

CYBER SECURITY ARTICULATION PROPOSAL PACK



APC CYBER SECURITY COURSE OUTLINES

22603VIC CERTIFICATE IV IN CYBER SECURITY

22610VIC ADVANCED DIPLOMA OF CYBER SECURITY



AUSTRALIAN
PACIFIC COLLEGE

Table of Contents

Introduction	3
About Australian Pacific College	4
Part 1: Training and Assessment	5
22603VIC Certificate IV in Cyber Security	5
22610VIC Advanced Diploma of Cyber Security	11
Part 2: Course Outlines	20
22603VIC Certificate IV in Cyber Security	20
22610VIC Advanced Diploma of Cyber Security	44

22603VIC Certificate IV in Cyber Security

Aims

The Certificate IV in Cyber Security is a technician-level course. It provides participants with knowledge and a range of technical skills to enable them to seek employment as a cyber security technician in a range of organisations and government bodies.

The course aims to equip the learners with the skills and knowledge to meet the following vocational/industry outcomes of the course:

- ability to respond to and monitor cyber security events in an organisation
- ability to use a range of tools and procedures to mitigate cyber security threats
- ability to protect an organisation from insider security breaches
- ability to develop systems to minimise network vulnerabilities and risks
- ability to recognise implications using cloud-based services
- ability to work effectively as a member of a cyber security team.

Job roles

Possible job roles for students who have completed this qualification is:

- cyber security technician

Duration

The expected duration for the 22603VIC Certificate IV in Cyber Security is 4 terms. Students who are identified as having difficulties in completing the course in the required duration may be able to extend their course as per APC's Intervention Policy. NOTE: Due to College closure over the Christmas/New Year period the maximum course length for students studying at this time is 49 weeks.

Entry requirements

ACADEMIC

- There are no essential entry requirements for the 22603VIC Certificate IV in Cyber Security.

ENGLISH LANGUAGE PROFICIENCY

- Satisfactory completion of General English at an Upper Intermediate level
- or
- equivalent English language proficiency test results.

Materials

The required texts for this course are the Australian Pacific College workbooks. You have access to your workbooks for all classes. These workbooks are provided to you free of charge in a pdf version in myAPC.hub and you can download them to your device.

Course structure

Australian Pacific College (APC) students are taught 12 subjects made up of 16 Units of Competency. The full length of the course is 4 terms. A student will study the relevant competencies as outlined by the training package and only after the award requirements have been met does APC award the qualification.

Subject code and name	Unit of Competency
-----------------------	--------------------

A50523 Work Health and Safety (WHS)	BSBWHS309 Contribute effectively to WHS communication and consultation processes
A50524 Basic Network Concepts and Cyber Security Foundations	VU23213 Utilise basic network concepts and protocols required in cyber security
	VU23214 Configure and secure networked end points
A50525 Research and Information Analysis	BSBINS401 Analyse and present research information
A50526 Cyber Security Legislation and Ethical Practices	VU23223 Apply cyber security legislation, privacy, and ethical practices
A50532 Windows security	VU23225 Investigate Windows security features
A50533 Industry Project and Cyber Security Awareness	VU23217 Recognise the need for cyber security in an organisation
	VU23220 Develop and carry out a cyber security industry project
A50534 ICT industry	ICTICT443 Work collaboratively in the ICT industry
A50527 Incident Response Plans	VU23221 Evaluate and test an incident response plan for an enterprise
A50528 Website Vulnerability	VU23222 Expose website security vulnerabilities
A50529 Data analysis and testing	VU23216 Perform basic cyber security data analysis
	VU23215 Test concepts and procedures for cyber security
A50530 Security infrastructure	VU23218 Implement network security infrastructure for an organisation
	VU23219 Manage the security infrastructure for an organisation
A50531 Cloud Security Systems	VU23224 Identify the implications of cloud-based security systems

Assessment Schedule

Information about your assessments is included in the Student Workbooks and Assessments for each subject. This information explains the assessment requirements and what you need to do to complete the assessments.

Assessments should be submitted on the due date. Your trainer will give you more comprehensive information about each assessment task.

You are required to complete all parts of the assessment and tick the declaration that it is all your own work i.e., that you have not plagiarised by copying from the internet or other sources. You are required to be competent in each unit of competency to achieve your qualification.

Note: Please refer to individual assessment sheets or ask your teacher for further information on the units of competency and the Elements (Elements describe the essential outcomes) and Performance

Criteria (Performance Criteria describe the performance needed to demonstrate achievement of the element) as listed below:

Unit Overview

Unit of Competency	Element	Performance Criteria
BSBWHS309 Contribute effectively to WHS communication and consultation processes	1. Participate in establishing consultation processes	1.1 Contribute to selecting WHS consultation and communication methods aligned to organisational policies and procedures, and compliant with WHS legislative requirements 1.2 Identify and record key stakeholders according to WHS laws and related documentation 1.3 Research and collate information on organisational WHS obligations relating to communication and consultation with required personnel 1.4 Assist with any required revisions to consultation and communication methods according to organisational policies and procedures 1.5 Participate in consultation with required personnel to agree any proposed consultation and communication methods
	2. Contribute to WHS consultation	2.1 Contribute to facilitating WHS consultation and participation processes according to WHS laws 2.2 Identify and report barriers to effective WHS consultation and participation processes to required personnel according to organisational policies and procedures 2.3 Make suggestions that could assist in removing identified barriers to effective WHS consultation and participation processes, according to organisational policies and procedures 2.4 Identify, record and communicate to others, the duties, rights and responsibilities of required personnel in the consultation process
	3. Consult and communicate effectively with required personnel	3.1 Identify appropriate forms of communication for required individuals and/or parties 3.2 Convey WHS information to required personnel in plain language and according to organisational policies and procedures 3.3 Participate in confirming that required personnel understand WHS information, instructions and signs

Unit of Competency	Element	Performance Criteria
	4. Raise WHS issues with required personnel	4.1 Raise relevant WHS issues in meetings and support others to do so 4.2 Record and communicate WHS discussions and their outcomes according to organisational policies and procedures 4.3 Follow up meeting outcomes according to own job role, and organisational policies and procedures 4.4 Communicate WHS-related outcomes of meetings to required individuals and/or parties
VU23213 Utilise basic network concepts and protocols required in cyber security	1. Outline key network security concepts	1.1 Network vulnerabilities that affect cyber security in a data network are defined 1.2 Differences between network security and cyber security are clarified 1.3 OSI and TCP/IP models of data communication are defined 1.4 Organisation/enterprises' security policy is sourced reviewed 1.5 Business implications of cyber security breaches are identified
	2. Define key features of the TCP/IP suite of protocols	2.1 Binary number system and hexadecimal number systems are defined 2.2 Conversions between number systems are demonstrated 2.3 IPv4 and IPv6 (internet protocol versions 4 & 6) addressing schemes are identified 2.4 Differences and commonalities between the OSI and TCP/IP models are described and demonstrated 2.5 Key protocols of the TCP/IP suite are identified and demonstrated 2.6 TCP/IP Network Interface Layer standards are identified 2.7 TCP/IP Internet Layer standards and protocols are defined and demonstrated 2.8 TCP/IP Transport Layer Standards and protocols are defined and demonstrated 2.9 TCP/IP Application Layer standards and protocols are identified and demonstrated with particular emphasis on how TLS and HTTPS can provide security for network communications

Unit of Competency	Element	Performance Criteria
	3. Define services, standards and protocols that facilitate security and the functional operation of a network	3.1 Server Message Block (SMB) in the local area network are defined and demonstrated 3.2 Use of Quick (QUIC) User Datagram Protocol (UDP) to establish more secure HTTP traffic is investigated 3.3 Narrowband Internet of Things (NB-IoT) and Long Range IoT (LoRa-IoT) standards for IoT devices are investigated
	4. Implement and demonstrate the function and operation of key networking devices	4.1 Physical and logical network representations of a local area network are implemented 4.2 Function and operation of network switches and network routers are described and implemented 4.3 Function and operation of a firewall is identified 4.4 Function and operation of a wireless access point (WAP) and a wireless enabled end point is described and implemented 4.5 End to end network troubleshooting methodologies and commands are demonstrated
	5. Implement the components of a network security laboratory and testing environment	5.1 Software tools for the testing environment are identified and implemented 5.2 Use of virtualisation is described and demonstrated in the testing environment 5.3 Interconnectivity of the virtualised tools is described and demonstrated 5.4 Use of the testing environment is demonstrated
	6. Present current examples of cyber network attacks and resources	6.1 Example of a Distributed Denial of Service (DDoS) attack is presented 6.2 Example of a current ransomware breach is presented 6.3 Example of Local Area Network (LAN) Address Resolution Poisoning (ARP) is presented 6.4 Useful resources that increase industry's awareness of cyber security awareness are identified
VU23214 Configure and secure networked end points	1. Identify the role of personal computers and other computing devices in cyber security	1.1 Computer system components are identified and how they work together is explained 1.2 Role of security relevant peripherals is defined 1.3 Common computer input output devices are identified 1.4 Emerging Internet of Things (IOT) devices are identified and demonstrated

Unit of Competency	Element	Performance Criteria
		1.5 Security concerns for the network due to the inherent lack of security of IoT devices is identified
	2. Undertake preventative maintenance and base level troubleshooting procedures	2.1 Preventative maintenance procedures for a personal computer are described and demonstrated 2.2 Base level troubleshooting procedures for the operation of a personal computer are demonstrated
	3. Configure and use a computer operating system and relevant applications	3.1 Computer Operating System (OS) installation is performed 3.2 Structure of the OS for a personal computer is examined and the function of the components are explained 3.3 Security applications for a personal computer are installed and configured 3.4 Routine system management tasks with appropriate operating system tools are demonstrated 3.5 Common preventative maintenance techniques for operating systems are described and demonstrated 3.6 Configuring access controls for a personal computer is described and implemented 3.7 Setting passwords and allocating privileges for the operating system are described and implemented
	4. Define principles of safe software upgrade security practises	4.1 Models of resource access for a computer system are identified 4.2 Client/Server and Client/Client security issues are explained 4.3 Strategies for updating software for a Client/Server to minimise security risks are investigated
	5. Configure and use virtualised images	5.1 System requirements for installing the virtualisation software are reviewed 5.2 Required services within the virtualised environment are installed 5.3 System requirements to ensure virtual machines function are configured 5.4 Remote client access to virtual machines is configured

