providing information on security implications
   - Highlighting legal implications, including ethical behaviour
   - Monitoring security events
   - Reporting on security issues
   - Responding to security events
   - Working within teams
   - Communicating clearly
   - Applying security concepts
   - Identifying security weaknesses proactively
   - Maintaining business relationships

   In the ensuing discussion, it was determined that, “Highlighting legal implications, including ethical behaviour” should be removed from the list and that the following items should be integrated within the other duties.

   - Working within teams
   - Communicating clearly
   - Applying security concepts

   It was also suggested that the items on “monitoring” and “responding” to security events should be combined to read “Monitoring and responding to security events”.

4. **Establishing the tasks associated with each duty:**
   Each duty was then taken in turn and the tasks necessary to perform the duty effectively were identified by completing the sentence,” In order to perform the (duty) effectively, the junior Security Analyst must be able to...................

   This resulted in the following information.

   A Maintaining security control
   A1 Apply security concepts
   A2 Provide information on security implications
   A3 Follow standard operating procedures (SOPs)

   B Providing information on security issues
   B1 Communicate effectively in oral and written form
   B2 Maintain Professional Knowledge
   B3 Follow reporting procedures

C Monitoring and responding to security events
C1 Report on security issues
C2 Rectify security issues
C3 Suggest improvements
C4 Analyse security issues

D Maintain business relationships
D1 Communicate effectively with internal stakeholders (In oral and written form)
D2 Display a high degree of professional integrity
D3 Identify the implications of unethical behaviour

5. Required Skills and Knowledge

The skills and knowledge required to complete these tasks were then defined in a brain storming manner, resulting in the following information.

Knowledge:

- Basic understanding of threats and their implications
- Team work techniques
- Difference between threats and risks
- Basic statistics (This item was eventually removed after some debate)
- Network features and functions
- Operating systems
- Algorithms and programming
- Fundamentals of computer hardware
- Authentication mechanisms
- Conceptual understanding of databases
- Web application
- Defence In-depth and Kill Chain security concepts
- Security frameworks and standards
- Security capabilities
- Professional ethics

Skills:

- Working effectively in teams
- Applying sound computer skills
- Following professional ethics
- Applying analytical skills
- Demonstrating organising skills
- Displaying good interpersonal skills
- Interpreting technical specifications
- Solving problems
- Displaying effective communication skills
- Working independently

6. **Future action:**
   Sam advised that he would prepare a report on the DACUM session, which would be circulated to all the members of the group for their feedback and endorsement that it is an accurate record of the proceedings. This would also provide the opportunity to provide additional feedback on any issues that may have been overlooked at the DACUM session.

   When the feedback has been analysed, the Job Profile for the junior Security Analyst will be used to identify existing endorsed units of competency that can be used for training purposes and/or the need to write new units of competency to address any training gaps that may be identified.

7. **Conclusion:**
   Sam thanked the group for their valuable input to the DACUM process.

Appendix 2 - Glossary of Terms and Definitions:

Unit VU21988 - Utilise basic network concepts and protocols required in cyber security

Open system interconnection model (OSI) means:

- Open Systems Interconnection model (OSI model) is a conceptual model that characterizes and standardizes the communication functions of a computing system without regard to their underlying internal structure and technology

TCP/IP means:

- The TCP/IP is another conceptual model that characterizes and standardizes the communication functions of a computing system without regard to their underlying internal structure and technology

Transmission control protocol (TCP) means:

- It the main transport layer protocol used to facilitate the transfer of data between two devices

Security policy means:

- The policy the organisation has to describe the processes and procedures that are to be followed in the case of a security breach

Binary number system and ***hexadecimal number systems*** means:

- These are alternative number systems that are used in computer operatations

IPv4 and IPv6 means:

- The standards that describe internet protocol (IP) addressing schemes.

Physical and logical network representations means:

- **Physical network representation** conveys the cabling diagram of the network
- **Logical network representation** displays the network status of IP addresses for each device

Network switches means:

- Those devices which operate at layer 2 of the OSI or TCP/IP layers.

