Skills and Career Guide

Document Control	
Last Edited and Published	23 February 2018
Document Source	www.securitycolony.com
Concept & Use	Hivint prepared this document as an attempt to put together a fairly comprehensive compilation of cyber security industry qualifications and certifications in Australia, and to associate them with key roles within the industry. It is targeted to support selection of certifications and training when pursuing a particular career objective and also to identify relevant certifications and training when recruiting for a particular cyber security role.
Copyright	Hivint tools and template documents are provided for the use of subscribers to Hivint's "Security Colony" Portal. The detailed copyright statement associated with all Hivint resources is available at www.securitycolony.com however the short version is that subscribers to the portal may use this document either in whole or in part as a basis and guide for document creation without any need to attribute the work to Hivint, and without any further obligations. Other consultants or professionals may work with these documents for their clients provided that *the end-client is a subscriber to the portal*. Feel free to delete this Document Control page when using.
Disclaimer	While we are confident in the quality of our work, as we don't know exactly how you're going to use this information, to the extent permitted by law, this document is provided without any liability or warranty. This document is intended as a general guide only and users should use their professional expertise – or seek professional advice as necessary – in deciding how and where to use it. This information is not legal, regulatory or compliance advice and should not be relied upon as such.

Skills and Career Guide

Executive Summary

The objective of this guide is to draw together information on cyber security industry qualifications and certifications, and associate them with key roles within the industry to support:

1. The selection of certifications and training to pursue a particular career objective;
2. The identification of relevant certifications and training to look for when recruiting for a particular cyber security role; and
3. The cross-training of broader IT professionals wishing to move into cyber security.

The intent of the Career Path section of the Guide is to support cyber security professionals in understanding the best accreditations or skills development programs for entering the industry and moving through the industry into the various specialisations available.

The intent of the Skill Selection section of the Guide is to support both recruiters (internal and external) and businesses (via vendor selection processes), to understand which accreditations and skills are relevant for the particular problem they are trying to solve within their business.

The roles selected are generic extrapolations of the many descriptions available for similar appointments, so readers should be able to find a close match to their needs. To this end the document endeavours to remain consistent throughout by adhering to the chosen nomenclature.

Note that the report does not seek to be the 'source of truth' on individual accreditation programs, but rather references the sites maintained by the program providers for this purpose; the intent of the report is explaining the positioning and use of the accreditation programs within the industry.

It is anticipated that the ultimate manifestation of this report will be an online resource, allowing for easy linking of the elements contained within. It is also noted that the industry and the programs within it are changing rapidly so this will necessarily be a living a document.

Contents

How to Read this Document

It is widely acknowledged that cyber security is growing at a rapid rate and that there is increasing demand for cyber security talent. This skills and career guide is intended to provide insights to support professionals within the industry – or seeking to get into the industry – understand the requirements needed to move upwards within their field or land a first job in cyber security. We have assembled what we believe is a reasonably complete list of cyber security roles against industry based certifications, vocational training courses and university degrees, and have assessed and compared the merits and usefulness of each one as it relates to specific industry related appointments.

This guide recognises that diversity of thought is critical in cyber security, so we encourage candidates to pursue their passion into the industry. Concurrently, we encourage organisations to recruit people with the specific intention of providing and enabling them with the cyber security training and associated skills outlined in this document. As useful and valuable as all of these accreditations and education programs are, there is no replacement for real-world experience.

Cyber Security Programs. As shown in the 'map' on page 12, we have grouped cyber security courses into six groupings (with details of the groups at the bottom of the table):

- Industry certifications sponsored by recognised industry associations
- Vocational training courses usually offered at State level TAFE institutions
- Graduate courses offered by universities
- Cyber security bachelor's degrees
- Cyber security master's degrees
- General non-cyber security degree programs

While the cyber security industry is generally accommodating with regard to non-cyber security specific degrees, the scope of this guide requires that the focus is on cyber security related qualifications and certifications so non-cyber degrees are mapped as overarching streams within the cyber security courses and roles matrix, rather than identifying individual programs.

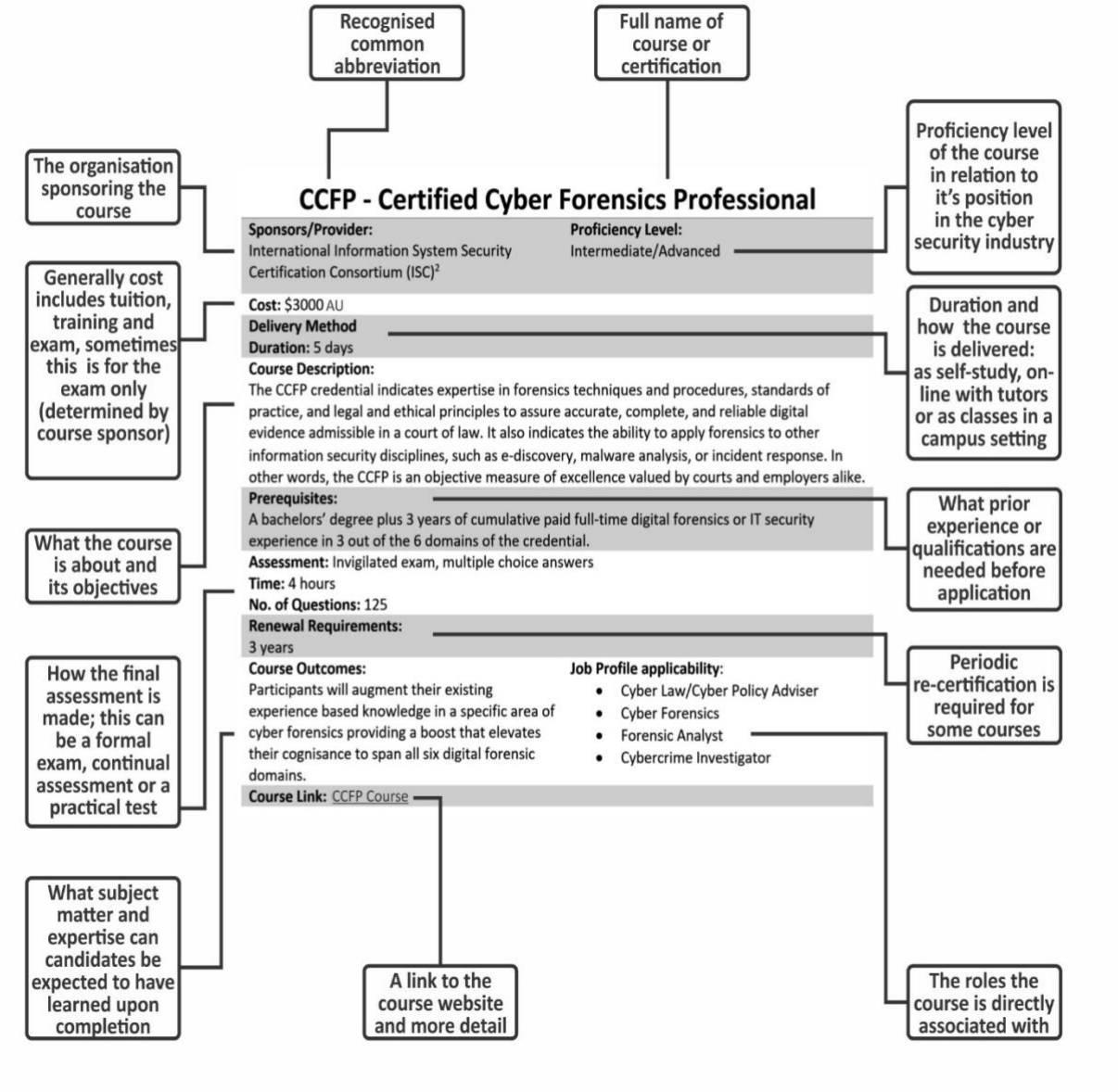
Each course description provides detail on the proficiency level offered, associated costs, the duration, mode of delivery, assessment method, and industry applicability as it may relate to identified cyber security roles. Proficiency level of certifications are categorised as:

- **Entry level:** Completion of the course allows candidates to undertake graduate level jobs, they have learned basic skills that will allow them to navigate a cyber related role under supervision.
- **Intermediate level:** Completion of the course allows candidates to undertake supervisory, team leader or independent advisory roles.
- **Advanced level:** Completion of the course should equip candidates with the necessary abilities to take on senior roles across a number of managerial disciplines or undertake complex technical lead roles in a supervisory capacity.

These assessments have been made based on Internet based research, reviewing course literature and associated institution websites. This was then measured against Hivint's in-house experience

and where necessary, the canvassing of external industry experts. The job profiles suitable for each course were identified and the courses rated for applicability and mapped against a set of agreed roles aggregated from the hundreds of possibilities available. For certifications that have mandatory renewal requirements, these are identified along with a link to the sponsoring body where more comprehensive detail, such as local availability, enrolment process and any prerequisites are required for each course are detailed.

Cyber Security Programs Template



Cyber Security Roles

Cyber security roles (left edge of the table on page 12) and their associated titles vary widely along with their responsibilities and the requirements that each role corresponds to. We have attempted to use relatively generic naming protocols that should allow for ready identification of what a given role is intended to represent. Roles in the table are described from the most technical skill requirements at the bottom of the list, to the least technical that populate the top – noting that obviously there can be significant variance within any particular role for any particular organisation. Each role in the description section is generally split into three experience and qualification related divisions:

- Entry level
- Intermediate level
- Advanced level

Intermediate and advanced level roles are grouped together in the description section, as the skills at these levels generally align with each other. The difference between the designated level is determined through the distinction of time spent in the industry. A third consideration described is that of lateral career transition, by non-cyber security ICT related professionals. ICT professionals with a relevant job profile and associated core skills that can potentially track across to a cyber security role; these are mapped with skills any such aspirant could potentially develop to enter the cyber security. The skill sets are populated through the analysis of job/recruitment sites, to help determine their suitability for transition into a cyber security role.

Entry level roles are often initially populated as part of an internship, first tier entry (having completed a tertiary or vocational education program), or through a formal graduate program. In this document, this is not presumed. The roles are linked to certifications that should be considered by incumbents as aspirational, and therefore, may not always be immediately available to those that do not meet the required industry related experience or associated preliminary qualifications. All role descriptions are accompanied - where applicable - by a list of advantageous or complimentary skills that fall outside the scope provided by formal qualifications.

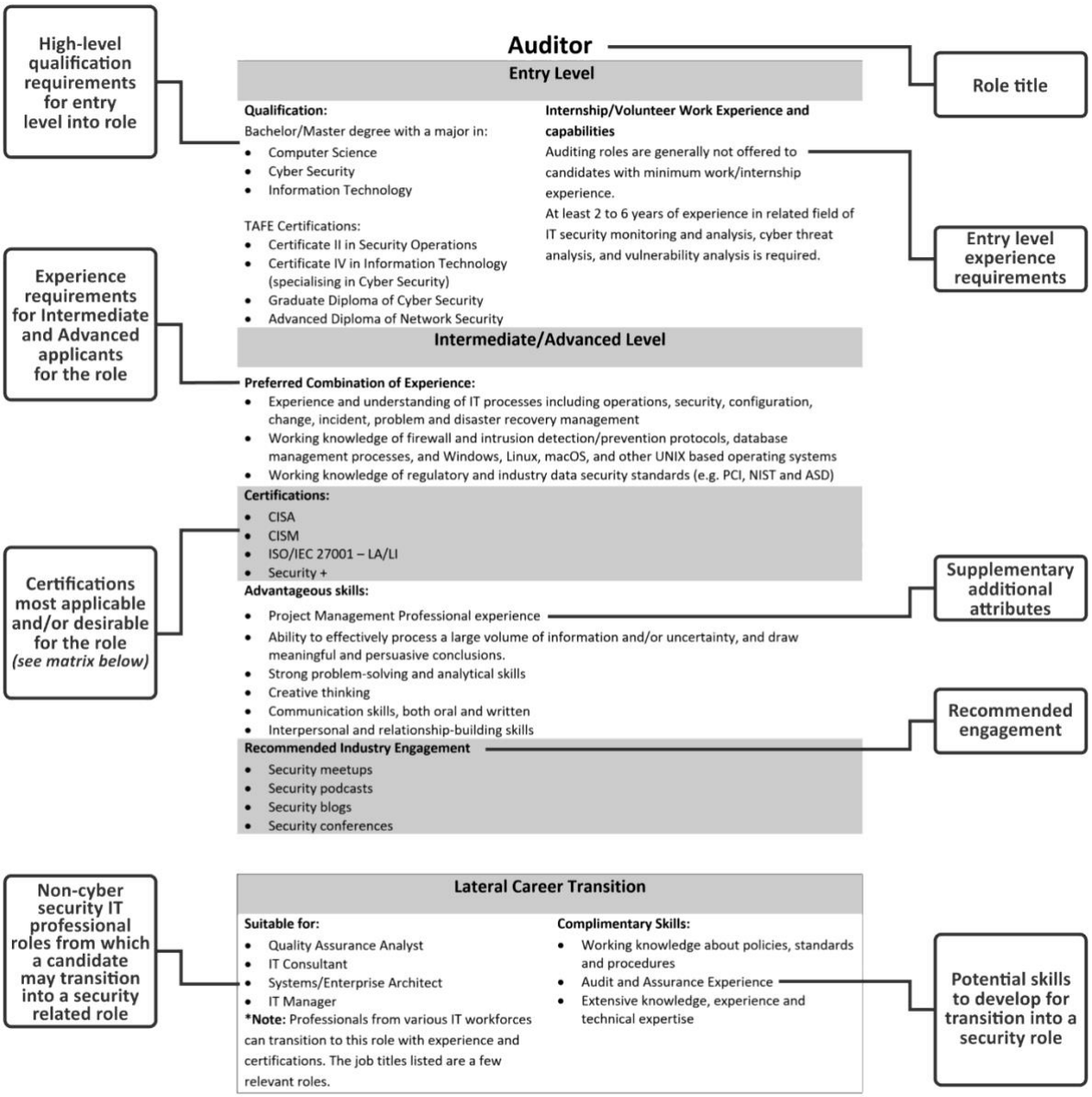
Advanced and intermediate level roles do however, presume necessary experience and the associated abilities along with suggested complimentary and developmental certifications.

This guide also takes care to includes suggestions for lateral career transition pathways as an encouragement for professionals with general information technology experience or those occupying non-security related technical roles. To this end, only relevant industry recognised cyber security courses – determined through canvassing industry and professional association websites, looking for certifications and qualifications, against individual staff members, researching of job boards and input from industry experts - have all been included. The existence of alternative transition pathways is certainly acknowledged, and while none are discouraged, we simply provide one approach that is likely to be effective in consideration of time, effort and money.