Unit of Competency	Element	Performance Criteria
	6. Identify key concepts in networking personal computers	6.1 Key components of a computer network are identified 6.2 Purpose and characteristics of networking standards are explained 6.3 Changing the IP address in an operating system is performed 6.4 Network connectivity between computers is configured and tested
	7. Connect devices to networks	7.1 Setting the IP address in an operating system is performed 7.2 Network connectivity between wired computers is configured and tested 7.3 Connectivity to an Internet Service Provider (ISP) from a wired Local Area Network (LAN) is demonstrated 7.4 Base level troubleshooting methods for wired networks are demonstrated 7.5 Network connectivity using a Wireless LAN (WLAN) is demonstrated 7.6 Connectivity to an ISP from the WLAN is demonstrated 7.7 Base level troubleshooting methods for WLAN networks are explained and demonstrated 7.8 Connectivity to an ISP from the WLAN is demonstrated
	8. Demonstrate base level Linux commands	8.1 Linux Operating system installation on a personal computer is performed 8.2 Structure and characteristics of the Linux operating system environment are defined 8.3 Linux security applications are identified 8.4 Basic system administration using Linux commands is performed 8.5 Linux commands to enable the personal computer to communicate with other devices in a network are defined and implemented
BSBINS401 Analyse and present research information	1. Identify and confirm research strategy	1.1 Identify research objectives according to organisational requirements 1.2 Identify potential sources for research information relevant to organisation requirements 1.3 Assess reliability of potential sources

Unit of Competency	Element	Performance Criteria
		1.4 Identify and confirm information research strategy is relevant to the research objectives
	2. Collect and store research information	2.1 Access and extract relevant information in a format suitable for analysis and distribution according to research strategy 2.2 Store research information according to security requirements and organisational policies and procedures
	3. Analyse and synthesise research information	3.1 Analyse stored information according to research strategy 3.2 Identify themes and draw conclusions according to research strategy 3.3 Demonstrate that assumptions and conclusions used in analysis are clear, justified, supported by evidence and consistent with research strategy
	4. Present research information	4.1 Identify methods of reporting that align with the intended audience and relevant organisational requirements 4.2 Draft research report on findings 4.3 Facilitate review of draft report according to organisational policies and procedures 4.4 Distribute research report according to organisational policies and procedures 4.5 Obtain feedback and comments on suitability and sufficiency of findings in accordance with organisational requirements
VU23223 Apply cyber security legislation, privacy, and ethical practices	1. Review the cyber security legislative and regulatory landscape for Australian organisations	1.1 Current Federal, State & Territory, and sector specific cyber security legislation is identified 1.2 International legislation that impacts Australian organisations is identified 1.3 Interdependencies between various legislative instruments, key regulators and their impact to Australian organisations is investigated and clarified 1.4 Current reforms in privacy, consumer and surveillance legislation are identified
	2. Examine an organisations policies and procedures for compliance with relevant standards	2.1 An organisations policies and procedures are identified 2.2 An organisations policies and procedures are reviewed for compliance in accordance with current standards 2.3 Organisational practises

Unit of Competency	Element	Performance Criteria
	3. Review the ethical practises and procedures for an organisation	3.1 Ethical practises developed by employees in using red and blue teaming tools are identified 3.2 Consequences of misuse of skills developed by employees in using red and blue teaming tools in public networks are explained 3.3 Consequences of unauthorised access to devices are investigated 3.4 Consequences of using file sharing services and tools to download and bypass copyright of various media or applications is explained 3.5 An ethical code of practise for cyber security technicians working in an organisation is prepared and implemented
VU23225 Investigate Windows security features	1. Examine the structure of the Windows Operating System	1.1 File system formats and layouts are identified 1.2 Purpose and structure of the registry is examined 1.3 Program execution in the form of processes and threads is examined 1.4 Role of the Dynamic Link Loader (DLL) is explained 1.5 Role of the task scheduler is identified and demonstrated
	2. Examine System Administration tools	2.1 Setting administration privileges is demonstrated 2.2 Windows event logs are identified 2.3 Windows Management Interface (WMI) is explained
	3. Investigate tools used to examine basic Windows attacks	3.1 Tools to detect malware attacks are investigated 3.2 Malware that reappears after being deleted is identified and exposed 3.3 Common malware hiding techniques are identified and explained
	4. Investigate the function and role of a Security Operation Centre (SOC) and Security Information Event Management (SIEM) tool	4.1 Types of SOC models are identified 4.2 Central storage of log files is defined 4.3 SIEM tool structure is defined 4.4 Commands to use a SIEM tool are demonstrated 4.5 Process to import log files to a SIEM tool is demonstrated

Unit of Competency	Element	Performance Criteria
	5. Examine methods to collect data from multiple end points into a SIEM tool	5.1 Log files created on a Windows end point are identified 5.2 Importing log files from a Windows client to a SIEM tool is demonstrated 5.3 Basic threat hunting is performed 5.4 Process of querying the data in the SIEM tool is explained
	6. Implement mitigation strategies for threats	6.1 Sources of mitigation strategies are identified 6.2 Mitigation strategies on detected threats are applied
VU23217 Recognise the need for cyber security in an organisation	1. Identify the need for cyber security for an organisation	1.1 Reasons to protect online identity and personal data are clarified 1.2 Reasons to protect an organisation's data are explained 1.3 Cyber security awareness practices for an organisation are identified 1.4 Concept of cyber threat is defined 1.5 Reasons for the need for cyber security professionals are explained
	2. Investigate common and emerging cyber security attacks, and techniques	2.1 Difference between threat actors, threat vectors and threat goals are clarified 2.2 Techniques used by attackers to infiltrate a system are described 2.3 Characteristics and operation of a cyber-attack are explained 2.4 Trends of cyber threats are examined 2.5 Cyber attack methods on an organisation infrastructure are identified 2.6 Examples of IoT devices are provided 2.7 Security vulnerabilities for IoT devices are explained
	3. Investigate methods to protect personal data and privacy	3.1 Techniques to protect personal devices from cyber threats are described and demonstrated 3.2 User authentication techniques are identified and demonstrated 3.3 Methods and tools to safeguard personal privacy are identified and demonstrated

Unit of Competency	Element	Performance Criteria
	4. Examine methods used to protect an organisation's data	4.1 Common infrastructure, equipment, and software used to protect an organisation from cyber security attacks are identified 4.2 Cyber security terms such as botnets, malware, virus's, worms, Root Kits are clarified 4.3 Mitigation strategies such as the cyber kill chain process, the MITRE Adversarial Tactics, Techniques and Common Knowledge (ATT&CK) in the context of cyber security protection and mitigation strategies are explained 4.4 Policies, tools and systems for protecting an organisation from cyber-attacks are investigated 4.5 Behaviour based approach to cyber security is investigated 4.6 Incident response policies, processes and systems are reviewed
	5. Investigate current Cyber Security Frameworks (CSF)	5.1 Fundamentals of the National Institute of Standards and Technology Cyber Security Framework (NIST CSF) are examined and explained 5.2 Essential Eight strategies from the Australian Cyber Security Centre (ACSC) to mitigate Cyber Security incidents are identified 5.3 Centre for Internet Security (CIS) controls identified for organisations to implement for Cyber Security protection are examined
VU23220 Develop and carry out a cyber security industry project	1. Establish project team	1.1 Team members for the project are selected 1.2 Individual responsibilities for each team member are determined 1.3 Team performance criteria are established 1.4 Methodology of team performance measurement is defined
	2. Determine context of business need or problem (project)	2.1 Scope and system boundaries of the business problem are determined together with the problem solving methodology 2.2 Background information is gathered and development of questions appropriate to the business problem are prepared 2.3 Objectives and expected outcomes to be achieved are identified and documented 2.4 Key elements for project milestones are identified 2.5 Work plan statement is developed

Unit of Competency	Element	Performance Criteria
	3. Support the project plan development	3.1 Process of identifying tasks and resources needed to complete the project plan is determined 3.2 Schedule of project tasks including realistic timeframes and costs is prepared 3.3 Specific responsibilities to project team members are allocated 3.4 Process to manage risks and/or unexpected events that may impact upon the project objectives and/or timelines is developed
	4. Evaluate the suitability of the gathered resources	4.1 Key components required from the project are identified 4.2 Resources for the project are allocated 4.3 Function and operation of selected resources allocated to team members are defined
	5. Implement the project design	5.1 Suitable systematic processes to implement the project are selected 5.2 Subtasks for the overall project are defined and allocated to team members 5.3 Subtasks are developed 5.4 A systematic testing procedure is defined 5.5 As part of the project Red and Blue teaming exercises are planned and executed 5.6 Verification of the functionality of the project in either part or full is performed 5.7 Documentation for the process such as meeting minutes, reports, emails is generated
	6. Support project completion and handover	6.1 An implementation plan with minimal end user's disruption is developed 6.2 Technical documentation including project timeframes, scope, cost is drafted 6.3 Technical documentation for approval by appropriate person/s is submitted 6.4 Developed project risk strategy is evaluated 6.5 Where required appropriate plan to train end users is presented 6.6 Final project sign-off from sponsor and key stakeholders is obtained 6.7 Project is closed and experience gained and lessons learnt are discussed and documented

