Canberra Institute of Technology

CYBER SECURITY

cit.edu.au

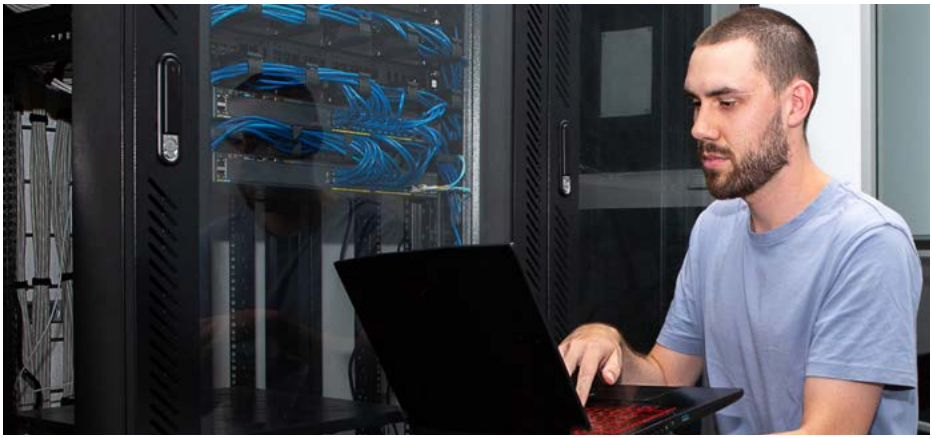
CYBER SECURITY COURSES

Our cyber security courses are designed to meet the needs of current workforce and employment opportunities in ICT security systems. You will gain skills to assess, manage and protect against cyber security threats across a range of industries.

Likely job outcomes

Qualifications in cyber security can lead to employment options in a variety of commercial enterprises, organisations and government bodies, including but not limited to:

- Cyber Security Support Officer
- Security Penetration Tester
- Information Systems Security Support Officer
- Network Security Support Officer
- Website Security Support Officer
- Cyber Security paraprofessional supporting the operation of large, small and medium enterprise computing environments
- Computer Helpdesk Technician
- Cyber Security Intrusion Tester
- Systems Tester
- PC Support
- Network Security Support Officer
- Network Security Trainee
- Website Security Support Officer
- Systems administration - Network Administrator
- Network Security Administrator - Cyber Security Engineer
- Cyber Security Analyst - Information Security Analyst
- Security Operations Centre (SOC) Analyst - Cyber Security Operations Specialist
- Intrusion Detection Analyst - Incident Responder
- Penetration Tester (Pen-Tester) - Digital Forensics Analyst.



Graduate Certificate in Networking and Cyber Security 10907NAT

This course is designed for Network Engineers and Cyber Security professionals who are currently working in the industry and/or on a study pathway in the field. It provides theoretical knowledge as well as hands-on practical application using industry standard hardware and software to develop your skills to:

- enhance technical network and cyber security capabilities
- meet organisational requirements under cybersecurity law
- ensure vigilance and adaptability to edge network security solutions
- understand cyber security management concepts and risk management
- use a range of high-level specialist IT networking and cyber security analytic skills

It prepares you to obtain the recognised industry certifications:

- CISCO certified professional (Security) - CISCO Cyber Operations
- Palo Alto certified network security engineering - Certified ethical hacker

Duration

The standard duration for this course is one year, with two sessions per week. A part-time option of one session per week over two years is also available.

Each session is three hours, with an additional three to five hours of self-directed learning per week required.

Entry requirements

For entry to this course, you must have:

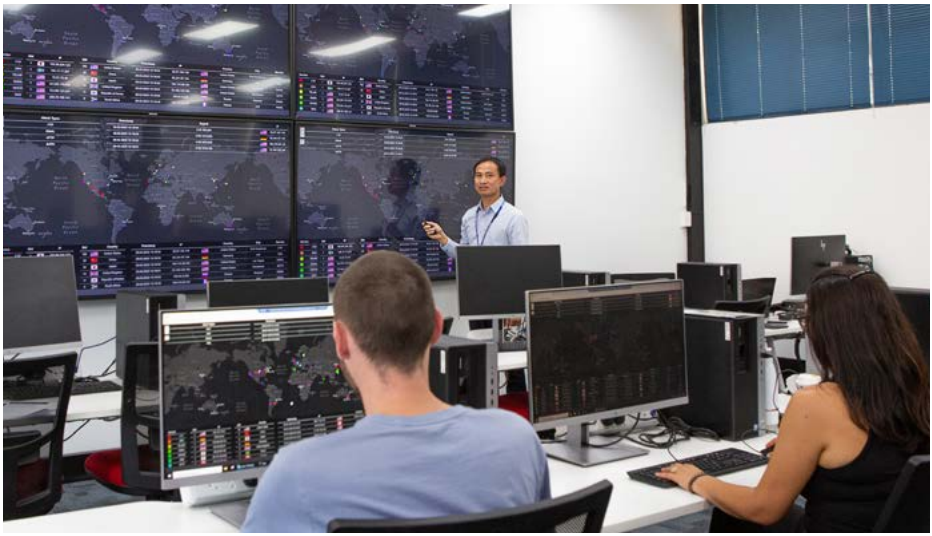
- a relevant higher education qualification

OR

- completed a diploma or advanced diploma in related fields of study **AND**
- at least one year full-time equivalent workplace experience with exposure to networking and cyber security

OR

- at least two years equivalent full-time relevant workplace experience with exposure to networking and cyber security.



Certificate IV in Cyber Security 22603VIC

This course provides you with a range of cyber security technical skills and knowledge. You will learn to monitor the risk of cyber security attacks, implement appropriate software, use a range of tools and procedures to mitigate cyber security threats, protect an organisation from insider security breaches, develop systems to minimise network vulnerabilities and risks, recognise implications using cloud-based services and work effectively as a member of a cyber security team.

Duration

This course can be completed in one year (2 semesters - approx. 15 hours per week) full-time, or part-time equivalent. It is expected that you will spend approximately the same number of hours in private study to practice skills and apply new knowledge.

Entry requirements

There are no formal entry requirements. However, to increase your likelihood of success it is recommended you have successfully completed Year 12 or equivalent, be a mature age applicant, or have level 3 ACSF for learning, reading, writing and literacy, and numeracy.

Prior IT and/or Networking experience or knowledge is not required but is an advantage.

Course Requirements

You must complete eight core units (c) and eight elective units (e) to achieve the Certificate IV in Cyber Security (22603VIC) qualification.

Statement of Attainment
Introduction to Organisational Cyber Security

This course provides introductory knowledge and skills for cyber security in an organisation. You will learn how to recognise threats, risks and vulnerabilities that affect networks, machines, applications, data, users, and infrastructure. Introduces the implementation of tools and systems an organisation can use to protect from cyber-attacks. It also covers an introduction to common cyber security attack mechanisms, identity and threat management and security issues surrounding Internet of Things (IOT) devices.

To achieve this statement of attainment you will need to complete the unit VU23217 Recognise the need for cyber security in an organisation.

Duration

Approximately six weeks. You will be required to participate in study for three to four hours per week to complete this course.

Delivery

Online, as a self-paced series of lessons and activities, which you can complete at your own pace