It is important to understand that all skills, degrees, courses, and certifications mentioned are not set in stone. They are suggestions, backed by an analytical methodology; designed not just to further careers in cyber security, but to grow the entire industry that in the coming years and decades will

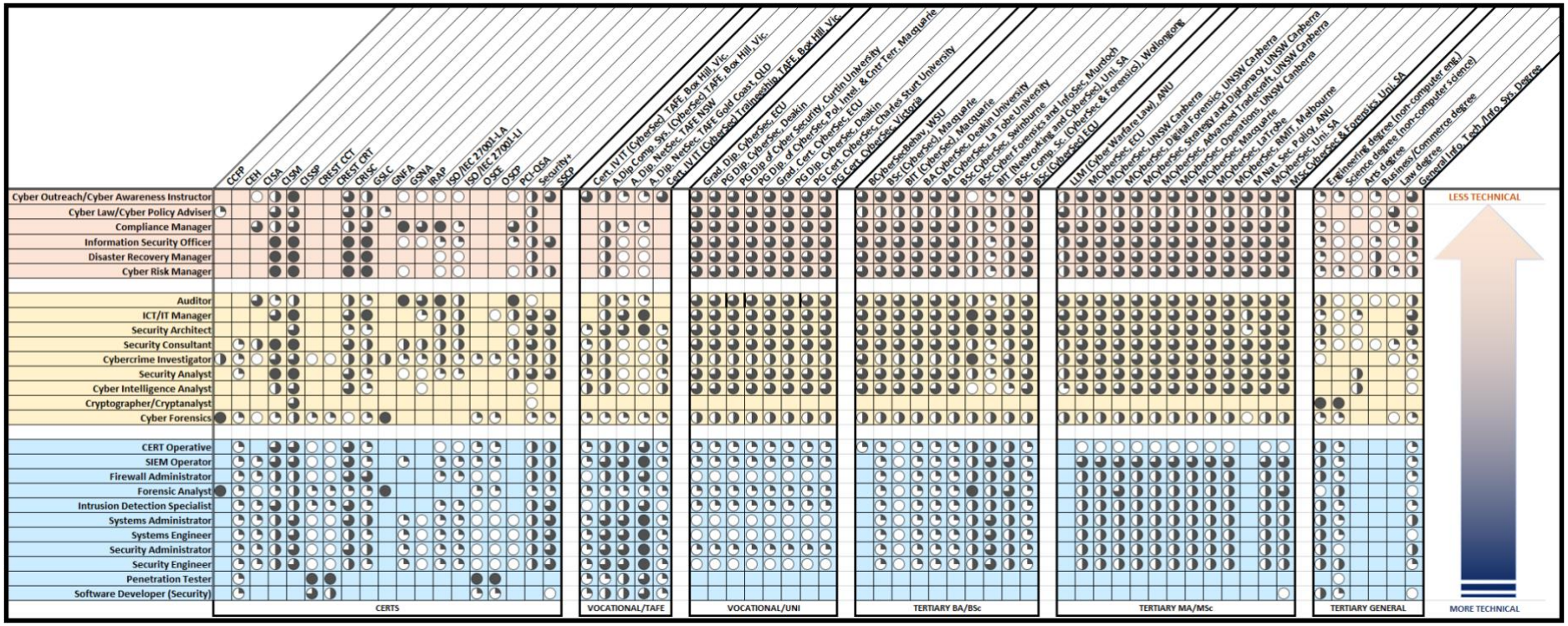
be required to monitor and secure the emerging hyper-connected society; cyber security as an industry benefits those with an enduring desire to learn, adapt and improve.

Cyber Security Role Template



Map of Cyber Security Courses and Roles

The following 'map' of courses and roles includes a 0 – 5 scale of relevance, as reflected via the shaded circles. No circle represents a '0' (that in our opinion, the certification is not relevant for that role), an empty circle represents a '1', a quarter shaded circle a '2', a half shaded circle a '3', a three-quarter shaded circle a '4', and a fully shaded circle a '5' (indicating that in our opinion, this certification demonstrates the skills required for that role comprehensively).



Cyber Security Programs - Certification

CCFP - Certified Cyber Forensics Professional

Sponsors/Provider: International Information System Security Certification Consortium (ISC)[2]	**Proficiency Level:** Intermediate/Advanced
Cost: Approximately $3,000 AUD, Cost of course is provided to candidates upon request from (ISC)[2]	
Delivery Method **Duration:** 5 days	
Course Description: The CCFP credential indicates expertise in forensics techniques and procedures, standards of practice, and legal and ethical principles to assure accurate, complete, and reliable digital evidence admissible in a court of law. It also indicates the ability to apply forensics to other information security disciplines, such as e-discovery, malware analysis, or incident response. In other words, the CCFP is an objective measure of excellence valued by courts and employers alike.	
Prerequisites: A bachelor's degree plus 3 years of cumulative paid full-time digital forensics or IT security experience in 3 out of the 6 domains of the credential.	
Assessment: Invigilated exam, multiple choice answers **Time:** 4 hours **No. of Questions:** 125	
Renewal Requirements: 3 years	
Course Outcomes: Participants will augment their existing experience based knowledge in a specific area of cyber forensics providing a boost that elevates their cognisance to span all six digital forensic domains.	**Job Profile applicability**: • Cyber Law/Cyber Policy Adviser • Cyber Forensics • Forensic Analyst • Cybercrime Investigator
Course Link: CCFP Course	

CEH - Certified Ethical Hacker

Sponsors/Provider:
EC-Council

Proficiency Level:
Entry Level

Cost: Approximately $3,300 AUD for training and exam

Delivery Method: Face -to- face and online training or ad hoc self-study from textbooks
Duration: 5 days training course

Course Description:
Certified Ethical Hacker is an entry level professional qualification. The CEH understands how to look for weaknesses and vulnerabilities in target systems and uses the same knowledge and tools as a malicious hacker, but in a lawful and legitimate manner to assess the security posture of a target system(s). The CEH credential certifies individuals in the specific network security discipline of Ethical Hacking from a vendor-neutral perspective.

Prerequisites:
Entry level certification. If you plan on attending the exam without attending official training, the candidate must have at least two years of information security related experience

Assessment:
Exam module: Multiple choice exam
Time: 4 hours
Question: 125 questions

Renewal Requirements:
None specified

Course Outcomes:
Participants will be able to:
- Demonstrate specialist ethical hacking skills
- Understand and locate network weaknesses

Job Profile applicability:
- Penetration Tester
- Auditor
- Cybercrime Investigator
- Cyber Forensics
- Security Analyst
- Security Consultant
- CERT Operative
- SIEM Operator
- Firewall Administrator
- Forensic Analyst
- Intrusion Detection Specialist
- Systems Administrator
- Systems Engineer
- Security Administrator
- Security Engineer

Course Link: CEH Course

CISA - Certified Information Systems Auditor

Sponsors/Provider:
ISACA

Proficiency Level:
Intermediate/Advanced Level

Cost: $2,960 AUD + GST for CISA training
Exam fee: ISACA member: $575 USD, non-member: $760 USD

Delivery Method: Face-to-face and online training or ad hoc self-study from textbooks
Duration: 4 days training course

Course Description:
Certified Information Systems Auditor. For many of the most in-demand IS/IT professionals, and the enterprises they serve, the attainment of Certified Information Systems Auditor (CISA) certification has become accepted proof of the necessary competency and experience for a wide range of essential roles

Prerequisites:
3 - 5 years of related work experience

Assessment:
Exam module: Multiple choice exam
Time: 4 hours
Questions:150 question

Renewal Requirements:
3 years

Course Outcomes:
Participants will be proficient in:
- IT assurance
- Technology controls
- Standards and practices
- Organisation and management
- Information security principles
- Software development
- Information systems

Job Profile applicability:
- Cyber Outreach/Cyber Awareness Instructor
- Compliance Manager
- Auditor
- Security Consultant
- Cybercrime Investigator
- Security Analyst
- Cyber Forensics
- SIEM Operator
- Firewall Administrator
- Forensic Analyst
- Intrusion Detection Specialist
- Systems Administrator
- Systems Engineer
- Security Administrator
- Security Engineer

Course Link: CISA Course

CISM - Certified Information Security Manager

Sponsors/Provider:	**Proficiency Level:**
ISACA	Advanced Level

Cost: $3,450 AUD + GST for CISM training
Exam fee: ISACA member: $575 USD, non-member: $760 USD

Delivery Method: Face-to-face and online training or ad hoc self-study from textbooks
Duration: 5 days training course

Course Description:
Certified Information Security Manager. For many of the most in-demand information systems professionals and the enterprises they serve, the attainment of a Certified Information Security Manager certification has become accepted proof of the necessary competency and experience for a wide range of information security, risk and senior management roles across the globe.

Prerequisites:
5 years related work experience

Assessment:
Exam module: Multiple choice exam
Time: 4 hours
Question: 150 questions

Renewal Requirements:
3 years

Course Outcomes:
Participants will be proficient in:
- Information Security Governance
- Information Risk Management
- Information Security Program Development and Management
- Information Security Incident Management

Job Profile applicability:
- Cyber Outreach/Cyber Awareness Instructor
- Cyber law/Cyber policy adviser
- Compliance Manager
- Information Security Officer
- Disaster Recovery Manager
- Cyber Risk Manager
- Auditor
- ICT/IT Manager
- Security Consultant
- Cybercrime Investigator
- Cybercrime Analyst
- Cyber Intelligence Analyst
- Cyber Forensics

Course Link: CISM Course

CISSP - Certified Information Systems Security Professional

Sponsors/Provider:
International Information System Security Certification Consortium (ISC)^2

Proficiency Level:
Intermediate/Advanced

Cost: $3,706 AUD at discount for defence personnel for $ 3,370 AUD for CISSP training
Exam cost: 759.53 AUD

Delivery Method: Face-to-face or ad hoc self-study from textbooks
Duration: 5 days training course

Course Description:
The CISSP curriculum covers subject matter in a variety of Information Security topics across eight domains. The CISSP examination is based on what (ISC)² terms as the Common Body of Knowledge (CBK). This is represented as a taxonomy and collection of topics relevant to information security professionals around the world, establishing a common framework of InfoSec terms and principles that professionals utilise to discuss, debate and resolve matters pertaining to the field with a common understanding.

The eight domains:

- Security and Risk Management
- Asset Security
- Security Engineering
- Communications and Network Security
- Identity and Access Management
- Security Assessment and Testing
- Security Operations
- Software Development Security

Prerequisites:
5 years industry related experience

Assessment: Invigilated exam, multiple choice answers
Time: 6 hours
No. of Questions: 250 questions

Renewal Requirements:
Over a period of three years, CISSP candidates must earn 120 CPE credits with a minimum 40 CPE credits every year before their certification's annual anniversary to maintain CISSP certification. An annual certification fee of 85 USD is applicable each year **of** the **three-year certification cycle**

Course Outcomes:
Participants will augment their existing experience-based knowledge in a specific area of information security, providing a boost that elevates their cognisance to span all eight information security domains.

Job Profile applicability:

- Cyber Outreach/Cyber Awareness Instructor
- Cyber Law/Cyber Policy Adviser
- Compliance Manager
- Information Security Officer
- Disaster Recovery Manager
- Cyber Risk Manager
- Auditor
- ICT/IT Manager
- Security Architect
- Security Consultant
- Cybercrime Investigator
- Security Analyst
- Cyber Intelligence Analyst
- Cryptographer/Cryptanalyst

- Cyber Forensics
- CERT Operative
- SIEM Operator
- Firewall Administrator
- Forensic Analyst
- Intrusion Detection Specialist
- System Administrator
- Systems Engineer
- Security Administrator
- Security Engineer

Course Link: CISSP Course

CREST CCT - Certified Infrastructure Tester

Sponsors/Provider:
Crest

Proficiency Level:
Intermediate Level

Cost:
Exam fee: Approximately $3,000 AUD + GST

Delivery Method: Exams held face-to-face at University of Canberra in the ACT with ad hoc self-study from textbooks

Course Description:
The examination is a rigorous assessment of the candidate's ability to assess a network for flaws and vulnerabilities at the network and operating system layer across:

- Public domain information sources
- Networking
- Windows operating systems
- Unix operating systems
- Desktops
- Databases
- Voice networking
- Wireless networking.

Prerequisites:
Unspecified related work experience

Assessment:
Exam module: The examination consists of three tasks:
- A hands-on practical examination
- A multiple choice technical examination
- long form 'essay style' written paper.

To pass the exam, the candidate must pass all three sections.
Time: 2 ½ hours for the written component, and 3 ½ hours for practical components of exam
Question:
Written exam: 90 multiple choice questions, and three long form questions
Practical exam: Subsections of application and infrastructure question with scenario question for each component

Renewal Requirements:
3 years

Course Outcomes:
Participants will be able to:
- Demonstrate specialist ethical hacking skills
- Understand and locate network weaknesses
- Identify and assess OS flaws

Job Profile applicability:
- Cybercrime Investigator
- Cyber Forensics
- CERT Operative
- SIEM Operator
- Firewall Administrator
- Forensic Analyst
- Intrusion Detection Specialist
- System Administrator
- Systems Engineer
- Security Administrator
- Security Engineer
- Penetration Tester
- Software Developer (Security)

Course Link: Crest CCT Course

CREST CRT - Certified Registered Tester

Sponsors/Provider:
Crest

Proficiency Level:
Intermediate Level

Cost:
Exam Fee: $1000 AUD + GST

Delivery Method: Exams held face-to-face at University of Canberra in the ACT with ad hoc self-study from textbooks

Course Description:
The entry level Registered Tester examination is designed to assess the candidate's ability to carry out basic vulnerability assessment and penetration testing tasks.

Prerequisites:
Unspecified related work experience

Assessment:
Exam module: The examination consists of two tasks:
- A hands-on practical examination
- A multiple-choice technical examination
To pass the exam, the candidate must pass both sections.
Time: 3 ½ hours
Question:
Written exam: 120 multiple choice questions
Practical exam: Series of stages split into structured tasks for assessment

Renewal Requirements:
3 years

Course Outcomes:
Participants will be able to:
- Demonstrate specialist ethical hacking skills
- Understand and locate network weaknesses

Job Profile applicability:
- Cybercrime Investigator
- Cyber Forensics
- CERT Operative
- SIEM Operator
- Firewall Administrator
- Forensic Analyst
- Intrusion Detection Specialist
- System Administrator
- Systems Engineer
- Security Administrator
- Security Engineer
- Penetration Tester
- Software Developer (Security)

Course Link: Crest CRT Course

CRISC- Certified Risk & Information Systems Control

Sponsors/Provider:
ISACA

Proficiency Level:
Intermediate/Advanced Level

Cost: $2,100 AUD + GST for CRISC training
Exam fee: ISACA member: $575 USD, non-member: $760 USD

Delivery Method: Face-to-face training or ad hoc self-study from textbooks
Duration: 3 days training course

Course Description:
CRISC prepares and enables IT professionals for the challenges of IT and enterprise risk management and positions them to become strategic partners to the enterprise.