Unit of Competency	Element	Performance Criteria
ICTICT443 Work collaboratively in the ICT industry	1. Identify team protocols requirements for working collaboratively in a virtual environment	1.1 Identify team protocols for virtual ways of working, including cyber safety protocol 1.2 Identify communication tools and technology available to support teams working collaboratively in virtual environments 1.3 Determine roles and responsibilities of team members according to team communication protocols 1.4 Determine areas to improve team protocols for working collaboratively in a virtual environment
	2. Develop protocols to work collaboratively in a virtual environment	2.1 Review technology utilised to support teams working collaboratively in virtual environments 2.2 Develop protocols to share knowledge collaboratively in a virtual environment according to work details and team objectives 2.3 Develop cyber security protocols in accordance with organisational cyber security procedures
	3. Review compliance with protocols to work collaboratively in a virtual environment	3.1 Review protocols utilised to support teams working collaboratively in virtual environments 3.2 Seek feedback from relevant personnel on team communication practices according to working collaboratively in virtual environments protocols 3.3 Determine improvements to future work protocols in virtual environments
VU23221 Evaluate and test an incident response plan for an enterprise	1. Form an incident response team	1.1 Members to form incident response team (IRT) are recruited 1.2 IRT members roles and responsibilities are defined 1.3 Communication strategies and reporting hierarchy for the IRT within the organisation are determined 1.4 Business implications to the organisation of cyber incidents are articulated to the IRT
	2. Define red, blue and purple team tasks	2.1 Fundamental red teaming activities for incident responses are created 2.2 Fundamental blue teaming activities for incident responses are created 2.3 Fundamental purple teaming activities are defined

Unit of Competency	Element	Performance Criteria
	3. Plan the implementation of the organisation's incident response plan (IRP)	3.1 Organisation's incident management plan is evaluated 3.2 Services the IRT will provide are defined 3.3 Response plans to a range of incidents are developed 3.4 Reporting procedures for incident handling are developed 3.5 Processes for collecting and protecting evidence during incident responses are developed 3.6 Incident response exercises and red-teaming activities are created 3.7 Incident response staffing and training requirements are specified
	4. Implement the IRP for prescribed incidents	4.1 Red-teaming activities are executed for the range of incident responses 4.2 Response to the incidents is reported 4.3 Incident response evidence is collected, processed and preserved in accordance with the organisation's guidelines 4.4 Strategy of blue-teaming activities to mitigate the incident responses are discussed and evaluated 4.5 Incident management measures are collected, analysed and reported
	5. Evaluate the IRP	5.1 Improvements learnt from the IRP activities are implemented 5.2 Effectiveness of red teaming and incident response tests, training and exercises are examined and modified as required 5.3 Communication between incident response team and organisations management are assessed for effectiveness and changes implemented if required
VU23222 Expose website security vulnerabilities	1. Explain the Hypertext Transfer Protocol (HTTP) and web server architectures	1.1 Web application server architecture is explained 1.2 Structure and operation of the HTTP protocol is described 1.3 Function and role of HTTP Headers is identified 1.4 Typical HTTP Headers are examined 1.5 Securing HTTP using headers is identified 1.6 OWASP Secure Headers Project tools are examined

Unit of Competency	Element	Performance Criteria
	2. Identify web site content	2.1 Technology stack of a web application and web server are identified 2.2 Web server scanner software and web content scanner software are demonstrated 2.3 Spiderling for web applications and websites are described and demonstrated
	3. Install web application proxy testing tools	3.1 Example of web application proxy testing tools are described and demonstrated 3.2 Proxy testing tools for a proxy server are configured and installed 3.3 Web application traffic is intercepted and logged with a web application testing tool suite
	4. Use current frameworks that identify common software vulnerabilities	4.1 Existing frameworks that identify common software vulnerabilities are investigated 4.2 Most common web security vulnerabilities are identified 4.3 Methods to determine injection weaknesses (SQLite) for web applications are described and demonstrated 4.4 Methods for basic Broken Authentication and Session Management weaknesses for web applications are described and demonstrated 4.5 Methods for basic Cross Site Scripting (XSS) weaknesses for web applications are described and demonstrated 4.6 Methods for Insecure Direct Object Reference (IDOR) weaknesses for web applications are described and demonstrated
	5. Report web application vulnerabilities	5.1 Technical issues and assigning risk are identified 5.2 Detailed reproduction steps are outlined 5.3 Remediation steps are identified 5.4 Penetration test report is written and presented to relevant technical persons 5.5 Executive summary is prepared and provided to appropriate persons.
VU23216 Perform basic cyber security data analysis	1. Demonstrate the process of basic cyber security data analysis	1.1 Sources of data used to monitor a network are identified 1.2 Information for a provided scenario from alerts, logs or reported events is collected 1.3 Strategies to process this data is developed

Unit of Competency	Element	Performance Criteria
		1.4 Data to be processed is broken down into subtasks and a range of strategies to analyse these subtasks are developed. 1.5 Effectiveness of the subtasks implementation is evaluated and modified as required
	2. Examine the use of data bases as a repository for data	2.1 Use of a data base to store personal information is described and demonstrated 2.2 Structured Query Language (SQL) commands to access the data are identified and demonstrated 2.3 Database security vulnerabilities are identified 2.4 Strategies for mitigating
	3. Identify discrepancies and anomalies in data sets	3.1 Detecting discrepancies in data is described and performed 3.2 Pattern recognition is demonstrated 3.3 Software tools to support the detection of anomalies and discrepancies are demonstrated 3.4 Detecting anomalies in data is demonstrated 3.5 Software tools to support the detection of anomalies and discrepancies are demonstrated 3.6 Use of automation in data collection and analysis is explained
VU23215 Test concepts and procedures for cyber security	1. Identify typical cyber security application layer testing methodologies and tools	1.1 Existing frameworks that identify common application layer vulnerabilities are investigated 1.2 Common application layer security vulnerabilities are identified 1.3 Current policies to minimise the identified application layer vulnerabilities are reviewed
	2. Use networking security testing methodologies, tools and commands	2.1 End to end testing commands for network continuity are demonstrated 2.2 Systematic troubleshooting procedures for network connectivity are demonstrated 2.3 Use of networking monitoring tools are demonstrated
	3. Implement the laboratory testing environment	3.1 Laboratory testing environment is configured 3.2 Using end to end testing commands, the laboratory environment is tested for functionality

Unit of Competency	Element	Performance Criteria
	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 (CVEs) are defined 4.6 Heuristics as a methodology for string analysis and their corresponding toolset are described
	5. Demonstrate ethical hacking principles and procedures	5.1 Ethical hacking process and procedures are described 5.2 Base level troubleshooting procedures are demonstrated 5.3 Fundamentals of penetration testing are described 5.4 Legal implications of hacking are explained 5.5 Process of foot printing the computer systems of a company is examined 5.6 Methodologies of enumeration to gather system usernames are described 5.7 Tools to port scan a computer system are demonstrated 5.8 Methodologies of system hacking are described then demonstrated 5.9 Common sniffing tools are described and demonstrated
	6. Identify security vulnerabilities of WLANs	6.1 WLAN physical vulnerabilities are identified 6.2 WLAN software issues and vulnerabilities are determined
	7. Demonstrate basic scripting for a cyber security environment	7.1 Introduction to scripting languages is demonstrated 7.2 Scripts for testing tools are described and demonstrated 7.3 Key system and third-party import libraries are described 7.4 Scripting basic programming language is described and demonstrated

Unit of Competency	Element	Performance Criteria
VU23218 Implement network security infrastructure for an organisation	1. Examine the different models of security solutions for an organisation	1.1 Physical security system solutions for an organisation are described 1.2 Hybrid security system solutions for an organisation are explained 1.3 Cloud based security system solutions for an organisation are described 1.4 Potential risks of network perimeter security devices for an organisation are identified
	2. Investigate methods used to authenticate users to a network	2.1 Process and reasons for configuring secure administrative access to network devices are explained 2.2 Authentication, Authorization and Accounting (AAA) procedures to access network devices are described 2.3 AAA authentication from a local server is implemented 2.4 Multifactor Authentication (MFA) processes to add security to an organisation's network access are examined
	3. Investigate the operation and role of software tools to monitor traffic and security in an organisation	3.1 Examples of Network Access Control (NAC) features are described and demonstrated 3.2 Function and role of End Point Protection (EPP), End point Detection and Response (EDR), Extended Detection and Response (XDR) and Data Loss Prevention (DLP) systems for end points is defined 3.3 Features of network monitoring tools are identified and demonstrated
	4. Prepare and implement a firewall	4.1 Features of basic and next generation firewalls are compared 4.2 Methods of traffic flow control for firewalls are identified 4.3 Function and operation of a firewall to mitigate network attacks is described and implemented 4.4 Basic configuration of firewall security zones is demonstrated and implemented 4.5 Basic packet filtering is demonstrated and implemented
	5. Investigate intrusion prevention and intrusion detection systems (IPS/IDS)	5.1 Differences between intrusion prevention and intrusion detection systems are clarified 5.2 Process of detecting malicious traffic using signatures is demonstrated