Statement of Attainment
Introduction to Cyber Security Awareness

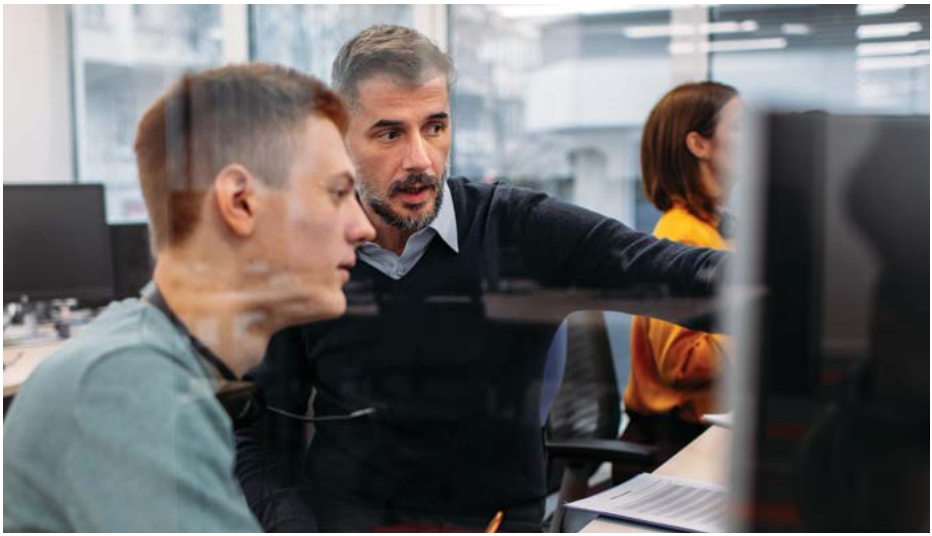
This course is a designed to give you the skills and knowledge needed to implement a range of security protection for your devices. This will reduce the risk of a device's operation being affected by spam or destructive software.

Duration

Approximately six weeks. You will be required to participate in study for three to four hours per week to complete this course.

Delivery

Delivery is online, as a self-paced series of lessons and activities, which you can complete at your own pace.



Statement of Attainment
Cyber Security Awareness Skill Set BSBSS00094

This course is designed for those working in a cyber related role. It will provide you with the introductory knowledge and skills to engage in cyber security threat assessments and protection against cyber security risk for your organisation. You will apply a broad set of skills and knowledge to assist an organisation improve cyber threat awareness and protect against cyber risk across a broad range of industries.

Duration

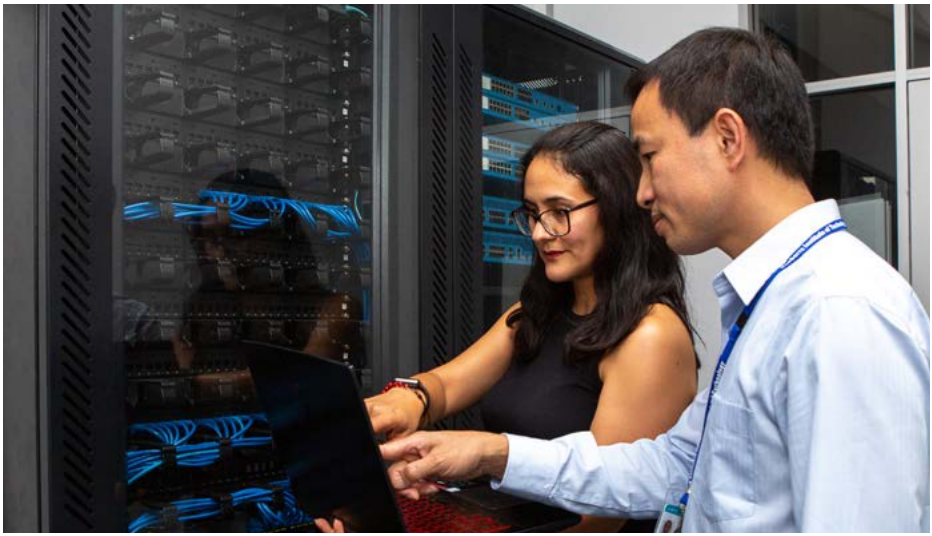
This course will be completed in a variety of models for approximately 51 hours. Please refer to a current timetable for more information

Delivery

Training will occur either face-to-face at one of our CIT campuses or virtually

Subjects

- Protect own personal online profile from cyber security threats BSBXCS301
- Identify and report online security threats BSBXCS302
- Securely manage personally identifiable information and workplace information BSBXCS303
- Promote workplace cyber security awareness and best practices BSBXCS402



Statement of Attainment
Cyber Security Threat Assessment and Risk Management Skill Set
BSBSS00093

This course will provide you with introductory knowledge and skills to contribute to cyber security threat assessments and cyber security risk management in your current role. You will apply a broad set of skills and knowledge to engage with assessment of cyber threats to an organisation and the management of the identified threats, across a broad range of industries.