Network routers means:

- Those devices which operate at layer 3 of the OSI or TCP/IP layers

Firewall means:

- Devices that operate across layers 2, 3 & 4 of OSI or TCP/IP layers Firewalls can implement various rules to block certain traffic types or even inspect data packets – then apply controls on contents of incoming or outgoing data packets

Wireless access point (WAP) means:

- Those devices which send and receive data over Radio Frequency (RF) signals which allow network connection

Interconnectivity means:

- The method deployed that connects virtualised images (VM's)

Unit VU21993 - Secure a networked personal computer

Specialized computer systems means:

- Special built computer systems to meet a different or enhanced industry or business specification

Security relevant peripherals means:

- Peripherals that relate specifically to security, eg intrusion prevention system (IPS), Intrusion detection system (IDS) and firewalls

Internet of Things (IOT) means:

- Portable intelligent devices that can monitor or control some physical characteristics and can communicate with other devices via TCP/IP

Base level troubleshooting means:

- Methodology used to systematically tackle computer based problems eg could be bottom up, top down, divide and conquer etc

Operating system (OS) means:

- Environment used to run applications on your PC. This is usually a graphics user screen (GUI) or can be command line interface (CLI) eg Windows, MAC and LINUX are examples of OS's that can be driven with a GUI or a CLI

Appropriate security applications means:

- Include Firewalls, Malware detecting software, audio visual software and tools that enable the analysis and detection of specific data streams

Unit VU21989 - Test concepts and procedures for cyber security

Trojans, Virus's and Worms:

- These types of malware change regularly. Those that are investigated are to be current

Ethical hacking process and procedures means:

- A process defined to systematically hack a system. Ethical indicating that the purposes are for noble purposes in order to gather information in order to harden the system to be more robust to further attacks

Penetration testing means:

- The processes used to test the soundness of a computer system from security attacks or breaches

Unit VU21994 - Perform basic cyber security data analysis

Data bases means:

- Organised set of data. Scripting language like SQL is used to access this data

Big Data means:

- Big data is a term for data sets that are so large or complex that traditional data processing applications are inadequate to deal with them. Treatment of Big data here is at an introductory level

Pattern recognition means:

- Ability to recognise data patterns within larger data sets

Unit VU21990 - Recognise the need for cyber security in an organisation

Identity and access management (IAM) means:

- Framework for business processes that facilitates the management of electronic identities. The framework will include the technology needed to support identity management

IOT devices means:

- Internet of Things (IOT) is small and compact devices which are implemented to monitor or control infrastructure. They are connected to the IP network

Logical and physical access controls means:

- Methods used to verify user access to a building and a computer system

Botnets means:

- A botnet can be a number of Internet-connected computers communicating with each other on networked computers which communicate and coordinate their actions by command and control or by passing messages to one another. Often used in cyber attacks

The cyber kill chain process means:

- Model to reveal the stages of a cyber security attack from early detection to when these data patterns have been quarantined.

Behaviour based security means

- Approach to security that attempts to assess the risk that computer code is malicious based on characteristics and patterns.

Behaviour based approach means:

- Methodology utilizes previous behaviours to detect security breaches

Unit VU21991 - Implement network security infrastructure for an organisation

Authentication, Authorization and Accounting (AAA) means:

- A methodology to ensure higher protection for a network by authenticating against a known data base of users, authorizing the user and then monitoring (accounting) the session

Access lists (ACL's) means:

- A set of commands/rules that incoming data needs to meet before communication can occur. They are placed on incoming ports of network equipment

Firewall means:

- Is a hardware or software device that monitors the network traffic and can have rules implemented to monitor and control different traffic types. Many firewalls implement various forms of intrusion protection systems and examine data within a data packets

Zone based policy firewall means:

- Is a type of firewall with enhanced feature sets to inspect data within a packet

Network based Intrusion Prevention System (NIPS) means:

- The NIPS monitors the network for malicious activity or suspicious traffic by analysing the protocol activity.

Proxy server means:

- A proxy server is a server (a computer system or an application) that acts as an intermediary for requests from clients seeking resources from other servers.