Unit of Competency	Element	Performance Criteria
		5.3 Artificial Intelligence (AI) and Machine Learning (ML) methods and tools to detect malicious data streams are investigated
	6. Examine proxy server vulnerability issues	6.1 Function and operation of a proxy server is explained 6.2 Methods used to compromise the security of a proxy server are identified 6.3 Mitigation strategies to protect a proxy server are defined
	7. Investigate wireless security access and common vulnerabilities	7.1 Overview of the 802.11 Wireless Local Area Network (WLAN) Standard is provided 7.2 Relationship between the Data Layer and the Physical layers for WLANs is defined 7.3 WLAN architecture of a typical system is defined and demonstrated 7.4 Authentication and Association methods for wireless clients are described and demonstrated 7.5 Strengths and weaknesses of WLAN encryption techniques are identified 7.6 Current tools to discover details about available WLANs are selected and utilised 7.7 WLAN security checklist is developed
	8. Demonstrate the fundamental operation of cryptographic systems	8.1 Overview of cryptography is provided 8.2 Process of working with symmetric & asymmetric algorithms is defined 8.3 Function and operation of encryption, hashes and digital signatures to secure a network is explained 8.4 Data integrity and authentication utilising encryption algorithms are defined 8.5 Data confidentiality utilizing encryption algorithms are summarised 8.6 Process of public key encryption to ensure data confidentiality is demonstrated 8.7 Cryptography standards and protocols are summarised 8.8 Common use of protocols that utilise cryptography are demonstrated

Unit of Competency	Element	Performance Criteria
	9. Demonstrate the fundamentals of Virtual Private Networks (VPN's)	9.1 Advantages and operation of VPN's are explained 9.2 Operation of tunnelling is described and demonstrated 9.3 Operation of Internet Protocol Security (IPSec) VPN's is summarised 9.4 Site to site IPSec VPN with pre shared key authentication is demonstrated 9.5 Different software VPN software packages enabling remote access to an organisations network are compared 9.6 VPN-Less alternatives for secure remote access to an organisations network are examined
VU23219 Manage the security infrastructure for an organisation	1. Identify the key features from information and security policies for an organisation	1.1 Information and security policy documents for the organisation are accessed and examined 1.2 Implications of the organisation's employees work habits relating to its security policy are evaluated 1.3 Implications of the organisation's configuration and change management capability are evaluated 1.4 Levels of security clearances to access organisational data are identified
	2. Determine risk category for the security infrastructure	2.1 Audit of existing tools and security infrastructure for the organisation is conducted 2.2 Asset valuation for the organisation is determined 2.3 Security infrastructure baseline is determined 2.4 Risk assessment of the organisation assets is conducted and associated risks categorised 2.5 Resources required by risk categories to minimise disruption to business operation is identified
	3. Identify the physical security vulnerabilities of the organisation's security infrastructure	3.1 Physical structure of the organisation's security infrastructure is examined 3.2 Security infrastructure vulnerabilities are identified and documented 3.3 Physical security infrastructure vulnerabilities are communicated to appropriate management personnel

Unit of Competency	Element	Performance Criteria
	4. Implement appropriate security system controls for managing the risk	4.1 Effective controls to manage risk are devised and implemented 4.2 Policies and procedures to cover user access to the system are developed 4.3 Security recovery plan is developed 4.4 System controls to reduce risks in human interaction with the system are implemented
	5. Monitor security infrastructure tools and procedures	5.1 Controls that manage risks are reviewed and monitored 5.2 Vendor products that monitor risk
	6. Promote cyber security awareness in the organisation	6.1 Strategies to promote security policy awareness amongst the staff of the organisation are planned and implemented 6.2 Security policy awareness strategies are evaluated for their effectiveness within the organisation and if required modified for increased impact 6.3 Training to implement the organisation's security policy practices is planned and implemented
	7. Implement cyber hygiene principles	7.1 Best practices in cyber hygiene are identified 7.2 Cyber hygiene process is identified and implemented
VU23224 Identify the implications of cloud-based security systems	1. Investigate testing in cloud-based environments	1.1 Testing techniques for cloud environments are identified 1.2 Limitations of testing techniques across different cloud environments are explained 1.3 Procedures for gaining approval to test are identified and applied 1.4 Sandboxes for cloud infrastructure using two cloud services are created
	2. Investigate security controls to cloud-based infrastructure	2.1 Approaches to securing cloud deployments are identified 2.2 Cloud security services are examined 2.3 Security services to meet a business needs are selected
	3. Secure access to cloud resources	3.1 Access controls to meet business needs are identified and configured 3.2 Testing methods are identified and applied against access controls

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

Employability skills

Reading

- read and interpret relevant regulations, signs, labels and other relevant workplace documents associated with cyber security

Writing

- write reports as part of the inspection and testing requirements and investigations in network security
- prepare written instructions for others

Oral communication

- negotiate complex cyber-related issues with team members
- speak clearly and directly on complex matters, when sharing data, requirements or other information relevant to inspection and testing outcomes in network security

Numeracy

- perform calculations in binary and hexadecimal number systems
- perform basic mathematical calculations when implementing network security infrastructure for an organisation

Learning

- listen to, or read, interpret and implement technical complex cyber security processes and procedures
- adapt own competence in response to change
- update own knowledge and skills required for network security

Problem-solving

- 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 cybersecurity issues
- monitor and anticipate problems that may occur in the course of cybersecurity vulnerability inspection and testing activities

Initiative and enterprise skills

- modify activities dependent on different situations
- respond appropriately to changes in equipment, standard operation procedures and the working environment
- take appropriate actions in a diverse range of cyber security incidents

Teamwork

- provide leadership during activities as appropriate
- collaborate with others
- work with diverse range of people within a team environment.

Planning and organising skills

- 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

Technology

- use testing equipment and systems as required
- use computers and printers to prepare reports
- implement and monitor the application of security software

Digital literacy

- undertake independent research in a range of technical cyber-related issues

- find, evaluate, and communicate information on various digital platforms
- produce text, images, audio and designs using technology to communicate information to others

22610VIC Advanced Diploma of Cyber Security

Aims

The Advanced Diploma of Cyber Security provides graduates with the knowledge and skills to manage and maintain cyber security in an organisation. It aims to equip them with the knowledge and skills to meet the following vocational outcomes

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

Job roles

Graduates of the course will be able to seek employment as cyber security paraprofessionals in a range of commercial enterprises/organisations and government bodies seeking to improve and maintain their cyber security or, to work independently as a freelance cyber security analyst.

Roles applicable to this qualification would be:

- Cyber security manager in an organisation or government department

Duration

The expected duration for the 22610VIC Advanced Diploma of Cyber Security is 4 terms. Students who are identified as having difficulties in completing the course in the required duration may be able to extend their course as per APC's Intervention Policy. NOTE: Due to College closure over the Christmas/New Year period the maximum course length for students studying at this time is 49 weeks.

Entry requirements

ACADEMIC

- Completion of the superseded (22334VIC) or current (22603VIC) – Certificate IV in Cyber Security or equivalent
- or
- minimum of two (2) years cyber security work experience.

ENGLISH LANGUAGE PROFICIENCY

International students must fulfil additional entry requirements as follows:

- Successful completion of UpPer Intermediate General English
- or
- equivalent English Language proficiency test result

Materials

The required texts for this course are the Australian Pacific College workbooks. You have access to your workbooks for all classes. These workbooks are provided to you free of charge in a pdf version in myAPC.hub and you can download them to your device.

Course structure

Australian Pacific College (APC) students are taught 12 subjects made up of 20 Units of Competency. The full length of the course is 4 terms.

Subject code and name	Unit of Competency
A50535 Fundamentals of Cyber Security	VU23289 Interpret and utilise key security frameworks, policies and procedures for an organisation pages
A50536 Legal and Compliance Considerations	VU23294 Identify and monitor an organisation's cyber security legal compliance requirements
A50540 Network Security	ICTNWK620 Design and implement wireless network security
A50537 Cyber Security Project Planning	BSBTWK502 Manage team effectiveness
	VU23293 Plan and implement a cyber security project
A50538 Identity Management	VU23292 Configure identity management processes and procedures for an organisation
	VU23308 Identify Active Directory security concepts
	VU23295 Gather and validate digital forensic data from workstations
A50541 Virtual Computing Environments	ICTNWK553 Configure enterprise virtual computing environments
A50539 Software Skills for Cyber Security	VU23291 Develop software skills for the cyber security practitioner
A50542 Cloud Security	VU23290 Assess and secure cloud services
	VU23307 Identify the implications of cloud based security systems
A50543 Intrusion Analysis & Response	VU23288 Communicate cyber security incidents within an organisation
	VU23298 Implement processes and procedures to deal with cyber security incidents
	VU23300 Detect and respond to cyber security threats
A50544 Security Risk Assessment	VU23297 Plan and conduct a security risk assessment for an organisation
A50545 Penetration Testing	VU23301 Manage penetration testing processes for an organisation

Subject code and name	Unit of Competency
	VU23302 Perform advanced penetration testing for web site vulnerabilities
A50546 Securing infrastructure and Devices	VU23304 Protect industrial networks and operational technology infrastructure for an organisation
	VU23305 Select and configure security devices for an organisation

Assessment Schedule

Information about your assessments is included in the Student Workbooks and Assessments for each subject. This information explains the assessment requirements and what you need to do to complete the assessments.

Assessments should be submitted on the due date. Your trainer will give you more comprehensive information about each assessment task.

You are required to complete all parts of the assessment and tick the declaration that it is all your own work i.e., that you have not plagiarised by copying from the internet or other sources. You are required to be competent in each unit of competency to achieve your qualification.