Prerequisites:
Three (3) years of work experience managing IT risk by designing and implementing IS controls, including experience across at least two (2) CRISC domains, of which one must be in Domain 1 or 2, is required for certification

Assessment:
Exam module: Multiple choice exam
Time: 4 hours
Question: 150 questions

Renewal Requirements:
3 years

Course Outcomes:
Participants will be able to undertake:
- IT Risk Identification
- IT Risk Assessment
- Risk Response and Mitigation
- Risk and Control Monitoring and Reporting

Job Profile applicability:
- Cyber Outreach/Cyber Awareness Instructor
- Cyber Law/Cyber Policy Adviser
- Compliance Manager
- Information Security Officer
- Disaster Recovery Manager
- Cyber Risk Manager
- Auditor
- ICT/IT Manager
- Security Architect
- Security Consultant
- Cybercrime Investigator
- Security Analyst
- Cyber Intelligence Analyst
- CERT Operative
- SIEM Operator
- Firewall Administrator
- Forensic Analyst
- Intrusion Detection Specialist
- System Administrator
- Systems Engineer
- Security Administrator
- Security Engineer

Course Link: CRISC Course

GSLC - GIAC Security Leadership Certification

Sponsors/Provider:
GIAC

Proficiency Level:
Advanced Level

Cost:
Exam fee: $1,699 USD for certification attempt

Delivery Method: Exams are delivered face -to- face
Duration: 120 days allowed for online on-demand/ad hoc self-study from textbooks for exam preparation

Course Description:
Equips security professionals with necessary skills for managerial or supervisory responsibility for information security staff.

Prerequisites:
Some IT risk management and information systems control experience

Assessment: Invigilated exam
Exam module: Multiple choice
Time: 3 hours
Question: 115
Pass: 68%

Renewal Requirements:
4 years

Course Outcomes:
Participants will be able to undertake:
- Change Management
- Attacks vectors
- Access Control
- Defence in Depth/Security Policy
- Disaster Recovery Planning
- Managing Employees
- Operational Security
- Physical Security
- Privacy and Web Security
- Risk and Ethics
- Security Awareness
- Network Infrastructure

Job Profile applicability:
- Cyber Outreach/Cyber Awareness Instructor
- Cyber Law/Cyber Policy Adviser
- Compliance Manager
- Information Security Officer
- Disaster Recovery Manager
- Cyber Risk Manager
- Auditor
- ICT/IT Manager
- Security Architect
- Security Consultant
- Cybercrime Investigator
- Security Analyst
- Cyber Intelligence Analyst
- CERT Operative
- SIEM Operator
- Firewall Administrator
- Forensic Analyst
- Intrusion Detection Specialist
- System Administrator
- Systems Engineer
- Security Administrator
- Security Engineer

Course Link: GSLC Course

GNFA - GIAC Network Forensic Analyst

Sponsors/Provider:
GIAC

Proficiency Level:
Advanced Level

Cost:
Exam fee: $1,699 USD for certification attempt

Delivery Method: Exams are delivered face -to- face
Duration: 120 days allowed for online on-demand/ad hoc self-study from textbooks for exam preparation

Course Description:
System attacks are becoming increasingly broad and complex. It is simply unfeasible to conduct full host-based forensic analysis on every system in an organization of any size. The proper use of network forensics can enable examiners to determine the origin and impact of malicious events quickly and effectively. The GNFA certification is for professionals who want to demonstrate that they qualified to perform examinations employing network forensic artefact analysis. Candidates are required to demonstrate an understanding of the fundamentals of network forensics, normal and abnormal conditions for common network protocols, the process and tools used to examine device and system logs, wireless communication and encrypted protocols.

Prerequisites:
Experience in a related field desirable

Assessment: Invigilated exam
Exam module: Multiple choice
Time: 2 hours
Question: 50
Pass: 70%

Renewal Requirements:
4 years

Course Outcomes:
Participants will be able to undertake:
- Common Network Protocols
- Encryption and Encoding
- Net-flow Analysis and Attack Visualization
- Network Analysis Tool and Usage
- Network Architecture
- Network Protocol Reverse Engineering
- Open Source Network Security Proxies
- Security Event and Incident Logging
- Wireless Network Analysis

Job Profile applicability:
- Cyber Law/Cyber Policy Adviser
- Cybercrime Investigator
- Cyber Forensics
- Forensic Analyst

Course Link: GNFA Course

GSNA – GIAC Systems and Network Auditor

Sponsors/Provider:
GIAC

Proficiency Level:
Advanced Level

Cost:
Exam fee: $1,699 USD for certification attempt

Delivery Method: Exams are delivered face -to- face
Duration: 120 days allowed for online on-demand/ad hoc self-study from textbooks for exam preparation

Course Description:
GIAC Systems and Network Auditor. GSNAs have the knowledge, skills and abilities to apply basic risk analysis techniques and to conduct a technical audit of essential information systems. Technical staff responsible for securing and auditing information systems; auditors who wish to demonstrate technical knowledge of the systems they are responsible for auditing.

Prerequisites:
Some IT risk management and information systems control experience

Assessment: Invigilated exam
Exam module: Multiple choice
Time: 3 hours
Question: 115
Pass: 73%

Renewal Requirements:
4 years

Course Outcomes:
Participants will be able to undertake:
- Auditing Concepts & Methodology
- Auditing Networking Devices & Services
- Auditing Unix Systems
- Auditing Windows Systems
- Web Application Security

Job Profile applicability:
- Cyber Outreach/Cyber Awareness Instructor
- Compliance Manager
- Information Security Officer
- Auditor
- Security Consultant
- Cybercrime Investigator
- Security Analyst
- SIEM Operator
- Systems Administrator
- Systems Engineer
- Security Administrator
- Security Engineer

Course Link: GSNA Course

IRAP – Information Security Registered Assessors Program

Sponsors/Provider:
Australian Federal Government/Australian Signals Directorate (ASD)

Proficiency Level:
Advanced

Cost: $2,200 AUD for course training and examination

Delivery Method: Face-to-face training
Duration: 2 days training

Course Description:
The Information Security Registered Assessors Program (IRAP) is a program of activities sponsored by the Australian Signals Directorate (ASD) culminating in the endorsement and registration of individuals as competent to assess information security systems in accordance with Australian Government information security standards and policy documents.

Prerequisites:

- 5 years of ICT experience; with
- 2 years of information security experience.
- This must include experience with applying the Australian Government Information Security Manual (ISM) and supporting publications on government systems.

Plus, one of these qualifications:

- CISM
- CISSP
- GSLC
- CISA
- CRISC
- GSNA
- 27001-LA
- PCI-QSA

Assessment: Invigilated exam
Exam module: Multiple choice and short answers
Time: 2 hours
Pass: 80%

Renewal Requirements:
Annually

Course Outcomes:
Candidates qualifying as IRAP registered assessors are endorsed to carry out the following types of assessment work:

- Gateway certifications
- Network/system assessments
- Gatekeeper assessments
- FedLink audits, and
- FedLink connection assessments

Job Profile applicability:

- Cyber Outreach/Cyber Awareness Instructor
- Compliance Manager
- Information Security Officer
- Auditor
- ICT/IT Manager
- Security Consultant
- Cybercrime Investigator
- Security Analyst
- Cyber Intelligence Analyst
- Systems Administrator
- Systems Engineer
- Security Administrator
- Security Engineer

Course Link: IRAP Course

ISO/IEC 27001 Lead Auditor

Sponsors/Provider:
ISO (through PWC)

Proficiency Level:
Entry level

Cost: $2,995 AUD for training and assessment

Delivery Method: face-to-face
Duration: 5 days training and an exam the final day

Course Description:
ISO/IEC 27001 Lead Auditor or Information Security Management Systems Lead Auditor. Outlines the key processes and approaches a business needs to manage information security risk in a practical way. Teaches how to implement and audit an information security management system adhering to the specific requirements of ISO/IEC 27001, in order to protect information assets such as customer details, sensitive corporate information and financial data.

Prerequisites:
None specified

Assessment: Continual assessment. During the course, participants will complete a series of workshops, which form part of the assessment. Upon the completion of each module there is a short multiple-choice exam. Participants receive continual assistance and feedback from the facilitator.

Renewal Requirements:
Not required

Course Outcomes:
Participants will gain the knowledge to conduct internal or external audits of an Information Security Management System, either as a sole auditor, a member of an audit team, or as the team leader:

- Learn how to plan and carry out an ISO 27001:2013 audit
- Learn report writing and how to document an InfoSec system
- Recognise the role of the auditor
- Understand, and be able to implement processes within the InfoSec system
- Improve an organisations conformance with ISO/IEC 27001:2013
- Learn how to identify gaps in an InfoSec management system
- Satisfy training needs for Exemplar Global certification

Job Profile applicability:

- Cyber Outreach/Cyber Awareness Instructor
- Compliance Manager
- Information Security Officer
- Disaster Recovery Manager
- Auditor
- ICT/IT Manager
- Security Architect
- Security Consultant
- Cybercrime Investigator
- Security Analyst
- CERT Operative
- SIEM Operator
- Firewall Administrator
- Intrusion Detection Specialist
- Systems Administrator
- Systems Engineer
- Security Administrator
- Security Engineer

Course Link: ISO/IEC 27001-LA Course

ISO/IEC 27001 Lead Implementer

Sponsors/Provider:	**Proficiency Level:**
ISO (through PWC)	Entry level

Cost: $2,995 AUD for training and assessment

Delivery Method: face-to-face
Duration: 5 days training and an exam the final day

Course Description:
Participants learn how to perform an audit in accordance with ISO 19011:2011 Guidelines for Auditing Management Systems. The course provides a comprehensive and practical understanding of how to conduct a successful internal or external audit, either as part of an audit team or as the team leader. Focus is on the principles and procedures of auditing, the importance of planning, the roles and responsibilities of an auditor, how to gather effective audit evidence and report on the audit findings, and the required follow up activities as an auditor. Participants also learn the auditing requirements of ISO 27001, and how to best apply and integrate the standard for the benefit of an organisation.

Prerequisites:
None specified

Assessment: Continual assessment. During the course, participants will complete a series of workshops, which form part of the assessment. Upon the completion of each module there is a short multiple-choice exam. Participants receive continual assistance and feedback from the facilitator.

Renewal Requirements:
Not required

Course Outcomes:
Participants will gain the knowledge to conduct internal or external audits of an InfoSec Management System, either as a sole auditor, a member of an audit team, or as the team leader. Specifically, you will:

- Learn how to plan and carry out an ISO 27001:2013 audit
- Learn report writing and how to document an InfoSec system
- Recognise the role of the auditor
- Understand, and implement processes within the InfoSec system
- Improve an organisations conformance with ISO/IEC 27001:2013
- Learn how to identify gaps in an InfoSec system
- Satisfy training needs for Exemplar Global certification
- The course includes a complimentary copy of ISO/IEC 27001:2013, along with all learning materials.

Job Profile applicability:

- Cyber Outreach/Cyber Awareness Instructor
- Compliance Manager
- Information Security Officer
- Disaster Recovery Manager
- Auditor
- ICT/IT Manager
- Security Architect
- Security Consultant
- Cybercrime Investigator
- Security Analyst
- CERT Operative
- SIEM Operator
- Firewall Administrator
- Intrusion Detection Specialist
- Systems Administrator
- Systems Engineer
- Security Administrator
- Security Engineer

Course Link: ISO/IEC 27001-LI Course

OSCE - Offensive Security Certified Expert

Sponsors/Provider:
Offensive Security

Proficiency Level:
Advanced

Cost: Depends on the number of months 'Lab Time' is purchased. Approximately CTP Course Materials + 60 days of Lab Access + OSCE Certification Exam Attempt = $1500 USD

Delivery Method: Online

Duration: The average time to go through the PWK and CTP course materials and exercises is approximately 100 hours. This estimate only reflects the time required to complete the course exercises and does not include the time required to attack the various lab systems

Course Description:
This certification is designated to students who take and successfully pass the Cracking the Perimeter (CTP) exam. This is a hands-on ethical hacking course designed by and for professional penetration testers.

Prerequisites:
Industry experience required (no further details)

Assessment: The OSCE examination consists of a remotely-hosted virtual network containing varying configurations and operating systems. The successful candidate will demonstrate their ability to research the network (information gathering), identify any vulnerabilities, and execute their attacks with the goal of compromising the systems to gain administrative access. The examinee is expected to submit a comprehensive penetration test report, containing in-depth notes and screen shots detailing their findings. Points are awarded for each compromised host, based on their difficulty and level of access obtained.

Renewal Requirements:
3 years

Course Outcomes:
An OSCE is able to identify hard-to-find vulnerabilities and misconfigurations in various operating systems and execute organized attacks in a controlled and focused manner. The intense forty-eight-hour examination also demonstrates that OSCE's have an above average degree of persistence and determination. Perhaps most importantly, an OSCE has demonstrated their ability to think laterally and perform effectively under pressure.

Job Profile applicability:

- Cybercrime Investigator
- Cyber Forensics
- CERT Operative
- SIEM Operator
- Firewall Administrator
- Forensic Analyst
- Intrusion Detection Specialist
- Systems Administrator
- Systems Engineer
- Security Administrator
- Security Engineer
- Penetration Tester
- Software Developer

Course Link: OSCE Course

OSCP - Offensive Security Certified Professional

Sponsors/Provider:
Offensive Security

Proficiency Level:
Entry level

Cost: Depends on the number of months 'Lab Time' is purchased. Approximately PWK Course Materials + 90 days of Lab Access + OSCP Certification Exam Attempt = $1150 USD

Delivery Method: Online

Duration: The average time to go through the PWK and CTP course materials and exercises is approximately 100 hours. This estimate only reflects the time required to complete the course exercises and does not include the time required to attack the various lab systems

Course Description:
An OSCP has an ability to be presented with an unknown network, enumerate the targets within their scope, exploit them, and clearly document their results in a penetration test report.