802.11 WLAN standards means:

- *802.11* are a set of media access control (MAC) and physical layer (PHY) specifications developed by the Institute of Electrical and Electronic Engineers (IEEE)**.** The 802.11 are standards for implementing *wireless local area network* **(***WLAN***)** computer communication in the 900 MHz and 2.4, 3.6, 5, and 60 GHz frequency bands**.**

802.1x security authentication means:

- *802.1x* refers to a family of *specifications* developed by the IEEE to *secure* communication between authenticated and authorized devices for a WLAN's or a wired devices

Public key encryption means:

- Is a cryptographic system that uses two keys -- a *public key* known to everyone and a *private or secret key* known only to the recipient of the message

Internet Protocol Security (*IPSec*) means:

- *IPsec* is a protocol suite for secure Internet Protocol (IP) communications that works by authenticating and encrypting each IP packet of a communication session

Encryption, hashes and digital signatures means:

- *Encryption* is the conversion of data into a form, called a ciphertext, that cannot be easily understood by unauthorized people
- *Hashing* is the transformation of a string of characters into a usually shorter fixed-length value or key that represents the original string
- *Digital signature is* a digital code (generated and authenticated by public key encryption) which is attached to an electronically transmitted document to verify its contents and the sender's identity

Unit VU21995 - Manage the security infrastructure for an organisation

Controls to manage risk means:

- Controls are implemented to deal with the identified risks of a risk assessment evaluation

Security plan and procedures means:

- A security plan sets out the role and responsibility of the organisation and links this to the security practices required to ensure minimal disruption to its operation and resources.

Security recovery plan means:

- Also called a security and disaster recovery plan. This plan seeks to minimize disruption to an organisation upon any disaster albeit natural or contrived. In order for it to operate as usual. It will involve sound backup strategies in place for data recovery and potential relocation requirements.

A cyber hygiene process means:

- The methodology used to implement sound cyber hygiene practices

Unit VU21992 - Develop a cyber security industry project

Key components relates to:

- The components that constitute a Cyber security Operations Centre (CSOC) (Or equivalent test system) and the development of a sandbox test environment to test simulated data This may include:
    - Firewalls
    - Virtual Images
    - Software
    - Hrdware

Team members means:

- In this context team members refer to Red Teaming and Blue Teaming
- **Red Teaming** is a process designed to detect network and system vulnerabilities and test security by taking an attacker-like approach to system/network/data access. This process is also called ethical hacking since its ultimate purpose is to enhance security
- **Blue Teaming** refers to the internal security team that defends against both real attackers and Red Teams

Systematic processes means:

- Procedures used to evaluate and identify data traffic anomalies

Prescribed test procedures means:

- Processes to follow to test the system or subsystems. This may be prescribed or may need to be developed in accordance with the organisations documented procedures

Implementation plan means:

- This plan describes how to implement the design to the customers location providing minimal disruption

Project risks means:

- The risks in the project that will cause delays and over budget issues

Project sign-off means:

- The project hand over is complete so this document is signed by the customer/client

Unit VU21996 - Evaluate and test an incident response plan for an enterprise

Incident Response Team (IRT) means:

- An Incident Response Team is established to provide a quick, effective and orderly response to computer related incidents such as virus infections, hacker attempts and break-ins, improper disclosure of confidential information to others, system service interruptions, breach of personal information, and other events with serious information security implications

Red teaming means:

- Red teams may be external entities brought in to test the effectiveness of a security infrastructure. They may be internal as well. This is accomplished by emulating the behaviors and techniques of likely attackers in the most realistic way possible

Blue teaming means:

- Blue teams refer to the internal security team that defends against both real attackers and red teams

Purple teaming means:

- Purple teams exist to ensure and maximize the effectiveness of the Red and Blue teams

Incident management policy means:

- An organisation's incident management policy will contain defined processes to follow upon the detection of an incident

Unit VU21997 - Expose website security vulnerabilities

HTTP protocol means:

- Hypertext Transfer Protocol (HTTP) is an application protocol for distributed, collaborative, hypermedia information systems and is the foundation of data communication for the World Wide Web. It is part of the IP suite of protocols

Spidering means:

- Process of examining tools (Spiders) that visit Web sites and reads their pages and other information in order to create entries for a search engine index. The major search engines on the Web all have such a program

Injection weaknesses (SQLi) means:

- (SQLi) describes direct insertion of attacker-controlled data into variables that are used to construct SQL commands

Broken Authentication and Session Management means:

- Authentication and session management includes all aspects of handling user authentication and managing active sessions

Cross Site Scripting (XSS) means:

- Cross-site scripting (XSS) is a type of computer security vulnerability typically found in web applications

Insecure Direct Object Reference means:

- Insecure direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory or database key

Penetration test report means:

- A report documenting the results of the outcomes of the penetration testing of the system