Note: Please refer to individual assessment sheets or ask your teacher for further information on the units of competency and the Elements (Elements describe the essential outcomes) and Performance Criteria (Performance Criteria describe the performance needed to demonstrate achievement of the element) as listed below:

Unit Overview

Unit of Competency	Element	Performance Criteria
VU23289 Interpret and utilise key security frameworks, policies and procedures for an organisation	1. Collate security frameworks, risk mitigation strategies and other supportive documents	1.1 Key organisations that provide useful cyber security resources to improve an organisation's security capability are identified 1.2 Key Australian and overseas cyber security incident mitigation strategies that improve an organisation's security are accessed and reviewed 1.3 Current working frameworks or practices that can support an organisation to improve its security capabilities are identified and assessed 1.4 Current Australian cyber security legal and ethics documents are identified and reviewed 1.5 Guidelines for security relating to Internet of Things (IOT) are identified and reviewed

Unit of Competency	Element	Performance Criteria
	2. Evaluate key information from relevant documents that will support an organisation to improve its security infrastructure	2.1 Australian compliance standards are identified and evaluated for an organisation 2.2 Compulsory Australian cyber security legal and ethics documents are identified for an organisation 2.3 Key strategies to mitigate cyber security risks are identified and evaluated
	3. Select relevant security frameworks and cyber security incident mitigation strategies	3.1 In consultation with relevant personnel, key incident response strategies including plans for an organisation are selected 3.2 In consultation with relevant personnel, appropriate working practices for an organisation are identified
	4. Implement the security frameworks and cyber security incident mitigation strategies	4.1 In consultation with relevant personnel, appropriate compliance standards for an organisation are identified and implemented 4.2 In consultation with relevant personnel, current Australian cyber security legal and ethics procedures are implemented 4.3 In consultation with relevant personnel, organisational processes and procedures to implement key incident response strategies are adopted or altered 4.4 In consultation with relevant personnel, training for organisational staff to adopt new or alter current working practices to improve the security culture is planned and implemented 4.5 In consultation with key personnel, appropriate working practices for an organisation are implemented
	5. Monitor the effectiveness of the organisation's implementation of the security frameworks and cyber security incident mitigation strategies	5.1 List of criteria that measures the effectiveness of implemented changes to working practices is created 5.2 Effectiveness of changes to the organisation's processes and procedures that deal with strategies to address incident responses are monitored 5.3 Effectiveness of changes made to working

Unit of Competency	Element	Performance Criteria
VU23294 Identify and monitor an organisation's cyber security legal compliance requirements	1. Identify the structure of the Australian legal system	1.1 Key legal terms are defined 1.2 Structure of the Australian legal systems are investigated 1.3 Common laws are identified 1.4 Structure of the Australian federal system of government is defined 1.5 Relationship between federal and state regulation is clarified
	2. Define Australian cyber law	2.1 Model laws on electronic commerce are investigated 2.2 Conventions on the use of electronic communications are defined 2.3 Relevant international cybercrime convention is investigated 2.4 Repercussions of the international General Data Protection Regulation (GDPR) and its adoption in Australia is investigated 2.5 Implication of Australian electronic transactions law is investigated
	3. Identify mandatory and discretionary cyber laws and practices	3.1 Categories of information the law affords cyber security protection for an organisation are identified 3.2 Legal resources pertaining to cyber law are identified 3.3 Relevant laws for particular industry sectors are identified and collated 3.4 Difference between State and federal legislation for relevant laws pertaining to cyber security are identified 3.5 Outcomes of current Commonwealth Acts as they pertain to cyber security for an organisation are identified 3.6 Mandatory outcomes of current State based Acts as they pertain to cyber security for an organisation are identified 3.7 Codes pertinent to an organisation's industry sector are identified 3.8 Frameworks pertinent to an organisation's industry sector are identified 3.9 Voluntary codes and best practices for the industry sector aligned to an organisation are identified

Unit of Competency	Element	Performance Criteria
	4. Evaluate and select relevant Australian regulation and practices pertaining to security for an organisation	4.1 Methodology of utilising legal resources relevant to cyberlaw for an organisation is defined and demonstrated 4.2 Mandatory regulations, standards, codes and frameworks pertaining to cyber security for an organisation are evaluated and selected 4.3 Discretionary standards, codes and frameworks pertaining to cyber security for an organisation are evaluated and selected 4.4 Voluntary codes and best practice for the industry sector aligned to an organisation are evaluated and selected
	5. Implement relevant Australian regulation and practices pertaining to security for an organisation	5.1 Strategies to implement mandatory regulations, standards, codes and frameworks for an organisation are developed 5.2 Strategies to implement discretionary standards, codes and frameworks for an organisation are developed 5.3 Strategies to implement voluntary codes and best practice guidelines for an organisation are developed 5.4 Organisational changes to appropriate personnel within an organisation are articulated
	6. Monitor the effectiveness of an organisation's implementation of regulation and practices	6.1 Criteria to measure the effectiveness of implemented changes to work practices adopted by an organisation is created 6.2 Utilising the developed criteria, the effectiveness of changes to an organisation's work practices are measured and monitored 6.3 Changes to the organisation's working practices are documented and reported to appropriate personnel
ICTNWK620 Design and implement wireless network security	1. Prepare to implement wireless network security	1.1 Evaluate benchmarked organisational and regulatory security policies and network security standards 1.2 Assess organisational requirements against regulatory security compliance 1.3 Develop and document security solution plan according to organisational requirements and future growth expectations

Unit of Competency	Element	Performance Criteria
	2. Design, implement and test guest access services	2.1 Analyse and select architecture for guest access services 2.2 Produce map and set up guest access accounts 2.3 Configure WLAN controller authorisation 2.4 Configure anchor and internal controllers 2.5 Troubleshoot guest access issues
	3. Design, implement and test security of wireless client devices	3.1 Design and configure authentication of clients and management frame protection on clients and controllers 3.2 Configure access control servers and integrate with wireless network 3.3 Configure client-and server-side digital certificate services 3.4 Troubleshoot secure wireless connectivity services
	4. Design, implement and test integration of wireless network	4.1 Analyse network admission control architectures and assess feasibility of network integration 4.2 Analyse high-level authentication process flow and confirm that integration is compatible 4.3 Configure and test admission control wireless controller 4.4 Troubleshoot network access integration issues of control
	5. Evaluate and plan secure wireless connectivity services	5.1 Configure intrusion detection system (IDS) and monitor network activities for malicious activities and policy violations 5.2 Analyse IDS report and review threat-mitigation strategies 5.3 Update security solution plan, mitigate wireless vulnerabilities and check network integrity according to network security requirements
	6. Manage WLAN integration requirements and advanced security platform requirements	6.1 Evaluate end-to-end security solutions and assess compatibility to integrate with required wireless solutions 6.2 Analyse WLAN firewall configuration requirements and confirm compliance with organisational and network security requirements 6.3 Configure and test WLAN controllers and detect wired and wireless intrusion prevention and detection system (IPDS) security protection

Unit of Competency	Element	Performance Criteria
		6.4 Finalise reports and documentation and submit to required personnel
BSBTWK502 Manage team effectiveness	1. Establish team performance plan	1.1 Identify team purpose, roles, and responsibilities according to organisational and task objectives 1.2 Develop performance plans with expected outcomes, key performance indicators (KPIs) and goals for work team 1.3 Support team members in meeting expected performance outcomes
	2. Develop and facilitate team cohesion	2.1 Develop strategies for facilitating team member input into planning, decision making and operational aspects of team tasks 2.2 Develop or modify policies and procedures for promoting team member accountability for personal work and team tasks 2.3 Provide feedback to team members on team effort and contributions 2.4 Develop processes for identifying and addressing issues, concerns and problems identified by team members
	3. Facilitate teamwork	3.1 Encourage team members to participate in and to take responsibility for team activities 3.2 Support the team in identifying and resolving work performance problems 3.3 Promote work team collaboration through individual behaviour
	4. Liaise with stakeholders	4.1 Establish and maintain open communication processes with relevant stakeholders 4.2 Communicate information from line management to the team 4.3 Communicate and follow-up unresolved issues, concerns and problems raised by team members with line management 4.4 Address unresolved issues, concerns and problems raised by stakeholders
VU23293 Plan and implement a cyber security project	1. Identify the strategic and operational needs for an organisation during the planning phase	1.1 Strategic and operational needs of the cyber security project during the planning phase are identified 1.2 Cyber security project's strategic context and requirements are identified

Unit of Competency	Element	Performance Criteria
		1.3 Implications of the organisation's strategic and business plans and the projects' output requirements are identified and considered 1.4 Client requirements and the impact of legislation and industry standards and codes are examined 1.5 Risk management analysis is conducted and a risk management plan is prepared and documented
	2. Support the preparation of the project design plan	2.1 Precise specifications and terms of reference for the cyber security project are defined and documented 2.2 Physical and other resources required to support the cyber security project are defined, documented and secured 2.3 Timelines, schedules and critical paths for the cyber security project, taking into consideration contingencies and planning for time slippages are developed and documented 2.4 Project budget taking into consideration the cost of the primary project, management of a range of sub-tasks and contingencies is prepared 2.5 Consultation strategies used to inform clients, contractors and other interested parties of the cyber security project's progress are defined and documented
	3. Support the assembly of personnel for the project team	3.1 Required skills needed for the successful completion of the cyber security project are identified 3.2 Required skills for the cyber security project are mapped against the available personnel 3.3 Effective communication processes to coordinate work are implemented 3.4 Clear reporting processes are identified and communicated 3.5 Modifications and improvements to the cyber security project are considered and implemented
	4. Design the sub-task for the project	4.1 Delegated tasks for the project are defined and communicated 4.2 Action plan for each project sub-task is prepared and where possible tested for functionality 4.3 Where possible outputs of the sub-task are tested for interconnectivity and functionality