Prerequisites:
Entry level, industry related interest an advantage

Assessment: The OSCP examination consists of a virtual network containing targets of varying configurations and operating systems. At the start of the exam, the student receives the exam and connectivity instructions for an isolated exam network that they have no prior knowledge or exposure to. The successful examinee will demonstrate their ability to research the network (information gathering), identify any vulnerabilities and successfully execute attacks. This often includes modifying exploit code with the goal to compromise the systems and gain administrative access. The candidate is expected to submit a comprehensive penetration test report, containing in-depth notes and screenshots detailing their findings. Points are awarded for each compromised host, based on their difficulty and level of access obtained.

Renewal Requirements:
Renewal not required

Course Outcomes:
An OSCP, by definition, is able to identify existing vulnerabilities and execute organized attacks in a controlled and focused manner, write simple Bash or Python scripts, modify existing exploit code to their advantage, perform network pivoting and data ex-filtration, and compromise poorly written PHP web applications.

Job Profile applicability:

- ICT/IT Manager
- Cybercrime Investigator
- Cyber Forensics
- CERT Operative
- SIEM Operator
- Firewall Administrator
- Forensic Analyst
- Intrusion Detection Specialist
- Systems Administrator
- Systems Engineer
- Security Administrator
- Security Engineer
- Penetration Tester
- Software Developer

Course Link: OSCP Course

PCI-QSA – Payment Card Industry – Qualified Security Assessor

Sponsors/Provider:
Payment Card Industry Security Standards Council

Proficiency Level:
Entry level

Cost: $2,750 USD + GST for instructor led classes

Delivery Method: Face-to-face
Duration: 2 days

Course Description:
Against disparate levels of PCI auditing and reporting requirements, this course focuses on the twelve high-level control objectives, and corresponding sub-requirements that need to be met either directly or through a set of compensating controls.

- PCI-DSS testing procedures
- Payment brand specific requirements
- PCI validation requirements
- PCI reporting requirements
- Real world case studies

Prerequisites:
Candidates resume must be approved to access online prerequisite course. Upon successful completion of online fundamental course and exam candidates seat for face-to-face training is confirmed.

For undertaking PCI assessment candidates must have a minimum of one year of experience in EACH of the following security disciplines:

- Application security
- Information systems security
- Network security
- IT security auditing
- Information security risk assessment or risk management

Candidates must have one or more professional certification
Acceptable certifications include:

- Certified Information System Security Professional (CISSP)
- Certified Information Security Manager (CISM)
- Certified Information Systems Auditor (CISA)
- GIAC Systems and Network Auditor (GSNA)
- Certified ISO 27001, Lead Auditor, Internal Auditor
- International Register of Certificated Auditors (IRCA)
- Information Security Management System (ISMS) Auditor
- Certified Internal Auditor (CIA)

Assessment:
Exam module: Online exam: 50 multiple choice questions
Invigilated exam:75 Multiple choice questions
Time: 90 minutes for invigilated exam

Renewal Requirements:
1-year renewal and re-qualification with a minimum of 20 Continuing Professional Education (CPE) hours per year and 120 CPE hours over a rolling three-year period.

Course Outcomes:

Job Profile applicability:

The primary goal of the QSA credential is to provide the ability to perform an assessment against the high-level control objectives of the PCI Data Security Standard (PCI DSS).	• Cyber Outreach/Cyber Awareness Instructor • Compliance Manager • Information Security Officer • Cyber Risk Manager • Compliance Manager • Security Consultant • ICT/IT Manager • Security Architect • Security Consultant • Cybercrime Investigator • Security Analyst • Systems Administrator • Systems Engineer • Security Administrator • Security Engineer
Course Link: PCI-QSA Course	

Security+

Sponsors/Provider:
Computing Technology Industry Association (Comp-TIA)

Proficiency Level:
Entry level

Cost: Full-time: $2,799 AUD, Part-time: $2,599 AUD
Exam cost: $321 AUD

Delivery Method: Online, Face-to-face and blended

Duration:
Full-time: 5 days,
Part-time: 4 weeks

Course Description:
In this course, students will implement, monitor, and troubleshoot infrastructure, application, information, and operational cyber security:

Module 1: Security Fundamentals
Module 2: Identifying Security Threats and Vulnerabilities
Module 3: Managing Data, Application, and Host Security
Module 4: Implementing Network Security
Module 5: Implementing Access Control, Authentication, and Account Management
Module 6: Managing Certificates
Module 7: Implementing Compliance and Operational Security
Module 8: Risk Management
Module 9: Troubleshooting and Managing Security Incidents
Module 10: Business Continuity and Disaster Recovery Planning

Prerequisites:
Basic Computer Knowledge

Assessment:
Exam module: Multiple choice
Time: 90 minutes
Question: 90
Pass: 750 (on a scale of 100 – 900)

Renewal Requirements:
3 years

Course Outcomes:
Knowledge of:

- Network security
- Compliance and operational security
- Threats and vulnerabilities
- Application, data and host security
- Access control and identity management
- Cryptography

Job Profile applicability:

- Cyber Outreach/Cyber Awareness Instructor
- Cyber Law/Cyber Policy Adviser
- Compliance Manager
- Information Security Officer
- Disaster Recovery Manager
- Cyber Risk Manager
- Auditor
- ICT/IT Manager
- Security Architect
- Security Consultant
- Cybercrime Investigator
- Security Analyst
- Cyber Intelligence Analyst
- Cryptographer/Cryptanalyst
- Cyber Forensics

- CERT Operative
- SIEM Operator
- Firewall Administrator
- Forensic Analyst
- Intrusion Detection Specialist
- System Administrator
- Systems Engineer
- Security Administrator
- Security Engineer

Course Link: Security+ Course

SSCP - Systems Security Certified Practitioner

Sponsors/Provider:
International Information System Security Certification Consortium (ISC)[2]

Proficiency Level:
Entry/Intermediate

Cost: Approximately $3,000 AUD for training
Exam Cost: $250 USD

Delivery Method & Duration:
5 days

Course Description:
Provides industry-leading confirmation of a practitioner's ability to implement, monitor and administer IT infrastructure in accordance with information security policies and procedures that ensure the confidentiality, integrity and availability of data. Augments a technical ability to tackle the operational demands and responsibilities of the security practitioner, including authentication, security testing, intrusion detection/prevention, incident response and recovery, attacks and countermeasures, cryptography, malicious code countermeasures, and more.

Prerequisites:
Minimum 1 year of cumulative industry related experience

Assessment: Invigilated exam, multiple choice answers
Time: 3 hours
No. of Questions: 125
Pass: 70%

Renewal Requirements:
3 years renewal and earn a minimum of 20 CPE credits per year. Annual maintenance fee of $ 65 USD must be paid before certification annual anniversary date.

Course Outcomes:
Participants will obtain a working knowledge of:

- Access Controls
- Security Operations and Administration
- Risk Identification, Monitoring, and Analysis
- Incident Response and Recovery
- Cryptography
- Network and Communications Security
- Systems and Application Security

Job Profile applicability:

- Cyber Outreach/Cyber Awareness Instructor
- Information Security Officer
- Cyber Risk Manager
- ICT/IT Manager
- Security Architect
- Security Consultant
- Cybercrime Investigator
- Security Analyst
- Cyber Forensics
- CERT Operative
- SIEM Operator
- Firewall Administrator
- Forensic Analyst
- Intrusion Detection Specialist
- System Administrator
- Systems Engineer
- Security Administrator
- Security Engineer
- Penetration Tester
- Software Developer (Security)

Course Link: SSCP Course

Cyber Security Programs - TAFE Course

Certificate IV in Cyber Security

Sponsors/Provider:
VIC TAFE – Box Hill Campus

Proficiency Level:
Entry

Cost: Full fee: $9,196 AUD per annum
Government subsidised standard fee: $3,330 AUD
Government subsidised concession fee: $660 AUD

Delivery Method & Duration:
1 year full-time, also available as a flexible part-time course.

Course Description:
The Certificate IV Cyber Security is specifically designed to develop skills and knowledge for a career as a Cyber Security para-professional. The role of the para-professional is to detect and determine cyber breaches to networks or system security, then escalate incidents discovered to the security response team. A Cyber Security para-professional works with a range of stakeholders, both internal and external, that need to be aware of cyber threats or vulnerabilities.

Prerequisites:
Successfully completed Year 12 or equivalent or be a mature age applicant

Assessment: No detail provided

Renewal Requirements:
N/A

Course Outcomes:
Course provides basic knowledge skills and the ability to:

- Penetration testing
- Identifying and reporting website and system vulnerabilities
- System Testing
- Securing Workstations/PCs in a workplace environment
- Evaluating and reporting cyber security incidents
- Networking concepts and protocols
- Setting up and managing network security
- Security script programming
- Website Security
- Problem researching
- Working with a team to develop cyber policies and procedures to meet workplace and legislative requirements

Job Profile applicability:

- Cyber Outreach/Cyber Awareness Instructor
- Security Architect
- Security Consultant
- Cybercrime Investigator
- Security Analyst
- Cyber Intelligence Analyst
- Cyber Forensics
- CERT Operative
- SIEM Operator
- Firewall Administrator
- Forensic Analyst
- Intrusion Detection Specialist
- System Administrator
- Systems Engineer
- Security Administrator
- Security Engineer
- Penetration Tester
- Software Developer (Security)

Course Link: Cert IV Cyber Security

Advanced Diploma of Computer Systems Technology (Specialising in Cyber Security)

Sponsors/Provider:
VIC TAFE – Box Hill Campus

Proficiency Level:
Entry

Cost: Full fee: $18,332 AUD per annum
Government subsidised standard fee: $10,467 AUD

Delivery Method & Duration:
1 year full-time, also available as an 18 months part-time course.

Course Description:
This course has been specifically developed by an industry panel of leaders in the Australian Cyber Security sector, it is designed to provide the skills and knowledge needed to work in this area of ICT security. The Advanced Diploma of Computer Systems Technology (Specialising in Cyber Security) prepares graduates for a career as a Cyber Security professional with comprehensive range of technical and non-technical cyber security skills.

Prerequisites:
Applicants must have successfully completed Year 12 or equivalent and have completed a Certificate IV or Diploma in Information Technology with specialisation in cyber security. Mature age applicants that have worked in the Cyber Security industry are required to attend an interview to establish that they have the necessary cyber security skills and knowledge to undertake Advanced Diploma level learning.

Assessment: No detail provided

Renewal Requirements: N/A

Course Outcomes:
Course provides proficiency in the ability to:

- monitor the risks of cyber security attacks
- prepare and implement appropriate risk management plans
- prepare and implement appropriate mitigation solutions
- use a range of tools and procedures to identify and block cyber security threats
- protect an organisation from insider security breaches
- develop and implement risk mitigation solutions for cloud systems
- implement privacy and compliance policies in accordance with Australian Cyber Law

Job Profile applicability:

- Cyber Outreach/Cyber Awareness Instructor
- Compliance Manager
- Information Security Officer
- Disaster Recovery Manager
- Cyber Risk Manager
- Auditor
- ICT/IT Manager
- Security Architect
- Security Consultant
- Cybercrime Investigator
- Security Analyst
- Cyber Intelligence Analyst
- Cyber Forensics
- CERT Operative
- SIEM Operator
- Firewall Administrator
- Forensic Analyst
- Intrusion Detection Specialist
- System Administrator
- Systems Engineer
- Security Administrator
- Security Engineer
- Penetration Tester
- Software Developer

Course Link: A. Dip. Comp. Sys. Tech. (CyberSec)

Advanced Diploma of Network Security

Sponsors/Provider:
NSW TAFE
Campus': Albury, Nirimba, Wagga Wagga

Proficiency Level:
Entry

Cost: $3,430 to $3,860 AUD depending on previous qualification

Delivery Method & Duration:
20 hours per week over a period of 2 years

Course Description:
Prepares students for a career as a network security specialist developing a comprehensive understanding of critical network security issues, and their importance in the business, industrial and social environments of intranet, extranet and Internet connectivity. Security compliance is emphasised throughout the course, and students learn to carry out network security activities in accordance with local and international industry standards. Upon successful completion of the diploma graduates will have the knowledge and skills to work as a Network Security Specialist.

Prerequisites:
None

Assessment: No detail provided

Renewal Requirements:
N/A

Course Outcomes:
This qualification provides the skills and knowledge for an individual to plan, design, manage and monitor an enterprise information and communications technology (ICT) network as an independent ICT specialist or as part of a team responsible for advanced ICT network security systems. The qualification has a high-level ICT technical base with appropriate security units and the ability to specialise in a number of areas, including voice, wireless, network infrastructure and sustainability**.**

Job Profile applicability (entry level):

- Cyber Outreach/Cyber Awareness Instructor
- Security Architect
- Security Consultant
- Cybercrime Investigator
- Security Analyst
- Cyber Intelligence Analyst
- Cyber Forensics
- CERT Operative
- SIEM Operator
- Firewall Administrator
- Forensic Analyst
- Intrusion Detection Specialist
- System Administrator
- Systems Engineer
- Security Administrator
- Security Engineer
- Penetration Tester
- Software Developer

Course Link: A.Dip. NetSec

Advanced Diploma of Network Security

Sponsors/Provider:
QLD TAFE: Gold Coast, Coomera Campus

Proficiency Level:
Entry

Cost: $9,690 AUD

Delivery Method & Duration:
16 hours per week over 12 months

Course Description:
Prepares students for a career as a network security specialist developing a comprehensive understanding of critical network security issues, and their importance in the business, industrial and social environments of intranet, extranet and Internet connectivity. Security compliance is emphasised throughout the course, and students learn to carry out network security activities in accordance with local and international industry standards. Upon successful completion of the diploma graduates will have the knowledge and skills to work as a Network Security Specialist.

Prerequisites:
Students must have completed a Diploma of Information Technology Networking, Diploma of Software Development or possess extensive demonstrable work experience. All applicants (direct entry or applying through QTAC) must provide a copy of their Year 12 certificate. Applicants that are not able to produce a copy of this document are required to complete the Basic Key Skills Builder (BKSB) test before enrolment. Mature aged students who are unable to provide a copy of their Year 12 certificate must submit a detailed work history or resume prior to enrolment and complete the Basic Key Skills Builder (BKSB) test.

