Student Program Information 2023

Certificate IV in Cyber Security (22603VIC)

The Certificate IV in Cyber Security is a technician level qualification that will provide graduates with the knowledge and a comprehensive set of technical skills that enables them to:

- 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

Graduates of the course will be able to seek employment as cyber security practitioners in a range of commercial enterprises/organisations and government bodies.

The recommended study plan will require 12 months of study to complete

Subsidised Training

- You may be eligible for government subsidised training based on your employment and training level.
- For full details, including visa eligibility, please see the Skills SA website
- While this course may attract government subsidies, there may also be upfront fees, depending on any required underpinning knowledge and skills.

ALL STUDENTS, IRRESPECTIVE OF PREVIOUS STUDIES, WILL BE REQUIRED TO DO THE CORE SKILLS PROFILE FOR ADULTS (CSPA) BEFORE THEY ARE ELIGIBLE FOR GOVERNMENT SUBSIDY.

Training Package

This qualification was developed in close collaboration with a range of industry partners, including NBN Co, Cisco Australia and New Zealand, BAE Systems, Telstra, Deloitte, TAFEs and others. The information below refers to the TAFE SA IT Studies subjects and outlines the competencies that makes up those subjects. Your final official results will refer to the competencies listed below.

Student Program Information 2023

Course Admission Requirements

- Satisfactory demonstration of reading, writing and numeracy skills by undertaking the Core Skills Profile for Adults (CSPA)
- Satisfactory performance in the Certificate IV Cyber Security Skills Assessment

Assumed Skills and Knowledge

This is not an entry level qualification. There are assumed skills and knowledge that are required to commence at the Certificate IV level. These could have been gained in several ways:

- Completed the Certificate III in Information Technology (ICT30120); or
- Other study equivalent to it; or
- Have work experience and knowledge equivalent to it.

Incidentals

This course also has an incidental cost of $550.00 for 1TB portable SSD, headset with microphone, National Police Clearance, and a Raspberry Pi Kit (Inc. Cables, Motion Sensor and Camera). For those intending to study online it is recommended that you have a webcam (optional for those studying on campus).

Hardware & Software

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

It is important to note that for students studying this course online (externally) it will be assumed that you have the hardware required to run the required resources. It is recommended that you have the following as a minimum;

- Intel i5 CPU (or equivalent AMD)
- 32GB of RAM
- 1Tb SSD
- Internet Access

Internet

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 from the Internet. Virtual machine file sizes can vary but are generally above 20GB in size. Downloading these virtual machines from the Internet may vary depending on your Internet connection speed.

Student Program Information 2023

Required Competencies

Certificate IV in Cyber Security

National Code: 22603VIC TAFE SA Code: AC00128

This table shows the competencies that you must have on your academic record to achieve this qualification and the IT subjects you would complete.

CORE AND ELECTIVE UNITS				
Unit Code	**Unit Title**	**Core/Specialist Elective/Elective**	**Assumed knowledge & skills**	**IT Studies subject code**
VU23213	Use basic network concepts and protocols required in cyber security	Core		CVU213CIN
VU23217	Recognise the need for cyber security in an organisation	Core		CVU217CSF
ICTICT443	Work collaboratively in the ICT industry	Core		ICT443
VU23215	Test concepts and procedures for cyber security	Core		CVU215PEN
VU23220	Develop and carry out a cyber security industry project	Core	VU23213 VU23215	CVU4C2PRO
BSBINS401	Analyse and present research information	Core		CVU4C2PRO
VU23223	Apply cyber security legislation, privacy and ethical practices	Core		CVU223
BSBWHS309	Contribute effectively to WHS communication and consultation processes	Core		WHS309
ICTPRG435	Write script for software applications	Elective		CVU435PYB
VU23214	Configure and secure networked end points	Elective		CVU214ITE
ICTNWK422	Install and manage servers	Elective		NWK422ICW
VU23216	Perform basic cyber security data analysis	Elective		CVU216SPB
VU23218	Implement network security infrastructure for an organisation	Elective	VU23213	CVU218FGT
VU23222	Expose website security vulnerabilities	Elective		CVU222WEB
VU23221	Evaluate and test an incident response plan for an enterprise	Elective		CVU221IRP
ICTCLD401	Configure cloud services	Elective		CLD401ACF

Student Program Information 2023

Subject Descriptions

Subject	Description
CVU213CIN	This subject introduces the skills and knowledge required to comprehend how data travels around the internet. It includes the function and operation of protocols such as Open System Interconnection (OSI) and Transmission Control Protocol/Internet Protocol (TCP/IP) suite and devices that facilitate data transfer such as routers and switches.
CVU214ITE	This subject provides the skills and knowledge required to configure an operating system on a personal computer, adding security, setting user level passwords and privileges to limit and identify user access – all required to increase protection of the end point from cyber security attacks.
CVU217CSF	This subject provides introductory knowledge and skills to recognise threats, risks, and vulnerabilities to cyber security in an organisation. The threats to an organisation include networks, machines, applications, data, users, and infrastructure.
ICT443	This subject 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.
NWK422ICW	This subject describes the skills and knowledge required to install and manage a 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.
CVU223	This subject 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.
PRG435PYB	This subject introduces the skills and knowledge required to plan, design and build scripts, using PYTHON as the scripting language that is highly sort after in the cyber security field. This will include use of libraries such as python-nmap to automate functions such as the identification of open ports and services available on a network host thus helping to build a map of a network to identify potential security vulnerabilities.
CVU216SPB	This subject introduces knowledge and skills required to detect and recognise discrepancies in data by performing analysis, and looks at the collection of data and performing basic analysis which includes the process of breaking down a set of subtasks which are examined for their effectiveness.
CVU218FGT	This subject 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.
CVU222WEB	This subject 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.
CVU215PEN	This subject 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.
CVU221IRP	This subject 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.
CLD401ACF	This subject describes the skills and knowledge required to configure core cloud services including compute, storage, databases and autoscaling according to business needs and workload.
WHS309	This subject 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.
CVU4C2PRO	Students will then 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 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 subject 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.

Student Program Information 2023

Choosing a Study Plan

TAFE SA Study Plan for Full-Time Students (12 months)

The following table shows the recommended study plan for the Certificate IV of Cyber Security (22603VIC). Each stage is one semester (or 6 months) in length for Full-Time student*.

These are eligible for Subsidised Training

Please Note: This program structure is subject to change.

Stage 1		Stage 2	
Term 1	**Term 2**	**Term 1**	**Term 2**
Subjects required to complete the Certificate IV qualification			
CVU214ITE (4) CVU213CIN (4) PRG435PYB (2)		CVU4C2PRO (4) CVU218FGT (2)	
CVU217CSF (4) ICT443 (4) IT Prac (4)	CVU216SPB (2) NWK422ICW (4) IT Prac (4)	CLD401ACF (4) WHS309 (2) CVU222WEB (2) IT Prac (6)	CVU215PEN (2) CVU223 (2) CVU221IRP (2) IT Prac (8)
(20)	(20)	(20)	(20)

Please Note: This program structure is subject to change.

Legend:

* The length of time for Part-Time students will depend on the number of subjects studied in each semester.

( ) The number in brackets after the subject is the indicative number of contact hours per week that you expect to study at a TAFE SA campus for that subject.

IT Prac sessions to complete subject activities, assignments and tests

NOTE: The study plan is for a full-time student with class-attendance (virtual or face-to-face). 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.

Click here to apply for this qualification