Unit of Competency	Element	Performance Criteria
	5. Gather resources and test the system design	5.1 Project resources are acquired according to organisational policy 5.2 Vendor documentation for the equipment purchased is collated 5.3 Operation and functionality of the acquired equipment to achieve the project outcomes is investigated 5.4 Project sub-tasks are built, and where appropriate tested for functionality
	6. Implement the project solution	6.1 Each sub-task of the project is interconnected and tested for functionality 6.2 Verification of end to end functionality of the project design is performed and changes are made if required to ensure the design brief is achieved 6.3 Red and Blue teaming exercises are planned and applied 6.4 Further testing and modification are undertaken to the system if required to ensure the design brief is achieved
	7. Finalise the project and facilitate handover	7.1 Cyber security project is completed in line with the requirements of the project design plan 7.2 Project handover is undertaken in accordance with organisational procedures to staff responsible for ongoing implementation and maintenance 7.3 Team members and relevant stakeholders are debriefed concerning the conduct of the project and outcomes achieved 7.4 Report analysing the strengths and weaknesses of the project design plan and the conduct of the project is prepared 7.5 If required training for the organisation' staff is prepared and conducted
VU23292 Configure identity management processes and procedures for an organisation	1. Explore the function and operation of key identity and access management features and operations	1.1 Differences between identities, accounts, access, authorisation and authentication are identified. 1.2 Function and operation of common authentication services are compared 1.3 Types of authorisation services are identified 1.4 Function and operation of access control services are evaluated 1.5 Privileged account management processes are examined

Unit of Competency	Element	Performance Criteria
		1.6 Identification and access management technologies are identified and evaluated 1.7 Identity and access management documentation processes are performed 1.8 Current and emerging best practices in password management for the organisation are compared
	2. Implement best practices for user account management	2.1 Identity theft and identity fraud methods are evaluated 2.2 Components of an account management service are defined 2.3 Fundamentals of secure account management are defined 2.4 Testing strategies for weak account management are utilised 2.5 Account management for an organisation is implemented
	3. Identify, configure and monitor identity management for an organisation	3.1 Working principles for identity management are examined 3.2 Components of an identity management service are examined 3.3 Fundamentals of secure identity management is investigated 3.4 Differences between Identity Federation and Single Sign On (SSO) are defined 3.5 Identity management processes are evaluated with key personnel and modified if required to improve security 3.6 Identity management for an organisation is implemented
	4. Identify, configure and monitor authentication and authorisation services for an organisation	4.1 Performance of a selected authentication and authorisation service is monitored 4.2 Testing strategies for vulnerabilities in authentication and authorisation are developed
VU23308 Identify Active Directory security concepts	1. Identity Access Management (AM) fundamentals	1.1 Differences between identities, accounts, access, authorisation and authentication are identified 1.2 Identity lifecycle management process is defined 1.3 Function and operation of common authentication services are compared 1.4 Types of authorisation processes are identified

Unit of Competency	Element	Performance Criteria
		1.5 Accountability and audit concepts, such as access logging and audit trails are identified 1.6 Current trends in identity determination such as Multi Factor Authentication (MFA) are investigated
	2. Investigate AD architecture	2.1 Logical structure of an AD is identified 2.2 AD physical structure is defined 2.3 Roles of the protocols used in AD are defined 2.4 Mechanics of AD are described 2.5 Structure of privileged accounts and groups in AD are examined 2.6 Group Policy Objects (GPO's) configuration issues especially if applying to the domain root or domain controller are identified 2.7 Cloud connectivity using Active Directory Federation Services (ADFS) is identified 2.8 Cloud connectivity of AD to Azure Active Directory (AAD) connect is performed
	3. Define the basic structure of Windows security	3.1 Windows services and scheduled tasks are identified 3.2 Differences between Local user and Local Administrator accounts is defined 3.3 Function and role of Local Security the Authority Server Service (LSASS) in a Windows environment is identified
	4. Investigate attack techniques on Microsoft end-points (workstations and servers)	4.1 Common end point attack techniques on end points are identified 4.2 Privilege escalation using credential dumping tools are examined 4.3 Common lateral movement techniques are identified 4.4 Fileless attack tools and techniques on AD are defined
	5. Investigate attack techniques on AD	5.1 Compromising methods for AD accounts are defined 5.2 AD accounts that are attractive to compromise are identified 5.3 Systems and processes to minimise compromising AD accounts are defined 5.4 Tactics, techniques, and procedures (TTP's) used to compromise AD accounts are identified

Unit of Competency	Element	Performance Criteria
		5.5 Insecure Windows protocols are identified
	6. Investigate securing and defending AD from cyber attacks	6.1 Methods of securing AD are investigated 6.2 AD monitoring tools and techniques for signs of compromise are investigated 6.3 AD attack patterns determined from logs are identified 6.4 Role of User and Entity Behaviour Analytics (UEBA) and Endpoint Detection and Response (EDR) tools are identified
	7. Develop safe AD working practices	7.1 Methods to protect keyboard entries are investigated 7.2 Clean source code build strategies are investigated 7.3 Zero Trust mechanics processes are investigated 7.4 Privileged access management principles are investigated 7.5 Methods to harden the environment against compromise are examined 7.6 Use of Credential Guard and how it protects LSASS memory is examined
VU23295 Gather and validate digital forensic data from workstations	1. Examine privacy laws and ethical practises pertaining to digital forensics	1.1 Difference between acquiring digital data and digital forensics for workstations is explained 1.2 Processes of forensic science and investigation for workstations are identified 1.3 Current Australian privacy laws and digital forensic legislation are collated and evaluated 1.4 Current Australian ethical practises for digital forensics are collated and evaluated 1.5 An ethical code of practise for an organisation performing digital forensics is identified and adopted
	2. Define data to be recovered using digital forensic tools	2.1 Forensic data to be recovered from the workstation is defined 2.2 Triage principles for acquiring and securing data for an organisation are developed 2.3 Tools for digital forensics are evaluated and selected

Unit of Competency	Element	Performance Criteria
	3. Acquire defined forensic data from storage media	3.1 Structure and operation of the workstation's file system structure is identified and examined 3.2 Forensic data provided by the Windows registry structure and content is identified and evaluated 3.3 Data from disk drives is acquired 3.4 Universal Serial Bus (USB) and bring your own device (BYOD) connection and disconnection times are determined 3.5 Disk file open and file closure times are determined
	4. Acquire defined email forensic data	4.1 Structure and operation of an email packet is reviewed 4.2 Different types of email formats are examined 4.3 Common forensic email tools are evaluated and selected 4.4 Email senders geographic locations are determined
	5. Acquire defined web forensic data	5.1 Existing web browser structures and operation are reviewed 5.2 Common browser forensic tools are evaluated and selected 5.3 Tools and techniques to examine web forensic data are evaluated and selected 5.4 Web forensic data for a particular browser is collated
	6. Review defined recovered data	6.1 Defined data from storage media, email and the web is collated 6.2 Acquired data is reviewed and checked for readability and completeness 6.3 Report on the acquired data is compiled and discussed with appropriate personnel
	7. Identify further data forensic tools and training	7.1 Advanced data collection forensic tools are identified and classified 7.2 Forensic training for staff is planned and implemented

Unit of Competency	Element	Performance Criteria
ICTNWK553 Configure enterprise virtual computing environments	1. Prepare to configure virtual environment	1.1 Analyse organisational environment and determine virtual environment requirements 1.2 Determine virtualisation software requirements 1.3 Determine environmental requirements for installing virtualisation software 1.4 Plan and document installation process according to organisational requirements and manufacturing specifications 1.5 Submit plan to required personnel and seek and respond to feedback
	2. Install and configure support services	2.1 Install and configure services and ports according to organisational requirements and manufacturing specifications 2.2 Install and configure virtualisation client and server management software according to organisational requirements and manufacturing specifications 2.3 Install and configure environmental requirements and virtual machines according to organisational requirements and manufacturing specifications 2.4 Test functionality of virtual machines and align with organisational and manufacturing requirements
	3. Design and configure virtual network	3.1 Plan and document virtual network according to organisational requirements 3.2 Submit plan to required personnel, seek and respond to feedback 3.3 Install and configure required virtual networks according to organisational requirements and manufacturing specifications 3.4 Verify functionality of virtualisation network, according to organisational requirements and manufacturing specifications
VU23291 Develop software skills for the cyber security practitioner	1. Identify the interplay of hardware and software of a computer when executing a program	1.1 Microprocessor architecture is identified 1.2 Overview of an assembler instruction set is provided 1.3 Operation of a program fetching and executing code is described 1.4 Tools to develop and debug assembly language programs are defined

Unit of Competency	Element	Performance Criteria
		1.5 Example of the structure and the compilation of an assembly language program is provided and interpreted 1.6 Structure and operation of an exe file is examined and described 1.7 Difference between a programming language that generates an executable file and a programming language that interprets instructions is compared 1.8 Skills and tools to reverse engineer code are identified
	2. Write programs using a modern programming language	2.1 Modern programming languages used in cyber security development applications is investigated 2.2 Software tools to develop Web pages are identified 2.3 Components of a programming language development environment are identified 2.4 Programs that require data entry are written 2.5 Tools to troubleshoot programs are selected and utilised as required
	3. Write and interpret software scripts	3.1 A comparison of common scripting languages used in cyber security code development is performed 3.2 Process of compiling a modern scripting language to bytecode is performed 3.3 A script that accepts run time parameters is written 3.4 Tools to troubleshoot the software script in the demonstration of the program operation are utilised
	4. Identify methods and strategies as to how malware code is executed	4.1 Process of malware infecting executable code via extraneous jump instructions is identified and demonstrated 4.2 Process of malware infecting executable code via stack overflow is identified and demonstrated 4.3 Process of malware infecting executable code via buffer overruns is identified and demonstrated 4.4 Other ways in which extraneous code is executed are described
	5. Identify principles and practices used to develop secure code	5.1 Strategies and tools to develop secure software are investigated 5.2 Software development lifecycle (SDLC) is defined