Assessment: No detail provided

Renewal Requirements:
N/A

Course Outcomes:
This qualification provides the skills and knowledge for an individual to plan, design, manage and monitor an enterprise information and communications technology (ICT) network as an independent ICT specialist or as part of a team responsible for advanced ICT network security systems. The qualification has a high-level ICT technical base with appropriate security units and the ability to specialise in a number of areas, including voice, wireless, network infrastructure and sustainability**.**

Job Profile applicability (entry level):

- Cyber Outreach/Cyber Awareness Instructor
- Compliance Manager
- Information Security Officer
- Disaster Recovery Manager
- Cyber Risk Manager
- Auditor
- ICT/IT Manager
- Security Architect
- Security Consultant
- Cybercrime Investigator
- Security Analyst
- Cyber Intelligence Analyst
- Cyber Forensics
- CERT Operative
- SIEM Operator
- Firewall Administrator
- Forensic Analyst
- Intrusion Detection Specialist
- System Administrator
- Systems Engineer
- Security Administrator
- Security Engineer
- Penetration Tester
- Software Developer

Course Link: A.Dip. NetSec

Certificate IV in Information Technology (Specialising in Cyber Security) Traineeship

Sponsors/Provider:
VIC TAFE – Box Hill Campus

Proficiency Level:
Entry

Cost: Full fee: $9,266 AUD per annum
Government subsidised standard fee: $3,263 AUD
Government subsidised concession fee: $653 AUD

Delivery Method & Duration:
12 to 24 months depending on the employer

Course Description:
Help employers employ a trainee to undertake general IT and Cyber Security tasks within their organisation. Prepares students to work within the organisation to support detection and determination of breaches in network and system security, to escalate incidents to a security response team, and to complete general IT duties. Students get the opportunity to work with a range of stakeholders (either internal or external to the organisation) that need to be aware of a threat or vulnerability.

Prerequisites:
Students must be registered with an Australian Apprenticeship Centre and have a training contract with an employer. Students do not require prior IT experience for the traineeship. Prior to enrolment the Institute and CAE will assess all students' language, literacy and numeracy and digital literacy by conducting a self-assessment review to ensure suitability of the course for the student.

Assessment: No detail provided

Renewal Requirements:
N/A

Course Outcomes:
This qualification provides the skills and knowledge for an individual to communicate and work with teams at work place. The qualification ensures students get practical knowledge of networking, system testing, programming security scripts, website and network security and managing system security. Students get the opportunity to work on cyber security industry based projects

Job Profile applicability (entry level):

- Cyber Outreach/Cyber Awareness Instructor
- Security Architect
- Security Consultant
- Cybercrime Investigator
- Security Analyst
- Cyber Intelligence Analyst
- Cyber Forensics
- CERT Operative
- SIEM Operator
- Firewall Administrator
- Forensic Analyst
- Intrusion Detection Specialist
- System Administrator
- Systems Engineer
- Security Administrator
- Security Engineer
- Penetration Tester
- Software Developer (Security)

Course Link: Cert IV IT(Cyber Sec)

Cyber Security Programs - Graduate Courses

Graduate Diploma of Cyber Security, Edith Cowan University

Sponsors/Provider:
Edith Cowan University – Joondalup Campus

Proficiency Level:
Entry/Intermediate

Cost: $20,000 AUD, (see Online fees calculator) depending upon student needs

Delivery Method & Duration:
1 year full-time, 2 years part-time
Full-time and part-time course available online

Course Description:
Designed to meet the demand for cyber security professionals in government, law enforcement, and industry. The course engages with, and provides a pathway for, information technology professionals seeking to commence or further progress their careers in the cyber security domain. It is also relevant to those seeking to enter the IT profession who have no previous experience in the cyber discipline.

Prerequisites:
Bachelor's Degree, bachelor's with Honours, or equivalent.

Assessment: Depending on course subject assessment components are test reports, exercise and examinations

Renewal Requirements:
N/A

Course Outcomes:
Course provides in-depth knowledge of:

- Applied Communications
- Computer Security
- Network Security Fundamentals
- Wireless Security
- Programming Principles
- Introductory Computer Forensics
- Information Security
- Ethical Hacking and Defence
- Cyber Security Management.

Job Profile applicability:

- Cyber Outreach/Cyber Awareness Instructor
- Compliance Manager
- Information Security Officer
- Disaster Recovery Manager
- Cyber Risk Manager
- Auditor
- ICT/IT Manager
- Security Architect
- Security Consultant
- Cybercrime Investigator
- Security Analyst
- Cyber Intelligence Analyst
- Cyber Forensics
- CERT Operative
- SIEM Operator
- Firewall Administrator
- Forensic Analyst
- Intrusion Detection Specialist
- System Administrator
- Systems Engineer
- Security Administrator
- Security Engineer

Course Link: Graduate Diploma of Cyber Security

Graduate Diploma of Cyber Security, Deakin University

Sponsors/Provider:
Deakin University – Fully Online

Proficiency Level:
Entry/Intermediate

Cost: $3,285 AUD per unit/credit point for both online and campus courses

Delivery Method & Duration:
1 year full-time, 2 years part-time
Full-time and part-time course available online

Course Description:
In an increasingly digital world, cyber-attacks are an everyday occurrence. Expert cyber security professionals who can protect organisations from these threats are in high demand and this course can prepare you for a successful career anywhere in the world. Throughout the Graduate Diploma of Cyber Security, you'll learn how to confront cyber security - one of the 21st Century's most critical issues. Focusing on a range of studies, you'll gain knowledge from system security and digital forensics to analytics and organisational security. This course gives you the cyber security skills that are crucial to the success of our digital future. And, once you graduate, you'll have the knowledge and talent to take on an expert security role within business, government or law enforcement.

Prerequisites:
Bachelor's degree in the same discipline (including information technology or computing) or, a Graduate Certificate of Information Technology or equivalent.

Assessment: Depending on course subject selection, components are; test reports, technical reports, multiple-choice test and end semester exams

Renewal Requirements:
N/A

Course Outcomes:
Course provides in-depth knowledge across four of the following disciplines:

- Discipline-specific knowledge and capabilities: appropriate to the level of study related to a discipline or profession. Develop specialised and essential knowledge of security needs, design and development, systems, processes, concepts and technologies to develop software systems, products and solutions that automates business processes at par with industry standards and based on cyber security needs.
- Communication: using oral, written and interpersonal communication to inform, motivate and effect change. Communicate IT solutions as appropriate to the context to inform, motivate and effect change utilising a range of verbal, graphical and written methods, recognising the needs of diverse audiences.
- Digital literacy: using technologies to find, use and disseminate information. Use digital media to locate, collect and

Job Profile applicability:

- Cyber Outreach/Cyber Awareness Instructor
- Compliance Manager
- Information Security Officer
- Disaster Recovery Manager
- Cyber Risk Manager
- Auditor
- ICT/IT Manager
- Security Architect
- Security Consultant
- Cybercrime Investigator
- Security Analyst
- Cyber Intelligence Analyst
- Cyber Forensics
- CERT Operative
- SIEM Operator
- Firewall Administrator
- Forensic Analyst
- Intrusion Detection Specialist
- System Administrator
- Systems Engineer
- Security Administrator
- Security Engineer

evaluate information from technical channels and apply information to identify approaches and solutions that meet user requirements.

- Critical thinking: evaluating information using critical and analytical thinking and judgment. Use the frameworks of logical and analytical thinking to evaluate specialist IT information, technical problems and user requirements, and develop approaches to identify solutions.
- Problem solving: creating solutions to authentic (real world and ill-defined) problems. Develop IT solutions for automating processes by investigating technical and business problems; design and propose alternative solutions that improve services and user experiences.
- Self-management: working and learning independently and taking responsibility for personal actions. Demonstrate the ability to work in a professional manner, learn autonomously and responsibly in order to identify and meet development needs.
- Global citizenship: engaging ethically and productively in the professional context and with diverse communities and cultures in a global context. Engage in professional and ethical behaviour in the design of IT systems, in a global context, in collaboration with diverse communities and cultures.

Course Link: Graduate Diploma of Cyber Security

Graduate Diploma of Cyber Security, Curtin University

Sponsors/Provider:
Curtin University –On-campus

Proficiency Level:
Entry/Intermediate

Cost: $26,700 AUD per annum

Delivery Method & Duration:
1 year full-time, 2 years part-time
Full-time and part-time course

Course Description:
This course can help you fast-track your career in cyber security. It is designed for computer professionals who have an interest in finding and fixing vulnerabilities, encryption, intrusion detection and managing cyber risks and network security.
Depending on your choice of units, you may study evidence collection, counterintelligence, internet crime, business continuity, network security policies, network firewalls, authentication and web server security.
This course is for graduates with a computing background. It provides a detailed coverage of the key concepts and challenges in data and resource protection and computer software security, with a focus on both high-level concepts and low-level practical aspects of information security.

Prerequisites:
Bachelor's degree in computer science, information technology or software engineering along with English language proficiency.

Assessment: Depending on course subject selection, components are; test reports, technical reports, multiple-choice test and end semester exams

Renewal Requirements:
N/A

Course Outcomes:
This course equips graduates with the ability to Course provides in-depth knowledge across four of the following disciplines:

- assess the theoretical concepts involved in data encryption and intrusion detection and deploy them in a modern day Information Technology system
- evaluate the various approaches to encryption and security detection and develop a strategy for adapting them to a specific situation
- evaluate and synthesise information from a variety of sources and develop a plan to optimize computer security, data encryption and intrusion management
- assess computer security management processes and explain them in written and oral form to both technical and non-technical audiences
- evaluate and select appropriately from existing and emerging encryption, computer security prevention and intrusion technologies

Job Profile applicability:

- Cyber Outreach/Cyber Awareness Instructor
- Compliance Manager
- Information Security Officer
- Disaster Recovery Manager
- Cyber Risk Manager
- Auditor
- ICT/IT Manager
- Security Architect
- Security Consultant
- Cybercrime Investigator
- Security Analyst
- Cyber Intelligence Analyst
- Cyber Forensics
- CERT Operative
- SIEM Operator
- Firewall Administrator
- Forensic Analyst
- Intrusion Detection Specialist
- System Administrator
- Systems Engineer
- Security Administrator
- Security Engineer

- engage in continual updating of knowledge with regard to new and emerging computer security concepts, issues and management strategies
- evaluate and interpret The Institute of Electrical and Electronics Engineers, The Association for Computing Machinery and the Australian Computer Society standards related to data encryption, computer security protection and management
- understand the ethical issues related to protecting the rights of individuals from diverse cultures and how that maps to ensuring the security and integrity of data in an Information Technology system
- develop policies and practical procedures to improve the security setup of an Information Technology organization

Course Link: Graduate Diploma of Cyber Security

Graduate Diploma of Cyber-Security, Policing, Intelligence and Counter Terrorism, Macquarie University

Sponsors/Provider:
Macquarie University

Proficiency Level:
Entry/Intermediate

Cost: Approximately $25,462 AUD per annual

Delivery Method & Duration:
0.5 to 1 years full-time or equivalent part-time

Course Description:
Graduate Diploma of Cyber-Security, Policing, Intelligence and Counter Terrorism program are designed to equip students with the ability to respond to major security, policing and defence issues both locally and internationally. Students will gain knowledge and understanding in contemporary cyber-security, policing, intelligence, terrorism and security studies. The program engages with all aspects of contemporary and applied security studies, drawing from both academic experts and world class practitioners with significant practical experience. Students have the choice of gaining a specialization in either cyber-security, policing, intelligence or terrorism studies.

Prerequisites:
Bachelor degree or its equivalent in addition to English language(IELTS) score of 6.5 or above

Assessment: Assignments, practical assessments or examinations

Renewal Requirements:
N/A

Course Outcomes:
Depending on the stream of choice course provides proficiency in the ability to:

- identify contemporary and emerging security threats in the domains of cyber, policing, intelligence and terrorism, whilst applying critical thinking skills in conceptualising risk and threat assessment
- explore a range of research principles and methodologies that are utilised to underpin independent research within the field of International Security Studies
- analyse a significant and contemporary body of literature related to key concepts that underpin the domains of cyber, policing, intelligence and terrorism studies and which identify key theoretical and thematic concepts, as well as traditional and emerging security threats
- communicate acquired knowledge and skills effectively to a range of professional audiences
- present informed, considered and logical judgements supporting and contradicting the arguments of others, in a professional manner, and within a relevant contextual framework

Job Profile applicability:

- Cyber Outreach/Cyber Awareness Instructor
- Cyber Law/Cyber Policy Adviser
- Compliance Manager
- Information Security Officer
- Disaster Recovery Manager
- Cyber Risk Manager
- Auditor
- ICT/IT Manager
- Security Architect
- Security Consultant
- Cybercrime Investigator
- Security Analyst
- Cyber Intelligence Analyst
- Cyber Forensics
- CERT Operative
- SIEM Operator
- Firewall Administrator
- Forensic Analyst
- Intrusion Detection Specialist
- System Administrator
- Systems Engineer
- Security Administrator
- Security Engineer

applicable to graduate employment opportunities
- critically evaluate government reports, professional documents, academic scholarship and literature pertinent to professional practice and relevant to graduate employment opportunities in a variety of related fields
- display advanced research skills, specifically the ability to select and integrate knowledge from a diverse range of relevant sources; critically evaluate significance and relevance; and synthesise findings in a coherent, rational and sustained academic argument
- synthesise theoretical, thematic and practical positions in relation to the domains of cyber, policing, intelligence and terrorism studies which evidence sustained engagement throughout the duration of the degree and permit graduates to present positions on contemporary security scholarship and practice necessary for employment in directly related fields
- apply ethical principles that manifest a global outlook built on interdisciplinary and international engagement

Course Link: Grad.dipCPICT (CyberSec), Macquarie

Graduate Certificate of Cyber Security, Edith Cowan University

Sponsors/Provider:
Edith Cowan University – Joondalup Campus

Proficiency Level:
Entry/Intermediate

Cost: Approximately $9,500 AUD, (see Online fees calculator) depending upon student needs

Delivery Method & Duration:
6 months full-time, 1 year part-time

Course Description:
Designed to meet the demand for cyber security professionals in government, law enforcement, and industry. The course engages with, and provides a pathway for, information technology professionals seeking to commence or further progress their careers in the cyber security domain. It is also relevant to those seeking to enter the IT profession who have no previous experience in the cyber discipline. The course provides flexibility in terms of unit choice for those wishing to further their knowledge in a particular discipline of cyber security.

Prerequisites:
Bachelor Degree, Bachelor's with Honours, or equivalent.

