Program Information Document

22603VIC Certificate IV in Cyber Security

This qualification comes from a training package created by the Department of Education and Training, Victoria defining the core and elective competency units. We've chosen specific elective units from the training package, based on input from industry experts, to address South Australia's workforce requirements.

The skills required for these roles may include, but are not restricted to:

- Respond to and monitor cyber security events in an organisation
- Use a range of tools and procedures to mitigate cyber security threats
- Protect an organisation from insider security breaches
- Develop systems to minimise network vulnerabilities and risks
- Recognise implications using cloud-based services
- Work effectively as a member of a cyber security team

Employment Opportunities

- Cyber Security Technician
- Cyber Analyst
- Penetration Tester
- Incident Response Officer
- Information Security Analyst
- Cyber Security Administrator
- Cyber Security Policy Specialist

The recommended fulltime study plan will require 12 months of study to complete this qualification.

Program Information Document

Assumed Skills and Knowledge

There are no formal entry requirements for this course however, participants are best equipped to achieve the course outcomes if they have the following digital capabilities:

- Navigate and manage files and folders in a Windows environment, or similar.
- Connect to a network through Wi-Fi.
- Use a word processor such as MS Word to produce well-structured documents.
- Able to install and configure new software on a Windows computer
- Use a video chat tools or video conferencing tools such as Google Meet, FaceTime, Zoom, Teams etc..
- Recognise the purpose of basic components of computer hardware such as RAM, hard drive, network card, external drive.
- Problem solve computer issues that may arise in relation to the above
- Use a web Browser and the internet to research a topic.
- Prompt an AI tool, such as ChatGPT, Gemini etc

If you need to develop yourself in many of these capabilities, we suggest you consider enrolling in our Certificate III in Information Technology.

Information on the contents of the Certificate III can be found here:

Certificate III in Information Technology Program Information Document.

Program Information Document

Incidentals Costs

You will be required to provide your own access to the following hardware. This hardware costs approximately $550.00.

- 1TB SSD portable hard drive,
- Webcam,
- Headset with microphone,
- Raspberry Pi 4 (or higher) Starter Kit with minimum 4GB and minimum 16GB SD card. Accessories required are as following:
  - PIR Motion Sensor (compatible with your Raspberry Pi)
  - Raspberry Pi Camera Module 3 with cable suitable for your Pi
  - 150mm Socket to Socket (F to F) Jumper Leads

Software

All software required to complete this course will be available for students at no additional cost.

Hardware

Access to computer hardware is provided at certain TAFE SA campuses.

It is important to note that for students studying this course and not able to attend a suitable campus it will be assumed that you have the necessary computer hardware to run the required resources. You will need to have a Windows machine with the following as a minimum.

- Intel i5 CPU (or equivalent AMD), (Intel i7, recommended)
- 16GB of RAM, (32GB, recommended)
- 1Tb SSD

Note: Apple MAC notebooks are not compatible with some of the software required for this course and cannot be supported.

Internet

To study away from a campus you will be required to have internet access.

This qualification requires students to use virtual machines for learning activities and assessments. Students will be required to obtain these from either their local campus or download from the Internet. Virtual machine file sizes can vary but are generally above 20GB in size. The time to download these virtual machines from the Internet may vary depending on your Internet connection speed.

Program Information Document

Required Competencies

Certificate IV in Cyber Security
National Code: 22603VIC TAFE SA Code: AC00128

This table shows the units of competency that you must have on your academic record to achieve this qualification. The National Training Package requires 16 units. The units are listed in the sequence that you should complete them. This is particularly important for part-time students. Standard study plans are provided below. The table also provides details of any assumed knowledge and skills for each unit. You must have these skills before attempting these units.

Units of Competency (listed in delivery sequence)

Unit Code	Unit Title	Core/Specialist Elective/Elective	Assumed knowledge & skills
VU23214	Configure and secure networked end points	Elective	None
ICTPRG435	Write script for software applications	Elective	None
VU23217	Recognise the need for cyber security in an organisation	Core	None
VU23216	Perform basic cyber security data analysis	Elective	None
VU23213	Use basic network concepts and protocols required in cyber security	Core	None
ICTICT443	Work collaboratively in the ICT industry	Core	None
ICTNWK422	Install and manage servers	Elective	VU23213
BSBWHS309	Contribute effectively to WHS communication and consultation processes	Core	None
VU23223	Apply cyber security legislation, privacy and ethical practices	Core	None
ICTCLD401	Configure cloud services	Elective	None
VU23218	Implement network security infrastructure for an organisation	Elective	VU23213
VU23221	Evaluate and test an incident response plan for an enterprise	Elective	VU23213 ICTNWK422
VU23222	Expose website security vulnerabilities	Elective	VU23213
VU23215	Test concepts and procedures for cyber security	Core	VU23213
VU23220	Develop and carry out a cyber security industry project	Core	VU23213 VU23215 VU23216 VU23218 VU23222
BSBINS401	Analyse and present research information	Core	None

Program Information Document

Study Plan for Full-Time Students (12 months)

The following table shows the recommended study plan for Certificate IV of Cyber Security. Each stage is one semester (or 6 months) in length. Codes in brackets are the IT Subject names which are described in the Subject Description table below.