Unit of Competency	Element	Performance Criteria
		5.3 Outcomes of the Open Web Application Security Project (OWASP) secure coding practise guide are identified 5.4 Other tools and frameworks used to develop secure code are investigated
	6. Investigate principles and practises to secure code execution	6.1 Operating system tools to secure code are examined 6.2 Methods to protect and secure code are explained
VU23290 Assess and secure cloud services	1. Categorise cloud service, security services and deployment models	1.1 Cloud service models are identified 1.2 Cloud deployment models are classified 1.3 Cloud infrastructure is explained 1.4 Risk assessment for cloud based data services is performed 1.5 Cloud security services are reviewed
	2. Develop a risk management plan for cloud based data storage and services	2.1 Security risks and consequences in accordance with the Australian legislative requirements and relevant standards for cloud based data and services are identified 2.2 Acceptable and unacceptable risks for cloud based data storage and services are identified 2.3 For high priority risks of cloud based data storage and services appropriate controls are developed 2.4 Existing controls to determine the impact on risk occurrence are monitored and modified if required 2.5 Risk management plan for cloud based data storage and services for the organisation are documented
	3. Evaluate, select and implement cloud based services for the organisation	3.1 Australian legislative requirements and relevant standards relating to cloud based services for the organisation are identified and evaluated 3.2 Insurance of cloud data and services are recommended to the appropriate organisational bodies
	4. Evaluate, select and implement cloud based services for the organisation	4.1 Cloud service providers for the organisation are evaluated and selected 4.2 Cloud services to access the organisation's data are selected and deployed 4.3 Deployment of cloud micro-services and containers utilised by an organisation are explained

Unit of Competency	Element	Performance Criteria
		4.4 Cloud security services are selected and deployed 4.5 Cloud Identity and Access Management (IAM) services are evaluated
	5. Develop strategies to protect cloud services	5.1 Key personnel tasked to deal with user account management are identified 5.2 Strategies to secure cloud services are developed for the organisation 5.3 Back up strategies are developed for the organisation 5.4 Disaster recovery (DR) strategies are developed for the organisation 5.5 Strategies for cryptographic key management of cloud services are developed 5.7 Shared security responsibility models for cloud services are identified
	6. Monitor the effectiveness of strategies developed to protect cloud based data and services for the organisation	6.1 Tools used to audit and monitor cloud based services and data are evaluated, selected and deployed 6.2 Changes to the strategies and tools used to monitor the cloud services and data are presented to appropriate organisational bodies
VU23307 Identify the implications of cloud based security systems	1. Identify key features, design and consequences of cloud- based environments.	1.1 Different cloud architectures and models are compared and contrasts identified 1.2 Implications, limitations and consequences of high availability and scaling in cloud environments are explained 1.3 Testing techniques for cloud environments are identified 1.4 Limitations of testing techniques across different cloud environments are defined 1.5 Sandboxes for cloud infrastructure using cloud services are created
	2. Determine the best mechanism and techniques to secure cloud networks	2.1 Mechanisms used for securing cloud networks are identified 2.2 Appropriate application security and Operating System (OS) controls in cloud environments are applied 2.3 Appropriate compliance controls in cloud environments to protect data are applied

Unit of Competency	Element	Performance Criteria
		2.4 Cloud security services required to meet business needs are identified
	3. Identify mechanism and techniques used to operate and support cloud environments	3.1 Logging, monitoring and alerting to protect cloud environments are identified and configured 3.2 Policies, procedures and techniques to maintain cloud environment security are determined 3.3 Mechanisms and business requirements to performing disaster recovery tasks in a cloud environment are identified 3.4 Ways to perform cloud migrations and their limitations are identified 3.5 Security monitoring services and tools that align with business needs are investigated and documented
	4. Determine the best way to troubleshoot cloud-related issues	4.1 Methods to troubleshoot common security issues in cloud environments are defined 4.2 Methods to troubleshoot common deployment issues in cloud environments are identified
VU23288 Communicate cyber security incidents within an organisation	1. Compile information on key groups who need to be notified on security breaches	1.1 Information on the organisation's ethical practices and security policies is sought and examined 1.2 Organisational personnel structure documents are identified and collated 1.3 Decision making responsibilities for each organisational group are interpreted and clarified 1.4 Process of escalating an incident to appropriate organisational group/s is identified 1.5 Negotiation process with appropriate groups to address cyber incidents is implemented
	2. Collate information on communication styles	2.1 Different communication styles are identified and compared 2.2 Appropriate communication style is identified to explain impact of an incident to different
	3. Address cyber security incidents	3.1 Data sources to detect incidents are selected 3.2 Risk impact of the incidents is assessed 3.3 Functional tasks within the team are allocated 3.4 Communication expectations within the incident team are determined 3.5 Process for engaging external skilled personnel to deal with incidents is clarified

Unit of Competency	Element	Performance Criteria
	4. Monitor the team's effectiveness and communication during an incident	4.1 Team functionality is monitored 4.2 Decision making and communication within the team is monitored 4.3 Group decision making processes are evaluated and monitored and changes implemented if required 4.4 Effectiveness of utilising external or extra specific skilled personnel to deal with incidents is assessed 4.5 Welfare of the staff involved with the incident is monitored
	5. Formulate and present appropriate presentations and reports to an organisation	5.1 Appropriate presentations and reports are prepared for each defined organisational decision making group 5.2 Effects of high risk incidents are communicated to relevant organisational decision making groups 5.3 Feedback from individuals and groups regarding the effectiveness of the incident handling process is reviewed in order to affect incident handling policy improvements if required
VU23298 Implement processes and procedures to deal with cyber security incidents	1. Prepare to respond to an incident	1.1 Procedures to address incidents in the organisation's incident response plan (IRP) are identified and reviewed 1.2 Organisation's processes to deal with incident responses are benchmarked against published incident response strategies 1.3 Incident response team (IRT) members to deal with the incident are identified 1.4 IRT member's roles and responsibilities are clearly defined 1.5 IRT member's communication expectations during incidents are clarified 1.6 IRT reporting and communication procedures to relevant organisational groups are defined 1.7 Function and role of cyber security tools and techniques chosen to detect incidents are defined 1.8 Data sources to gather incident information are identified
	2. Identify the cyber security incident	2.1 System messages and events to identify malicious activity are evaluated 2.2 Data is collected from appropriate data sources 2.3 Initial triage of the incident is performed

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

Unit of Competency	Element	Performance Criteria
		7.6 Procurement of new security equipment is organised with appropriate personnel if required
VU23300 Detect and respond to cyber security threats	1. Define endpoint threat analysis and computer forensics	1.1 Common Vulnerability Scoring System CVSS 3.0 for risk assessment is defined 1.2 Cyber security features are classified for risk assessment 1.3 Windows file system components are defined 1.4 Linux file system components are defined 1.5 Evidence types are contrasted 1.6 Altered and unaltered disk images are contrasted 1.7 Role of assets and threat actors are defined
	2. Analyse network intrusion events	2.1 Vulnerabilities in networking protocols are evaluated 2.2 Elements from a NetFlow record of a security event are analysed 2.3 Network monitoring tools are identified, evaluated and selected 2.4 Key elements in an intrusion are identified 2.5 Data from an event is acquired 2.6 Selected intrusion elements from an event to common source technologies are mapped 2.7 Intrusion detection flags such as False Positive, False Negative, True Positive and True Negative are defined
	3. Prepare to deal with incident responses	3.1 Incident response plan from the National Institute of Standards and Technology (NIST) described in the NIST.SP800-61 r2 document is evaluated and implemented 3.2 Organisation incident response plan is implemented 3.3 Function and role of the Cyber Security Incident Response Team (CSIRT) is defined 3.4 Elements for network profiling are defined 3.5 Elements for server profiling are defined 3.6 Acquired data is mapped to finance, health or credit card compliance frameworks

Unit of Competency	Element	Performance Criteria
	4. Compose processes for data and event analysis	4.1 Steps and methods used to gather data are described and evaluated 4.2 Domain Name Server (DNS) and HTTP logs are mapped to identify threat actors 4.3 Threat intelligence data is collated from internal records and public trusted sites 4.4 Organisational detection tools and methods are utilised to correlate generated alerts from multiple data sources 4.5 Alternative tools and techniques used for data analysis are utilised
	5. Apply models and processes to incidents	5.1 Models of intrusion detection (e.g. MITRE ATT&CK) are described and evaluated 5.2 Intrusion events are classified 5.3 Incident response processes are applied to the event 5.4 Selected range of activities relating to incident handling are defined 5.5 Documents that support the organisation to collect forensic data for incident responses are identified, evaluated and adopted 5.6 Data evidence and collection forensic activities are defined according to organisational guidelines 5.7 Structured Threat Information Expression (STIX) language for describing cyber threat information for it to be shared, stored, and analysed is evaluated 5.8 STIX methods are applied to the incident
VU23297 Plan and conduct a security risk assessment for an organisation	1. Compile and evaluate risk management plan for the organisation	1.1 Methodologies for risk assessment are investigated 1.2 Vulnerabilities and threats for an organisation are identified 1.3 Risk management plan for the organisation is sourced 1.4 Risk assessment analysis process for an organisation is defined 1.5 A cyber security disaster recovery plan for an organisation is developed
	2. Compile risk categories for the security system	2.1 Information assets for the organisation are ranked and documented 2.2 Risk analysis classification criteria is determined

Unit of Competency	Element	Performance Criteria
		2.3 Use risk analysis processes to qualify and quantify risks and threats 2.4 Risk priorities for information assets are allocated 2.5 Risk analysis outcomes for inclusion in the risk register and the risk management plan are documented
	3. Implement appropriate security system controls for managing the risk	3.1 Effective controls to manage risk are devised documented and implemented 3.2 Emerging risks or threats are monitored with corrective measures planned documented
	4. Monitor security system controls and processes	4.1 Controls that manage risks are reviewed and monitored for their continued effectiveness 4.2 Regular risk review processes to maintain currency of risk plans are established 4.3 Environment is regularly monitored to determine changed conditions 4.4 If environment or a condition changes, implement and document appropriate changes to the risk controls and report changes to appropriate personnel
	5. Promote cybersecurity awareness in the organisation	5.1 Implications of the organisation's security policy are defined and evaluated 5.2 Strategies to promote security policy awareness in the organisation are planned and implemented 5.3 Organisation's security policy awareness strategies are evaluated for their effectiveness and if required, modified to increase their effectiveness
VU23301 Manage penetration testing processes for an organisation	1. Compile information on the organisation's technology	1.1 Information regarding the organisation's IT security infrastructure, web systems, cloud services and security infrastructure is sourced 1.2 Information on the function and operation on each item of the IT infrastructure, web systems, cloud services and security infrastructure is collated 1.3 Design of the IT infrastructure, web systems, cloud services, and security infrastructure is evaluated 1.4 Secure Development Lifecycle (SDLC) and the importance of integrating it with security during all phases of development is established