Assessment: Depending on course subject assessment components are test reports, exercise and examinations

Renewal Requirements:
N/A

Course Outcomes:
Course provides in-depth knowledge across four of the following disciplines:

- Applied Communications
- Computer Security
- Network Security Fundamentals
- Wireless Security
- Programming Principles
- Introductory Computer Forensics
- Information Security
- Ethical Hacking and Defence

Job Profile applicability:

- Cyber Outreach/Cyber Awareness Instructor
- Compliance Manager
- Information Security Officer
- Disaster Recovery Manager
- Cyber Risk Manager
- Auditor
- ICT/IT Manager
- Security Architect
- Security Consultant
- Cybercrime Investigator
- Security Analyst
- Cyber Intelligence Analyst
- Cyber Forensics
- CERT Operative
- SIEM Operator
- Firewall Administrator
- Forensic Analyst
- Intrusion Detection Specialist
- System Administrator
- Systems Engineer
- Security Administrator
- Security Engineer

Course Link: Graduate Certificate of Cyber Security

Graduate Certificate of Cyber Security, Deakin University

Sponsors/Provider:	**Proficiency Level:**
Deakin University	Entry/Intermediate

Cost: $Online fee: $3,285 per unit/credit point
Campus fee: $3,949 per unit/credit point

Delivery Method & Duration:
6 months full-time, 1 year part-time on campus
Full-time and part-time course available online

Course Description:
Throughout the Graduate Certificate of Cyber Security, you'll learn how to confront cyber security - one of the 21st Century's most critical issues. Focusing on a range of studies, you'll gain knowledge from system security and digital forensics to analytics and organisational security. This course gives you the cyber security skills that are crucial to the success of our digital future. And, once you graduate, you'll have the knowledge and talent to take on an expert security role within business, government or law enforcement.

Prerequisites:
Bachelor's degree in the same discipline (including information technology or computing)

Assessment: Depending on course subject assessment components are reports, multiple-choice test, group case investigation reports and end semester exams

Renewal Requirements:
N/A

Course Outcomes:
Course provides in-depth knowledge across four of the following disciplines:

- Discipline-specific knowledge and capabilities: appropriate to the level of study related to a discipline or profession. Develop specialised and essential knowledge of security needs, design and development, systems, processes, concepts and technologies to develop software systems, products and solutions that automates business processes at par with industry standards and based on cyber security needs.
- Communication: using oral, written and interpersonal communication to inform, motivate and effect change. Communicate IT solutions as appropriate to the context to inform, motivate and effect change utilising a range of verbal, graphical and written methods, recognising the needs of diverse audiences.
- Digital literacy: using technologies to find, use and disseminate information. Use digital media to locate, collect and evaluate information from technical channels and apply information to

Job Profile applicability:

- Cyber Outreach/Cyber Awareness Instructor
- Compliance Manager
- Information Security Officer
- Disaster Recovery Manager
- Cyber Risk Manager
- Auditor
- ICT/IT Manager
- Security Architect
- Security Consultant
- Cybercrime Investigator
- Security Analyst
- Cyber Intelligence Analyst
- Cyber Forensics
- CERT Operative
- SIEM Operator
- Firewall Administrator
- Forensic Analyst
- Intrusion Detection Specialist
- System Administrator
- Systems Engineer
- Security Administrator
- Security Engineer

identify approaches and solutions that meet user requirements.

- Critical thinking: evaluating information using critical and analytical thinking and judgment. Use the frameworks of logical and analytical thinking to evaluate specialist IT information, technical problems and user requirements, and develop approaches to identify solutions.
- Problem solving: creating solutions to authentic (real world and ill-defined) problems. Develop IT solutions for automating processes by investigating technical and business problems; design and propose alternative solutions that improve services and user experiences.
- Self-management: working and learning independently and taking responsibility for personal actions. Demonstrate the ability to work in a professional manner, learn autonomously and responsibly in order to identify and meet development needs.

Course Link: Graduate Certificate of Cyber Security

Graduate Certificate in Cyber Security, Charles Sturt University

Sponsors/Provider:
Charles Sturt University

Proficiency Level:
Entry/Intermediate

Cost: $3,250 per unit/credit point
Full fee: $13,000 per year

Delivery Method & Duration:
6 months full-time, 1 year part-time on campus
Full-time and part-time course available online

Course Description:
With a strong technical focus, this course includes contemporary topics in cyber security such as digital forensics, dark web, cloud security, cyberwarfare and terrorism and hacking countermeasures. The Graduate Certificate of Cyber Security builds a foundation in cybersecurity and skills with critical focus on encryption technologies, how to maintain cloud security and become adept across digital forensic tactics.

Prerequisites:
Bachelor's degree in the same discipline (including information technology or computing) or professional attainment and/or work experience

Assessment: Depending on course subject assessment components are reports, multiple-choice test, group case investigation reports and end semester exams

Renewal Requirements:
N/A

Course Outcomes:
Course provides in-depth knowledge across four of the following disciplines:

- Investigate and analyse key evidence to address and reduce crimes associated with cyber security
- Maintain cyber security management systems while building mobility and accessibility through secure cloud-based technology for your organisation. Use emerging technologies and information to enhance network security and secure the operations of business
- Work as a pivotal team member in countering cyber warfare and terrorism.
- Develop skills across hacking countermeasures, incident response and forensic investigation will support broader national and international efforts to improve community safety

Job Profile applicability:

- Cyber Outreach/Cyber Awareness Instructor
- Compliance Manager
- Information Security Officer
- Disaster Recovery Manager
- Cyber Risk Manager
- Auditor
- ICT/IT Manager
- Security Architect
- Security Consultant
- Cybercrime Investigator
- Security Analyst
- Cyber Intelligence Analyst
- Cyber Forensics
- CERT Operative
- SIEM Operator
- Firewall Administrator
- Forensic Analyst
- Intrusion Detection Specialist
- System Administrator
- Systems Engineer
- Security Administrator
- Security Engineer

Course Link: Graduate Certificate of Cyber Security

Graduate Certificate in Cyber Security, Victoria University

Sponsors/Provider:
Victoria University

Proficiency Level:
Entry/Intermediate

Cost: $3,850 per unit (Cost of the course depends upon students' dependence on Commonwealth support Online Calculator)

Delivery Method & Duration:
6 months full-time, or equivalent part-time
Course available on-campus and blended

Course Description:
This course content covers the essential areas of cyber security, from proactive cyber threat detection, risk management to cyber law and regulations. Course concentrates on cyber security fundamentals, architecture, technologies such as digital signature, public key infrastructure, virtual private networks, firewalls, intrusion detection, data encryption, cloud security, and cyber security regulations, policies and laws.

Prerequisites:
Bachelor's degree or Advanced diploma in the same discipline (including information technology or computing) or minimum four years of work experience in related discipline

Assessment: Depending on course subject assessment components are reports, multiple-choice test, group case investigation reports and end semester exams

Renewal Requirements:
N/A

Course Outcomes:
Upon completion of course, student will be able to:

- Critically apply cyber security knowledge and skills to new and uncertain situations in professional practice, exhibiting a high level of personal autonomy and accountability
- Evaluate cyber security architecture and state-of-the-art technologies including firewalls, virtual private networks, public key infrastructure, digital signature and anti-malwares
- Apply commercial tools to secure computers and networks in enterprise and cloud systems to ensure privacy and prevent data loss
- Develop organisational strategies relating to cyber security law, policies and regulations to solve legal challenges of the cyber world

Job Profile applicability:

- Cyber Outreach/Cyber Awareness Instructor
- Compliance Manager
- Information Security Officer
- Disaster Recovery Manager
- Cyber Risk Manager
- Auditor
- ICT/IT Manager
- Security Architect
- Security Consultant
- Cybercrime Investigator
- Security Analyst
- Cyber Intelligence Analyst
- Cyber Forensics
- CERT Operative
- SIEM Operator
- Firewall Administrator
- Forensic Analyst
- Intrusion Detection Specialist
- System Administrator
- Systems Engineer
- Security Administrator
- Security Engineer

Course Link: Graduate Certificate of Cyber Security

Cyber Security Programs - Bachelor Degrees

Bachelor of Cyber Security and Behaviour, Western Sydney University

Sponsors/Provider:
Western Sydney University – Parramatta Campus

Proficiency Level:
Entry

Cost: Approximately $20,000 AUD

Delivery Method & Duration:
3 years full-time, 6 years part-time

Course Description:
This course meets the pressing need for the application of psychological theory and research to understand cyber security issues in the context of decision-making, human errors, social influence, organisational cultures and vulnerable populations. As cyber threats become more sophisticated and damaging across all types of organisations, cyber security has become one of the nation's top priorities. Students will gain a solid grounding in conventional computer and network security concepts and skills.

Prerequisites:
HSC, ATAR 75

Assessment: Depending on course subject assessment components are assignments, presentations and end semester exams

Renewal Requirements:
N/A

Course Outcomes:
This course meets the growing need for the application of psychological theory and research to understand cyber security issues in the context of decision-making, human errors, social influence, organisational cultures and vulnerable populations. As cyber threats become more sophisticated and damaging across all types of organisations, cyber security is a top priority. You will gain a solid grounding in conventional computer and network security concepts and skills, leading to a range of rewarding career options. Examples of career opportunities include cyber safety officer, data security, security analyst, risk analytics, cyber policing, cyber intelligence, intelligence analytics and terror-informatics.

Job Profile applicability:

- Cyber Outreach/Cyber Awareness Instructor
- Compliance Manager
- Information Security Officer
- Disaster Recovery Manager
- Cyber Risk Manager
- Auditor
- ICT/IT Manager
- Security Architect
- Security Consultant
- Cybercrime Investigator
- Security Analyst
- Cyber Intelligence Analyst
- Cyber Forensics
- CERT Operative

Course Link: BCyberSecBehav

Bachelor of Science with a major in Cyber Security, Macquarie University

Sponsors/Provider:
Macquarie University – North Ryde Campus

Proficiency Level:
Entry

Cost: $10,754 per annum

Delivery Method & Duration:
3 years full-time, 6 years part-time

Course Description:
Bachelor of Science with a Cyber Security major provides graduates with the knowledge needed to create an effective cyber security environment for commercial, private and industrial applications. It combines units from the Department of Computing with those from Security Studies and Criminology to give students practical insights into technology risks and countermeasures and the role that security management plays in the bigger picture of cyber governance.

Prerequisites:
HSC, ATAR 75

Assessment: No detail provided

Renewal Requirements:
N/A

Course Outcomes:
The course provides a foundation in mathematics and computer programming, networking and systems administration bolstered by in-depth knowledge of cyber security, cybercrime and law as well as an introduction to information warfare and cyber terrorism.

Job Profile applicability:

- Cyber Outreach/Cyber Awareness Instructor
- Compliance Manager
- Information Security Officer
- Disaster Recovery Manager
- Cyber Risk Manager
- Auditor
- ICT/IT Manager
- Security Architect
- Security Consultant
- Cybercrime Investigator
- Security Analyst
- Cyber Intelligence Analyst
- Cyber Forensics
- CERT Operative
- SIEM Operator
- Firewall Administrator
- Forensic Analyst
- Intrusion Detection Specialist
- System Administrator
- Systems Engineer
- Security Administrator
- Security Engineer

Course Link: BSc (CyberSec)

Bachelor of Information Technology with a major in Cyber Security, Macquarie University

Sponsors/Provider:
Macquarie University – North Ryde Campus

Proficiency Level:
Entry

Cost: $9,185 per annum

Delivery Method & Duration:
3 years full-time, 6 years part-time

Course Description:
Bachelor of Information Technology with a Cyber Security major provides graduates with the knowledge needed to create an effective cyber security environment for commercial, private and industrial applications. It combines units from the Department of Computing with those from security studies to give students practical insights into technology risks and countermeasures and the role that security management plays in the bigger picture of cyber governance.

Prerequisites:
HSC, ATAR 75

Assessment: No detail provided

Renewal Requirements:
N/A

Course Outcomes:
The course provides a foundation in IT, computer programming, computer networks and data base design, and management augmented with cyber security, cybercrime and web technologies as well as an introduction to cryptography and Information Security.

Job Profile applicability:

- Cyber Outreach/Cyber Awareness Instructor
- Compliance Manager
- Information Security Officer
- Disaster Recovery Manager
- Cyber Risk Manager
- Auditor
- ICT/IT Manager
- Security Architect
- Security Consultant
- Cybercrime Investigator
- Security Analyst
- Cyber Intelligence Analyst
- Cyber Forensics
- CERT Operative
- SIEM Operator
- Firewall Administrator
- Forensic Analyst
- Intrusion Detection Specialist
- System Administrator
- Systems Engineer
- Security Administrator
- Security Engineer

Course Link: BSS (CyberSec)

Bachelor of Cyber Security, Deakin University

Sponsors/Provider:
Deakin University – Victoria

Proficiency Level:
Entry

Cost: $9,010 AUD per year

Delivery Method & Duration:
3 years full-time, equivalent part-time

Course Description:
Bachelor of Cyber Security provides a solid foundation of the cyber security literacy and technical skills required by industry for a cyber security professional including those allowing you to be able to investigate and combat cyber-crime and cyber terrorism.
The degree focuses on technical elements and sets you up with strong skills in critical thinking and problem solving.

Prerequisites:
Admission will be based on Victorian Certificate of Education (VCE), its equivalent or Certificate IV or diploma in related discipline

Assessment: No detail provided

Renewal Requirements:
N/A

Course Outcomes:
Graduates will be able to develop and apply their skills with IT discipline in the following areas:

- Discipline-specific knowledge and capabilities
- Communication
- Digital literacy
- Critical thinking
- Problem solving
- Teamwork

Job Profile applicability:

- Cyber Outreach/Cyber Awareness Instructor
- Compliance Manager
- Information Security Officer
- Disaster Recovery Manager
- Cyber Risk Manager
- Auditor
- ICT/IT Manager
- Security Architect
- Security Consultant
- Cybercrime Investigator
- Security Analyst
- Cyber Intelligence Analyst
- Cyber Forensics
- CERT Operative
- SIEM Operator
- Firewall Administrator
- Forensic Analyst
- Intrusion Detection Specialist
- System Administrator
- Systems Engineer
- Security Administrator
- Security Engineer

Course Link: BSc/BA (CyberSec)

Bachelor of Cyber Security, La Tobe University

Sponsors/Provider:	**Proficiency Level:**
La Trobe University – Victoria	Entry

Cost: Approximately $4,000 AUD per unit (Online fee calculator is available for verification)

Delivery Method & Duration:
3 years full-time, equivalent part-time

Course Description:
La Trobe's Bachelor of Cybersecurity is a brand new degree that addresses the global shortage of cybersecurity professionals and prepares students with skills across IT, business, law, policy and strategic communication. The course covers history of hacking and explore the various methods used to defend and protect against malicious cyber-threats. As cybersecurity is as much about people the course will cover sophisticated techniques that cyber-criminals use to manipulate individuals to access confidential information online.