Duration

This course will be completed in a variety of models for approximately 30 hours. Please refer to a current timetable for more information.

Delivery

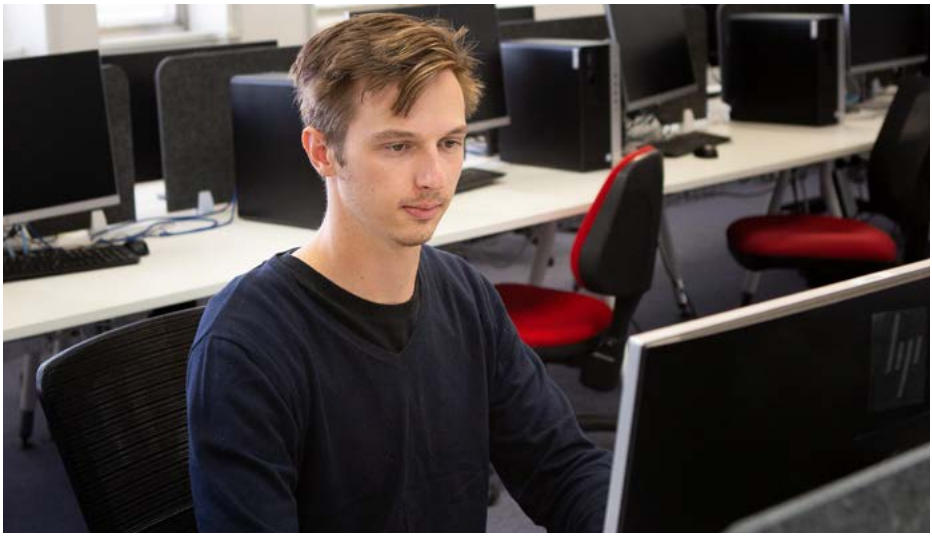
Training will occur either face-to-face at one of our CIT campuses or virtually

Subjects

- Contribute to cyber security threat assessments BSBXCS403
- Contribute to cyber security risk management BSBXCS404

Likely job outcome

- Cyber Security Support Officer
- Security Penetration Tester
- Information Systems Security Support Officer
- Network Security Support Officer
- Website Security Support Officer



Essential Eight Training

The Essential Eight Assessment Course has been designed by the Australian Signals Directorate's Australian Cyber Security Centre (ACSC) and is delivered in partnership by TAFEcyber.

This course uses a blend of specialist knowledge, experience and hands-on technical training to enable cyber security and ICT professionals to understand the ACSC's Essential Eight Assessment Guidance Package and the Essential Eight Maturity Model. These skills and knowledge will enable participants to effectively assess and improve their organisation's cyber security posture.

You will learn the intent and application of ASCS's Essential Eight mitigation strategies, how to use ASCS-designed tools, how to accurately test the implementation of the Essential Eight security controls and how to develop an accurate actionable assessment report.

You will receive a certificate upon successfully passing the exam.

Duration

24 hours including exam workshop

Location

CIT Reid

Essential Eight Assessment Course designed by:

Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Delivered in partnership by:

TAFEcyber

CYBER SECURITY

POSSIBLE STUDY PATHWAY

Below is an example pathway option available to you when you study one of our cyber security courses. Direct entry into any course is also available.

Statement of Attainment Cyber Security Threat Assessment and Risk Management Skill Set BSBSS00093

Statement of Attainment Cyber Security Awareness Skill Set BSBSS00094

Statement of Attainment Introduction to Cyber Security Awareness

Statement of Attainment Introduction to Organisational Cyber Security

CERTIFICATE III IN INFORMATION TECHNOLOGY ICT30120

↓

CERTIFICATE IV IN CYBER SECURITY 22603VIC

↓

DIPLOMA OF INFORMATION TECHNOLOGY ICT50220

↓

GRADUATE CERTIFICATE IN NETWORKING AND CYBER SECURITY 10907NAT
(Entry requirements necessary)

Canberra Institute of Technology

For more information:
cit.edu.au/cyber
infoline@cit.edu.au
02) 6207 3188

CRICOS NO. 00001K – RTO 0101
OCT 23 – 5547613752