Unit of Competency	Element	Performance Criteria
	2. Evaluate and select tools to test the security infrastructure	2.1 Tools used to perform Vulnerability and Penetration (VPEN) testing on the organisation's IT infrastructure, web systems and cloud services are sourced and evaluated 2.2 Tools to perform VPEN testing are selected 2.3 Testing environment is setup and configured 2.4 Web site testing frameworks are evaluated and selected 2.5 Vulnerabilities within a testing environment are identified
	3. Develop penetration testing skills	3.1 Familiarity with the function and configuration of the VPEN testing tools is developed 3.2 Skills in using the VPEN testing tools for detecting vulnerabilities in security infrastructure are developed 3.3 Familiarity with sources of information for vulnerabilities, threat intelligence and exploits is developed 3.4 Differences between infrastructure vulnerability scanning, web vulnerability scanning, cloud security assessment, and penetration testing are articulated 3.5 Familiarity with identifying and using sources of threat intelligence and exploit information is developed
	4. Identify tools to establish a vulnerability baseline	4.1 Locations and devices where vulnerability information comes from within the organisation are identified and documented 4.2 Tools to determine the vulnerability baseline within the organisation are identified and documented 4.3 Regular procedures and processes for VPEN testing for the organisation are proposed
	5. Research new security technology developments	5.1 Current developments in cyber security infrastructure testing developments are sourced and reviewed 5.2 New tools for VPEN testing are researched

Unit of Competency	Element	Performance Criteria
VU23302 Perform advanced penetration testing for web site vulnerabilities	1. Comprehend the web application development process	1.1 Web application development process is explained 1.2 Web application development environment and associated test phases are determined 1.3 Web architecture concepts are reviewed 1.4 Examples of web frameworks are reviewed
	2. Utilise tools and technology for testing web site content	2.1 Tools used to determine the technology stack used in web applications and web servers are utilised 2.2 Custom wordlists for spidering are created 2.3 Value of user-agent strings used in testing tools are evaluated 2.4 Identifying the technology stack of a web application utilising current resources are investigated
	3. Examine the advanced features of a current proxy testing tool suite	3.1 Review of a current proxy tool suite is demonstrated 3.2 Dangers of live scanning are explained 3.3 Utilising extended features of a current proxy testing tool, the vulnerabilities of the organisation's web site are explored
	4. Perform vulnerability scanning	4.1 Difference between automated testing and manual testing is compared 4.2 Use of an automated web application scanner to test an application is demonstrated 4.3 Results from the automated scanner report are interpreted 4.4 Use of manual testing of a web application is explored
	5. Identify common web application vulnerabilities	5.1 Common web application vulnerabilities are reviewed 5.2 Content and vulnerabilities of Content Management Systems and plugin are investigated 5.3 Remediation strategies to mitigate the defined web application vulnerabilities are formulated 5.4 Vulnerabilities for software rework are reported to the developer

Unit of Competency	Element	Performance Criteria
	6. Exploit web application vulnerabilities	6.1 Testing tools and manual methods used to exploit web application vulnerabilities are selected 6.2 Advantages and disadvantages of web application testing tools are evaluated 6.3 Use of testing tool operation to exploit web site vulnerabilities is demonstrated
VU23304 Protect industrial networks and operational technology infrastructure for an organisation	1. Define IoT and ICS differences and relevant security frameworks	1.1 Differences between IoT and ICS is identified 1.2 Key standards bodies and organisations that provide useful resources that address security issues for IoT and ICS infrastructure are identified 1.3 Current IoT infrastructure architectures are reviewed and evaluated 1.4 Current working frameworks or practices that can support the improvement of IoT and ICS from cyber security attack are identified
	2. Evaluate current IoT and ICS infrastructure for an organisation with related vulnerabilities	2.1 ICS devices used in an organisation are identified and classified 2.2 IoT devices used in an organisation are identified and classified 2.3 Responsibility for the installation and maintenance of the IoT and ICS devices for the organisation is identified 2.4 Connectivity of the ICS and IoT devices for the organisation is determined 2.5 Current vulnerabilities of the IoT and ICS devices for an organisation are identified 2.6 Risk assessment for ICS and IOT devices used in an organisation is performed 2.7 Case studies of two critical infrastructure attacks performed on an organisation are investigated 2.8 Cyber-attacks on critical infrastructure as part of military campaigns are identified
	3. Classify current cyber security vulnerabilities for IoT and ICS devices	3.1 Classification of current cyber security vulnerabilities for ICS's and IoT devices are identified 3.2 Risk assessment of vulnerabilities for current organisation's IoT and ICS devices is conducted

Unit of Competency	Element	Performance Criteria
	4. Select relevant cyber security frameworks and security critical infrastructure for IoT and ICS mitigation strategies	4.1 Resources that provide strategies to protect IoT and ICS infrastructure are sourced 4.2 Organisational security policies to protect IoT and ICS infrastructure are evaluated and selected 4.3 Strategies to enhance the protection of IoT and ICS infrastructure are adopted 4.4 Training for staff to improve the security culture is planned and implemented
	5. Monitor the effectiveness of adopted IoT and ICS infrastructure mitigation strategies	5.1 Criteria to measure the effectiveness of implemented IoT and ICS mitigation strategies is developed 5.2 Tools to monitor the organisation's IoT and ICS from cyber attacks are identified and selected 5.3 Monitoring tools for an organisation's IoT and ICS infrastructure are implemented 5.4 Effectiveness of the monitoring tools implemented for an organisation's IoT and ICS systems is reviewed and updated where necessary 5.5 Changes to organisational processes and procedures to deal with IoT and ICS infrastructure incident responses are reviewed for their effectiveness and updated where necessary
VU23305 Select and configure security devices for an organisation	1. Collate the current network security diagram, security infrastructure functional operation and security device documentation	1.1 Existing security infrastructure diagram for the organisation is sourced 1.2 In consultation with appropriate personnel the function and operation of the existing network security infrastructure is evaluated 1.3 Network security devices, systems and tools are identified
	2. Configure security devices according to their functional specification	2.1 Resources to configure the network security devices for the organisation are gathered 2.2 Organisations security policy document is sourced 2.3 Network security devices, systems and tools are configured according to the functionality described in the network security policy
	3. Verify operation of security devices	3.1 Baseline performance of the network security devices for the organisation is determined 3.2 In accordance with baseline functionality and utilising software or hardware tools the network security device performance is monitored

Unit of Competency	Element	Performance Criteria
		3.3 With appropriate personnel the effectiveness of the security device operation is evaluated
	4. Investigate and implement new network security architectures and devices	4.1 New network security devices and technologies are researched and examined 4.2 Higher level packet inspection technology for a network security device is reviewed and implemented 4.3 Holistic approaches to traffic inspection technologies for a network security device is examined 4.4 Concept of dynamic update technology to defend against new cyber-attacks for a network security device is described then implemented 4.5 Virtual network security technologies are investigated and selected 4.6 Virtual network security technology solution is configured and implemented

Employability skills

Reading

- interpret and review complex information from reference texts, vendor catalogues and websites associated with cybersecurity

Writing

- write technical reports that include analysis and/or research
- prepare written instructions for others

Oral communication

- negotiate complex cyber-related issues with team members
- speak clearly and directly on complex matters, when sharing data, requirements or other information relevant to inspection and testing outcomes in network security
- use correct cybersecurity terminology and language appropriate to the situation and target audience

Numeracy

- perform calculations in binary and hexadecimal number systems
- perform basic mathematical calculations when implementing network security infrastructure for an organisation

Learning

- listen to, or read, interpret and implement complex technical cyber security processes and procedures
- adapt own competence in response to change
- update own knowledge and skills required for network security

Problem-solving

- monitor and anticipate problems that may occur including risks and take appropriate action
- respond to network security risks in a range of complex and diverse situations
- resolve client concerns in relation to cyber security issues
- monitor and anticipate problems that may occur in the course of cyber security vulnerability inspection and testing activities

Initiative and enterprise skills

- make modification to work plans and schedules to overcome unforeseen difficulties or developments
- respond appropriately to changes in equipment, standard operation procedures and the working environment
- take appropriate actions in a diverse range of cyber security incidents
- provide leadership during unforeseen cyber security activities

Teamwork

- collaborate with others and work effectively in team problem-solving activities
- work with diverse range of people within a team environment.

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
- delegate and supervise work where appropriate

Self-management

- interpret and apply relevant enterprise procedures
- establish and follow own work plans and schedules
- manage time and priorities to meet work completion targets
- ensure work activities are compliant with legislation, codes of practices national standards and company policy

- evaluate and monitor own work performance

Technology skills

- use testing software and tools to perform risk assessment and to protect critical infrastructure and systems
- implement and monitor the application of security software
- use security protection devices and software
- secure cloud services
- perform digital forensic investigation on workstations and mobile devices

Digital literacy

- undertake independent research in a range of technical cyber-related issues
- find, evaluate, and communicate information on various digital platforms
- produce text, images, audio and designs using technology to communicate information to others



SYDNEY | MELBOURNE | BRISBANE | GOLD COAST | MANLY BEACH | ADELAIDE