Prerequisites:
Admission will be based on Minimum ATAR 60 and Victorian Certificate of Education (VCE)

Assessment: No detail provided

Renewal Requirements:

Course Outcomes:
Students will graduate with knowledge, skills, and experience that could apply to a range of roles in the evolving area of cybersecurity including national security, IT, Risk Management, Forensics, Cyber intelligence, banking and finance, telecommunications, health care and law.

Job Profile applicability:

- Cyber Outreach/Cyber Awareness Instructor
- Compliance Manager
- Information Security Officer
- Disaster Recovery Manager
- Cyber Risk Manager
- Auditor
- ICT/IT Manager
- Security Architect
- Security Consultant
- Cybercrime Investigator
- Security Analyst
- Cyber Intelligence Analyst
- Cyber Forensics
- CERT Operative
- SIEM Operator
- Firewall Administrator
- Forensic Analyst
- Intrusion Detection Specialist
- System Administrator
- Systems Engineer
- Security Administrator
- Security Engineer

Course Link: BSc/BA (CyberSec)

Bachelor of Cyber Security, Swinburne University

Sponsors/Provider:
Swinburne University – Melbourne

Proficiency Level:
Entry

Cost: $9,185 AUD per annum
Approximate course fee: $AUD 45,925

Delivery Method & Duration:
3-5 years full-time, 6-8 years part-time

Course Description:
Cyber security is essential for the political, social and economic global health. The degree provides a fundamental overview of encryption systems, access control protocols, Internet vulnerabilities and insight into malware, hacking and cybercrime.
Swinburne offers a number of undergraduate degrees with a cyber security major:

- Computer Science
- Engineering
- Law
- Research
- Information Technology

Prerequisites:
HSC, ATAR 75

Assessment: No detail provided

Renewal Requirements:
N/A

Course Outcomes:
Overall learning bias is dependent on the degree course selected. All cyber security majors include units on cybercrime, IT security, forensics, network security as well as information systems risk and security.

Job Profile applicability:

- Cyber Outreach/Cyber Awareness Instructor
- Compliance Manager
- Information Security Officer
- Disaster Recovery Manager
- Cyber Risk Manager
- Auditor
- ICT/IT Manager
- Security Architect
- Security Consultant
- Cybercrime Investigator
- Security Analyst
- Cyber Intelligence Analyst
- Cyber Forensics
- CERT Operative
- SIEM Operator
- Firewall Administrator
- Forensic Analyst
- Intrusion Detection Specialist
- System Administrator
- Systems Engineer
- Security Administrator
- Security Engineer

Course Link: BSc/BA (CyberSec)

BSc. Cyber Security and Forensics, Murdoch

Sponsors/Provider:
Murdoch University, WA

Proficiency Level:
Entry

Cost: Approximately $34,000 AUD

Delivery Method & Duration:
3 years full-time, 6 years part-time

Course Description:
In this course, students will learn how to identify, mitigate and prevent cyber security threats and respond to security incidents for government agencies and corporate organisations. Students will also develop strong analytical and critical thinking skills and learn how to forensically examine digital evidence to solve computer crimes. As part of studies, complete practical experience and have the opportunity to engage with industry and the community on current issues.
To expand students' expertise even further possibility to combine Cyber Forensics and Information Security with another major, such as Computer Science, Business Information Systems or Internetworking and Network Security is available. This course is accredited at the Professional level with the Australian Computer Society (ACS). When you graduate, you could pursue a career as an information security officer, cyber forensic investigator, forensic auditor, computer security officer, IT consultant, systems administrator or even work as an ethical hacker.

Prerequisites:
HSC, ATAR 70

Assessment: No detail provided

Renewal Requirements:
N/A

Course Outcomes:
Graduates will be able to identify and counteract malicious activity conducted by hackers using advanced analytic capabilities and techniques.

Demonstrable knowledge of:

- Cyber risk mitigation strategies
- Network security
- Ethical hacking
- System and network security
- Cryptography
- Application security

Job Profile applicability:

- Security Consultant
- Auditor
- Security Architect
- Cyber Outreach/Cyber Awareness Instructor
- Information Security Officer
- Security Analyst
- Security Administrator
- Security Engineer
- Penetration Tester
- Software Developer

Course Link: BIT (CyberSec)

Bachelor of Information Technology (Networking and Cyber Security), University of South Australia

Sponsors/Provider:
University of South Australia – Adelaide, Technology Park Campus

Proficiency Level:
Entry

Cost: Approximately $32,000 AUD per annum (Online fee calculator and scholarship eligibility is available)

Delivery Method & Duration:
3 years full-time, 6 years part-time
Full-time and part-time course available online

Course Description:
The security of information and systems has become a very important aspect in contemporary IT. In this specialisation, you will be exposed to the techniques and theory that support network infrastructures in small to large businesses.

In 2015, 97 per cent of our Uni SA's research had been assessed at a world-class standard or above by the Excellence in Research for Australia ratings which included the fields of artificial intelligence and image processing, disrupted computing and information systems.

Students will acquire the skills to support a network roll-out and the maintenance of infrastructure, while gaining an understanding of networking topologies and networking devices such as routers and firewalls. In particular, the networking courses prepare you for industry certification examinations in CISCO, CCNA and CCNP where you will be in a position to not only graduate with a degree, but with this highly regarded industry certification, which will increase your employment prospects.

Prerequisites:
HSC, ATAR 70

Assessment: Depending on course subject assessment components are reports, essays, assignments, industry-relevant project, practicals and examinations

Renewal Requirements:
N/A

Course Outcomes:
Knowledge of the core concepts in information technology. Focus is on networking and security in areas such as network design, network implementation, intrusion detection, and security auditing.

Graduates are skilled in network support and roll-out, infrastructure maintenance with an understanding of networking topologies and networking devices such as routers and firewalls. In particular, the networking courses prepare students for industry certification examinations in CISCO, CCNA and CCNP. This degree has a hands-on approach where students gain experience at Uni SA's dedicated security and networking labs and engage in an industry-based project in their final year.

Job Profile applicability:

- Cyber Outreach/Cyber Awareness Instructor
- Compliance Manager
- Information Security Officer
- Disaster Recovery Manager
- Cyber Risk Manager
- Auditor
- ICT/IT Manager
- Security Architect
- Security Consultant
- Cybercrime Investigator
- Security Analyst
- Cyber Intelligence Analyst
- Cyber Forensics
- CERT Operative
- SIEM Operator
- Firewall Administrator
- Forensic Analyst

- Intrusion Detection Specialist
- System Administrator
- Systems Engineer
- Security Administrator
- Security Engineer

Course Link: BIT (CyberSec)

Bachelor of Computer Science (Cyber Security), University of Wollongong

Sponsors/Provider:
University of Wollongong – Wollongong Campus

Proficiency Level:
Entry

Cost: Approximately $32,000 AUD per annum (Online fee structure and support)

Delivery Method & Duration:
3 years full-time, 6 years part-time

Course Description:

Computer science focus on the theoretical foundations and practical approaches to computation and its applications. They design methods and tools and write programs for computer applications. These applications can be in areas such as computer systems to control machinery, information management and big data, applications for mobile devices, stock market trend analysis, game design, visualisation of chemical reactions, neural network design, computational geometry for robot navigation, patient monitoring in hospitals, and much more.

Students are able to choose a cyber security major from their second year after studying the core common of subjects that link the computer science, IT and information systems degrees. Students complete a final-year capstone team project. A major in Cyber Security can be combined with Big data, game and mobile development and software engineering.

Prerequisites:
HSC, ATAR 75

Assessment: Depending on course subject assessment components are reports, essays, assignments, industry-relevant project, practicals and examinations

Renewal Requirements:
N/A

Course Outcomes:
Graduates will be able to identify and counteract malicious activity conducted by hackers using advanced analytic capabilities and techniques.

Demonstrable knowledge of:

- Cyber risk mitigation strategies
- Network security
- Ethical hacking
- System and network security
- Cryptography
- Application security

Job Profile applicability:

- Cyber Outreach/Cyber Awareness Instructor
- Compliance Manager
- Information Security Officer
- Disaster Recovery Manager
- Cyber Risk Manager
- Auditor
- ICT/IT Manager
- Security Architect
- Security Consultant
- Cybercrime Investigator
- Security Analyst
- Cyber Intelligence Analyst
- Cyber Forensics
- CERT Operative
- SIEM Operator
- Firewall Administrator
- Forensic Analyst
- Intrusion Detection Specialist
- System Administrator
- Systems Engineer
- Security Administrator

- Security Engineer

Course Link: BIT (CyberSec)

Bachelor of Science (Cyber Security), Edith Cowan University

Sponsors/Provider:
Edith Cowan University

Proficiency Level:
Entry

Cost: Approximately &2,530 to $3,370 AUD per annum (Online fee structure and support)

Delivery Method & Duration:
3 years full-time, 6 years part-time

Course Description:
This course focus on the practical and theoretical dimensions of IT security across a range of fundamental areas, such as network security and vulnerability assessment, information security, digital forensics, wireless device security and database security.

Students will gain a solid grounding in conventional computer and network security concepts and skills. In addition, the course is designed to meet the changing landscape of secure computing, which involves not only computers, but also telecommunications networks and network enabled devices such as smartphones and tablet devices.

Prerequisites:
HSC, ATAR 70

Assessment: Depending on course subject assessment components are reports, essays, assignments, industry-relevant project, practicals and examinations

Renewal Requirements:
N/A

Course Outcomes:
This course prepares students for careers in the field of cyber security, including areas such as network security, computer forensics, information warfare and wireless security.

Job Profile applicability:

- Cyber Outreach/Cyber Awareness Instructor
- Compliance Manager
- Information Security Officer
- Disaster Recovery Manager
- Cyber Risk Manager
- Auditor
- ICT/IT Manager
- Security Architect
- Security Consultant
- Cybercrime Investigator
- Security Analyst
- Cyber Intelligence Analyst
- Cyber Forensics
- CERT Operative
- SIEM Operator
- Firewall Administrator
- Forensic Analyst
- Intrusion Detection Specialist
- System Administrator
- Systems Engineer
- Security Administrator
- Security Engineer

Course Link: BSc.Sc(Cyber Sec)

Cyber Security Master's Course

LLM Cyber Warfare Law– Master of Law with a major in Cyber Warfare

Sponsors/Provider:	**Proficiency Level:**
Australian National University	Intermediate

Cost: $3,252 AUD per unit, (see Online fees calculator) depending upon student needs

Delivery Method & Duration:
26 hours of face to face teaching, with approximately 120 hours of advance preparation

Course Description:
This course provides graduates with the knowledge in general international law, the international law that governs the recourse to armed force and international humanitarian law, all in the specific context of cyber warfare. With six weeks allotted for completion of the course, including 4 day intensive classes it will help students identify and assess the extent to which norms of existing law can properly be applied to the peculiarities of cyber operations.

Prerequisites:
Studying Master of Law, Juris Doctor, Graduate certificate in law or equivalent

Assessment: Class participation, oral presentation at the end of the course and two essays

Renewal Requirements:
N/A

Course Outcomes:
The course provides proficiency in the ability to:

- demonstrate an advanced understanding of various international law rules that apply to cyber warfare
- demonstrate cognitive skills to critically analyse the hypothetical cyber warfare scenarios
- evaluate international law issues arising from the employment of cyber operations
- execute complex legal research with independence

Job Profile applicability:

- Cyber Outreach/Cyber Awareness Instructor
- Cyber Law/Cyber Policy Adviser
- Compliance Manager
- Information Security Officer
- Disaster Recovery Manager
- Cyber Risk Manager
- Auditor
- ICT/IT Manager
- Security Architect
- Security Consultant
- Cybercrime Investigator
- Security Analyst
- Cyber Intelligence Analyst
- Cyber Forensics
- SIEM Operator
- Firewall Administrator
- Forensic Analyst
- Intrusion Detection Specialist
- System Administrator
- Systems Engineer
- Security Administrator
- Security Engineer

Course Link: LLM Cyber Warfare Law, ANU

Master of Cyber Security, Edith Cowan University

Sponsors/Provider:	**Proficiency Level:**
Edith Cowan University	Intermediate

Cost: Approximately $21,100 AUD per annum (Online calculator available to calculate fee)

Delivery Method & Duration:
2 years full-time or 4 years part-time

Course Description:
Master of Cyber Security **introduces** postgraduates to cyber security within **government, law enforcement and industry. With the primary focus of cyber security, this program covers** technical and non-technical skills of security issues and concepts. It combines units from information systems, programming, computer science, network security, ethical hacking defence and project management to enhance a career as a cyber security specialist.

Prerequisites:
Bachelor degree, Bachelor's with Honours, or equivalent

Assessment: Assignments, practical assessments or examinations

Renewal Requirements:
N/A

Course Outcomes:
Depending on the stream of choice course provides proficiency in the ability to:

- Understanding of network security and tools and techniques to deploy a secure network
- Examine security issues with the ability to detect threats and vulnerabilities
- develop knowledge and skills in for offensive and defensive tactical Cyber Operations
- develop project management skills
- automate tasks, extend capabilities of pre-existing software using scripting techniques
- understand and evaluate the vulnerability of Critical Infrastructure
- understanding of commuter forensics, software and tools used identify and analyse computer based evidence

Job Profile applicability:

- Cyber Outreach/Cyber Awareness Instructor
- Cyber Law/Cyber Policy Adviser
- Compliance Manager
- Information Security Officer
- Disaster Recovery Manager
- Cyber Risk Manager
- Auditor
- ICT/IT Manager
- Security Architect
- Security Consultant
- Cybercrime Investigator
- Security Analyst
- Cyber Intelligence Analyst
- Cyber Forensics
- CERT Operative
- SIEM Operator
- Firewall Administrator
- Forensic Analyst
- Intrusion Detection Specialist
- System Administrator
- Systems Engineer
- Security Administrator
- Security Engineer

Course Link: MCyberSec, ECU

Master of Cyber Security, UNSW Canberra

Sponsors/Provider:
University of South Australia

Proficiency Level:
Intermediate

Cost: Approximately $44,640 AUD for 48 units (Online Fees calculator available)

Delivery Method & Duration:
1 year full-time or equivalent part-time

Course Description:
Master of Cyber Security provides postgraduates understanding of the technical skills and expertise relevant to the technical implementation and leadership of the cyber security function. It combines units from information systems, systems engineering, computer science, network security, and defence to enhance a career as a cyber security specialist. A total of 48 Units of Credit must be completed, which includes core and elective courses.