Stage 1	
Term 1	**Term 2**
VU23214 (CVU214ITE) (4)	
VU23213 (CVU213CIN) (4)	
ICTPRG435 (PRG435PYB) (2)	
VU23217 (CVU217CSF) (4)	**VU23216** (CVU216SPB) (2)
ICTICT443 (ICT443) (2) *	**ICTNWK422** (NWK422ICW) (4)
IT Practical (4)	**IT Practical (4)**
20 hours / week	**20 hours / week**

Stage 2	
Term 1	**Term 2**
VU23220, BSBINS401 (CVU4C2PRO) (4)	
VU23218 (CVU218FGT) (2)	
ICTCLD401 (CLD401ACF) (4)	**VU23215** (CVU215PEN) (2)
BSBWHS309 (WHS309) (2) *	**VU23223** (CVU223) (2) *
VU23222 (CVU222WEB) (2)	**VU23221** (CVU221IRP) (2)
IT Practical (6)	**IT Practical (8)**
20 hours / week	**20 hours / week**

Please Note: This program structure is subject to change.

Legend:

* Competencies delivered online are marked with an asterisk

( ) The number in brackets after the subject is the number of hours per week that you would expect to attend class for that subject as a campus or virtual student.

IT Practical sessions provide support to complete subject activities and assessments.

NOTE: The study plan is for a full-time student with class-attendance. This is usually 20 hours a week of attendance. It is expected that an additional 12-15 hours would be required outside of class time to complete activities and assessments.

Program Information Document

Study Plan for Part-Time Students (24 months)

The following table shows the recommended study plan for studying the Certificate IV of Cyber Security as part-time (half-time). If a half-time plan does not meet your needs, you can study more or less subjects per term/semester, but you must follow the recommended sequence in the Required Competencies table above. Each stage is one semester (or 6 months) in length. Codes in brackets are the IT Subject names which are described in the Subject Description table below.

Stage 1	
Term 1	**Term 2**
VU23214 CVU214ITE (4)	
ICTPRG435 PRG435PYB (2)	
VU23217 CVU217CSF (4)	**VU23216** CVU216SPB (2)
IT Practical (0)	**IT Practical (2)**
10 hours / week	**10 hours / week**

Stage 2	
Term 1	**Term 2**
VU23213 CVU213CIN (4)	
ICTICT443 ICT443 (2) *	**ICTNWK422** NWK422ICW (4)
IT Practical (4)	**IT Practical (2)**
10 hours / week	**10 hours / week**

Stage 3	
Term 1	**Term 2**
VU23218 (CVU218FGT) (2)	
ICTCLD401 (CLD401ACF) (4)	**VU23223** (CVU223) (2) *
BSBWHS309 (WHS309) (2) *	
IT Practical (2)	**IT Practical (6)**
10 hours / week	**10 hours / week**

Stage 4	
Term 1	**Term 2**
VU23220, BSBINS401 (CVU4C2PRO) (4)	
VU23222 (CVU222WEB) (2)	**VU23215** (CVU215PEN) (2)
	VU23221 (CVU221IRP) (2)
IT Practical (4)	**IT Practical (2)**
10 hours / week	**10 hours / week**

Program Information Document

Please Note: This program structure is subject to change.

Legend:

* Competencies delivered online are marked with an asterisk

( ) The number in brackets after the subject is the number of hours per week that you would expect to attend class for that subject as a campus or virtual student.

NOTE: The study plan is for a part-time student studying a half-time load. This is approximately 10 hours a week of class time. It is expected that an additional 6-10 hours would be required outside of class time to complete activities and assessments

Program Information Document

IT Studies Subjects

TAFE SA IT Studies uses subject codes to indicate the context that has been chosen for the unit, guided by industry needs in South Australia. For example, **PRG435PYB** indicates that the content for delivery of unit PRG435**PYB** will include coverage of **Python** programming language.

The table below provided information on the context for each unit and provides the subject code that is used. If a subject contains more than one unit delivery and assessment will be done holistically so you will be awarded the same result for all units assessed in that subject that you have enrolled in. Your final official results will refer to the units.

Subject Description

Unit Code	IT Studies Subject Code	Description
VU23214	**CVU214ITE**	This unit provides the skills and knowledge to configure an operating system on a personal computer. It covers implementing security measures, setting user-level passwords, and managing privileges to control and monitor user access, critical steps for strengthening endpoint protection against cybersecurity threats.
ICTPRG435	**PRG435PYB**	This unit introduces the skills and knowledge needed to plan, design, and develop scripts, using **Python** a highly sought-after language in the cybersecurity field. You will explore libraries like python-nmap to automate tasks such as identifying open ports and available services on network hosts, which aids in building a network map to uncover potential security vulnerabilities.
VU23217	**CVU217CSF**	This unit provides introductory knowledge and skills to identify threats, risks, and vulnerabilities in an organisation's cybersecurity landscape. It covers potential threats across various areas, including networks, devices, applications, data, users, and infrastructure.
VU23216	**CVU216SPB**	This unit introduces knowledge and skills required to identify and analyse discrepancies in data using **Splunk**. It includes examining data collection methods, performing basic analysis, and breaking down a set of subtasks to assess their effectiveness in the overall process.
VU23213	**CVU213CIN**	This unit introduces the skills and knowledge required to understand how data is transmitted across the internet. Using the Open Systems Interconnection (OSI) model as a framework, it covers the functions and operations of key protocols, such as the Transmission Control Protocol/Internet Protocol (TCP/IP) suite, as well as the devices that facilitate data transfer, including routers and switches.
ICTICT443	**ICT443**	This unit provides the skills required to work collaboratively in virtual Information and Communications (ICT) team environments to achieve organisational objectives. It includes contributing to performance and capability within teams, participating in team activities, exchanging knowledge and skills, and providing support to team members. It applies to all individuals who work in teams that utilise multiple technologies to complete a collective task.
ICTNWK422	**NWK422ICW**	This unit describes the skills and knowledge required to install and manage a server, using **Windows Server**. It includes the ability to conduct initial configuration and testing, administration, software distribution and updates, profiling, and troubleshooting. It applies to individuals with Information and Communications Technology (ICT) skills, involved in network management, server administration and similar roles.

Program Information Document

BSBWHS309	**WHS309**	This unit describes the skills and knowledge required to contribute to work health and safety (WHS) communication and consultation in the workplace. It involves communicating WHS information to required personnel and taking appropriate follow-up action to assist in ensuring that communication and consultation processes are effective and conducive to others in the workplace who raise WHS issues.
VU23223	**CVU223**	This unit describes the skills and knowledge required to identify current Australian cyber security legislation and to be cognisance of the interdependence between the key regulators. It also looks at how to apply cyber security privacy policies and procedures for an organisation. Importantly, this subject will look at the ethical practices required for employees to conduct themselves professionally both privately and when working for an organisation, supporting their ability to work ethically and apply professional standards in their place of work.
ICTCLD401	**CLD401ACF**	This unit describes the skills and knowledge required to configure core cloud services including compute, storage, databases and autoscaling according to business needs and workload.
VU23218	**CVU218FGT**	This unit will provide a sound working knowledge of the features of the Fortinet product **FortiGate** that will support the network security for an organisation. This includes threat inspection and mitigation techniques, network security architectures, introduction to firewall setup and configuration, intrusion prevention system (IPS) setup and operation as well as internetworking operating system (IOS) software features to harden routers and switches. The subject also investigates proxy server vulnerabilities, Wireless Lan (WLAN) security vulnerabilities and the application of Virtual Private Networks (VPN's) and cryptography fundamentals.
VU23221	**CVU221IRP**	This unit provides the basic knowledge and skills required to examine an organisation's existing incident response plan (IRP) and expand it as necessary to deal with incidents more thoroughly. This will require the ability to form a team, clarify roles, interpret an incident response plan (IRP), use red, blue, and purple teams to test the IRP, implement an incident, evaluate the IRP for its effectiveness and if required make improvements.
VU23222	**CVU222WEB**	This unit provides the basic knowledge and skills required to maintain the security of an organisation's website by utilising the outcomes of the Open Web Application Security Project (OWASP). It requires the ability to apply penetration testing tools to determine the vulnerabilities of a web site, assess the vulnerabilities and report to appropriate personnel.
VU23215	**CVU215PEN**	This unit provides introductory skills and knowledge required to implement testing procedures for computer systems in an organisation. Examining common threats, ethical hacking principles, and an introduction to penetration testing, social engineering security issues, enumeration, port scanning, foot printing, traffic sniffers and wireless local area network (WLAN) vulnerabilities and includes treatment of intrusions.
VU23220 BSBINS401	**CVU4C2PRO**	Students will undertake a project that simulates a real cyber security environment. The project may include using a Cyber Security Operations Centre (CSOC) sandbox or equivalent laboratory environment. This environment allows the participant to demonstrate configuring and testing of firewalls, implementing Intrusion Detection/Prevention Systems (IDS/IPS) and evaluating and identifying

Program Information Document

		any traffic anomalies. The use of Red & Blue teaming exercises to identify security breaches and apply mitigation strategies to minimise further risk should be included as part of the exercise. This unit will also describe the skills and required to collect, organise, analyse, and present information using available systems and sources. This includes identifying research requirements and sources of information, evaluating the quality and reliability of the information, and preparing and producing reports.