Prerequisites:
Bachelor degree or its equivalent

Assessment: Assignments, practical assessments or examinations

Renewal Requirements:
N/A

Course Outcomes:
Depending on the stream of choice course provides proficiency in the ability to:

- demonstrate understanding of Information Assurance and Security
- develop knowledge and skills in for offensive and defensive tactical Cyber Operations
- understand numerous cyber defence technologies and their effectiveness against modern threats
- understand the relevance of big data, decision analytics, and their use for decision making with an emphasis on security
- understand and evaluate the vulnerability of Critical Infrastructure
- develop and implement effective administrative and technical risk management plans to protect and secure process control systems
- understanding of the technical and policy used in computer and network defence

Job Profile applicability:

- Cyber Outreach/Cyber Awareness Instructor
- Cyber Law/Cyber Policy Adviser
- Compliance Manager
- Information Security Officer
- Disaster Recovery Manager
- Cyber Risk Manager
- Auditor
- ICT/IT Manager
- Security Architect
- Security Consultant
- Cybercrime Investigator
- Security Analyst
- Cyber Intelligence Analyst
- Cyber Forensics
- CERT Operative
- SIEM Operator
- Firewall Administrator
- Forensic Analyst
- Intrusion Detection Specialist
- System Administrator
- Systems Engineer
- Security Administrator
- Security Engineer

Course Link: MCyberSec, UNSW Canberra (ADFA)

Master of Cyber Security, Digital Forensics, UNSW Canberra

Sponsors/Provider:	**Proficiency Level:**
University of NSW, Canberra	Entry/Intermediate/Advanced (while degree content may be Advanced. The proficiency level associated with any particular role would necessarily require some practical experience)

Cost: Approximately $44,640 AUD per annum (Online Fees calculator available)

Delivery Method & Duration:
1 year full-time or equivalent part-time

Course Description:
The Master of Cyber Security is designed for postgraduate scholars who wish to gain a more detailed understanding of the technical skills and expertise relevant to the technical implementation and leadership of the cyber security function. It is designed to meet the demand for technical experts who can implement and lead the technical cyber security function in government, industry, law enforcement and Defence. It provides principles gathered from information systems, systems engineering, computer science, network security, and defence to enhance a career as a cyber security specialist. The Master of Cyber Security is offered primarily via Intensive Delivery Mode due to the nature of the courses and the use of the Cyber Range.
The Master of Cyber Security in Digital Forensics is designed for postgraduate scholars with appropriate undergraduate qualifications in a relevant discipline and/or extensive professional experience who wish to develop a high level understanding of the principles and practices of Digital Forensics and to strengthen their skills in this area.

Prerequisites:
Anyone of the following prerequisites are required

- Bachelor's degree in Engineering or Bachelor's degree with Honours with a major in Information Technology, Information Systems, Science, Computer Science or Engineering
- Graduate Diploma in Information Technology, Information Systems, Science, Computer Science or Engineering
- Completion of a 3 or 4-year Bachelor degree in a cognate discipline which includes a major in Information Technology, Information Systems, Science, Computer Science or Engineering, and have completed at least 3-years full-time professional experience
- Completion of a Bachelor degree in any discipline and have completed at least 4 years full-time professional experience in a cognate discipline
- Evidence of other academic qualifications and professional experience to be submitted to the relevant Program Authority to be acceptable grounds for admission into the degree
- No tertiary qualifications but evidence of professional experience to be submitted to the relevant Program Authority to be acceptable grounds for admission into the degree

Assessment: Assignments, practical assessments or examinations

Renewal Requirements:
N/A

Course Outcomes:
Depending on the stream of choice course provides proficiency in the ability to:

- demonstrate understanding of Information Assurance and Security
- develop knowledge and skills in for offensive and defensive tactical Cyber Operations
- understand numerous cyber defence technologies and their effectiveness against modern threats

Job Profile applicability:

- Cyber Outreach/Cyber Awareness Instructor
- Cyber Law/Cyber Policy Adviser
- Compliance Manager
- Information Security Officer
- Disaster Recovery Manager
- Cyber Risk Manager
- Auditor
- ICT/IT Manager
- Security Architect

- understand the relevance of big data, decision analytics, and their use for decision making with an emphasis on security
- understand and evaluate the vulnerability of Critical Infrastructure
- develop and implement effective administrative and technical risk management plans to protect and secure process control systems
- understanding of the technical and policy used in computer and network defence

- Security Consultant
- Cybercrime Investigator
- Security Analyst
- Cyber Intelligence Analyst
- Cyber Forensics
- CERT Operative
- SIEM Operator
- Firewall Manager
- Forensic Analyst
- Intrusion Detection Specialist
- System Administrator
- Systems Engineer
- Security Administrator
- Security Engineer

Course Link: MCyberSec, (Digital Forensics)

Master of Cyber Security, Strategy and Diplomacy, UNSW Canberra

Sponsors/Provider:	**Proficiency Level:**
University of NSW, Canberra	Entry/Intermediate/Advanced (while degree content may be Advanced. The proficiency level associated with any particular role would necessarily require some practical experience)

Cost: Approximately $44,640 AUD per annum (Online Fees calculator available)

Delivery Method & Duration:
1 year full-time or equivalent part-time

Course Description:
The Master of Cyber Security, Strategy and Diplomacy provides advanced interdisciplinary study into the political, military, diplomatic and higher level management aspects of issues where cyber security, strategy and diplomacy interact. It is intended for students in the diplomatic, defence, justice, public safety, regulatory, management and information sciences. Governments, enterprises, communities and civil society around the world are grappling with strategy and regulation for the new domain of cyberspace, at the same time as their security and other interests are being transformed by the rapid pace of information technology exploitation -- both for beneficial and for malicious purposes. It is widely accepted that the threats in cyber space are escalating while responses to mitigate them are not able to keep up. This program will provide students with the ability to understand the main policy, operational, ethical and informational challenges for security thrown up by the integration or penetration of advanced information technologies into all spheres of human activity.

Prerequisites:
Anyone of the following prerequisites are required

- Bachelor's degree in Engineering or Bachelor's degree with Honours with a major in Information Technology, Information Systems, Science, Computer Science or Engineering
- Graduate Diploma in Information Technology, Information Systems, Science, Computer Science or Engineering
- Completion of a 3 or 4-year Bachelor degree in a cognate discipline which includes a major in Information Technology, Information Systems, Science, Computer Science or Engineering, and have completed at least 3-years full-time professional experience
- Completion of a Bachelor degree in any discipline and have completed at least 4 years full-time professional experience in a cognate discipline
- Evidence of other academic qualifications and professional experience to be submitted to the relevant Program Authority to be acceptable grounds for admission into the degree
- No tertiary qualifications but evidence of professional experience to be submitted to the relevant Program Authority to be acceptable grounds for admission into the degree

Assessment: Assignments, practical assessments or examinations

Renewal Requirements:
N/A

Course Outcomes:
Depending on the stream of choice course provides proficiency in the ability to:

- demonstrate understanding of Information Assurance and Security
- develop knowledge and skills in for offensive and defensive tactical Cyber Operations
- understand numerous cyber defence technologies and their effectiveness against modern threats

Job Profile applicability:

- Cyber Outreach/Cyber Awareness Instructor
- Cyber Law/Cyber Policy Adviser
- Compliance Manager
- Information Security Officer
- Disaster Recovery Manager
- Cyber Risk Manager
- Auditor
- ICT/IT Manager
- Security Architect

- understand the relevance of big data, decision analytics, and their use for decision making with an emphasis on security
- understand and evaluate the vulnerability of Critical Infrastructure
- develop and implement effective administrative and technical risk management plans to protect and secure process control systems
- understanding of the technical and policy used in computer and network defence

- Security Consultant
- Cybercrime Investigator
- Security Analyst
- Cyber Intelligence Analyst
- Cyber Forensics
- CERT Operative
- SIEM Operator
- Firewall Manager
- Forensic Analyst
- Intrusion Detection Specialist
- System Administrator
- Systems Engineer
- Security Administrator
- Security Engineer

Course Link: MCyberSec, (Strategy and Diplomacy)

Master of Cyber Security, Advanced Tradecraft, UNSW Canberra

Sponsors/Provider:	**Proficiency Level:**
University of NSW, Canberra	Entry/Intermediate/Advanced (while degree content may be Advanced. The proficiency level associated with any particular role would necessarily require some practical experience)

Cost: Approximately $44,640 AUD per annum (Online Fees calculator available)

Delivery Method & Duration:
1 year full-time or equivalent part-time

Course Description:
This program will give you the skills needed in an increasingly networked world, where the security of information is essential to the success of organisations. The information security and assurance master degree aim to equip you with the mathematical, technical and business tools to secure an organisation's information systems. Information security and assurance form a vital part of organisational responsibilities. In today's networked world it is more relevant than ever. From the latest internet worm to identity theft, the danger is no more than a mouse click away. You will learn about the Advanced Encryption Standard, RSA, elliptic curve cryptography, smartcards, biometrics and information systems risk management. There are opportunities for internships in the information security industry in the program.

Prerequisites:
Anyone of the following prerequisites are required

- Bachelor's degree in Engineering or Bachelor's degree with Honours with a major in Information Technology, Information Systems, Science, Computer Science or Engineering
- Graduate Diploma in Information Technology, Information Systems, Science, Computer Science or Engineering
- Completion of a 3 or 4-year Bachelor degree in a cognate discipline which includes a major in Information Technology, Information Systems, Science, Computer Science or Engineering, and have completed at least 3-years full-time professional experience
- Completion of a Bachelor degree in any discipline and have completed at least 4 years full-time professional experience in a cognate discipline
- Evidence of other academic qualifications and professional experience to be submitted to the relevant Program Authority to be acceptable grounds for admission into the degree
- No tertiary qualifications but evidence of professional experience to be submitted to the relevant Program Authority to be acceptable grounds for admission into the degree

Assessment: Assignments, practical assessments or examinations

Renewal Requirements:
N/A

Course Outcomes:
Depending on the stream of choice course provides proficiency in the ability to:

- demonstrate understanding of Information Assurance and Security
- develop knowledge and skills in for offensive and defensive tactical Cyber Operations
- understand numerous cyber defence technologies and their effectiveness against modern threats
- understand the relevance of big data, decision analytics, and their use for

Job Profile applicability:

- Cyber Outreach/Cyber Awareness Instructor
- Cyber Law/Cyber Policy Adviser
- Compliance Manager
- Information Security Officer
- Disaster Recovery Manager
- Cyber Risk Manager
- Auditor
- ICT/IT Manager
- Security Architect
- Security Consultant

decision making with an emphasis on security • understand and evaluate the vulnerability of Critical Infrastructure • develop and implement effective administrative and technical risk management plans to protect and secure process control systems • understanding of the technical and policy used in computer and network defence	• Cybercrime Investigator • Security Analyst • Cyber Intelligence Analyst • Cyber Forensics • CERT Operative • SIEM Operator • Firewall Manager • Forensic Analyst • Intrusion Detection Specialist • System Administrator • Systems Engineer • Security Administrator • Security Engineer
Course Link: MCyberSec (Advanced Tradecraft)	

Master of Cyber Security Operations, UNSW Canberra

Sponsors/Provider:
University of NSW, Canberra

Proficiency Level:
Entry/Intermediate/Advanced (while degree content may be Advanced. The proficiency level associated with any particular role would necessarily require some practical experience)

Cost: Approximately $44,640 AUD per annum (Online Fees calculator available)

Delivery Method & Duration:
1 year full-time or equivalent part-time

Course Description:
The Master of Cyber Security Operations is designed for postgraduate scholars and professional managers who wish to gain a more detailed understanding of the managerial and technical skills and expertise relevant to planning, operation and acquisition of the cyber security function. It is designed to meet the demand for executives and managers who oversee the cyber security function in government, industry, law enforcement and Defence. It provides principles gathered from information systems, cyber security, risk, management and governance for managers seeking to enhance their career in cyber security operations

Prerequisites:
Anyone of the following prerequisites are required

- Bachelor's degree in Engineering or Bachelor's degree with Honours with a major in Information Technology, Information Systems, Science, Computer Science or Engineering
- Graduate Diploma in Information Technology, Information Systems, Science, Computer Science or Engineering
- Completion of a 3 or 4-year Bachelor degree in a cognate discipline which includes a major in Information Technology, Information Systems, Science, Computer Science or Engineering, and have completed at least 3-years full-time professional experience
- Completion of a Bachelor degree in any discipline and have completed at least 4 years full-time professional experience in a cognate discipline
- Evidence of other academic qualifications and professional experience to be submitted to the relevant Program Authority to be acceptable grounds for admission into the degree
- No tertiary qualifications but evidence of professional experience to be submitted to the relevant Program Authority to be acceptable grounds for admission into the degree

Assessment: Assignments, practical assessments or examinations

Renewal Requirements: N/A

Course Outcomes:
Depending on the stream of choice course provides proficiency in the ability to:

- demonstrate understanding of Information Assurance and Security
- develop knowledge and skills in for offensive and defensive tactical Cyber Operations
- understand numerous cyber defence technologies and their effectiveness against modern threats
- understand the relevance of big data, decision analytics, and their use for decision making with an emphasis on security
- understand and evaluate the vulnerability of Critical Infrastructure

Job Profile applicability:

- Cyber Outreach/Cyber Awareness Instructor
- Cyber Law/Cyber Policy Adviser
- Compliance Manager
- Information Security Officer
- Disaster Recovery Manager
- Cyber Risk Manager
- Auditor
- ICT/IT Manager
- Security Architect
- Security Consultant
- Cybercrime Investigator
- Security Analyst
- Cyber Intelligence Analyst
- Cyber Forensics

• develop and implement effective administrative and technical risk management plans to protect and secure process control systems • understanding of the technical and policy used in computer and network defence	• CERT Operative • SIEM Operator • Firewall Manager • Forensic Analyst • Intrusion Detection Specialist • System Administrator • Systems Engineer • Security Administrator • Security Engineer
Course Link: MCyberSec, (Operations)	

Master Cyber Security, Macquarie University

Sponsors/Provider:
University of South Australia

Proficiency Level:
Intermediate

Cost: $26,240 per annum

Delivery Method & Duration:
1.5 years full-time or 3 years part-time

Course Description:
Master of Cyber Security focuses on risk, IT, finance, law, governance and policing providing post graduates the opportunity to build skill sets that will enable students to lead more effective responses to security challenges. This course offers three specialisations to choose from: Cyber Security Analysis, Cyber Governance and Management and Internetworking.

Prerequisites:
Depending on **specialisation** admission requirements vary for bachelor degree or its equivalent

Assessment: Assignments, practical assessments or examinations

Renewal Requirements:
N/A

Course Outcomes:
Depending on the stream of choice course specialisation provides proficiency in the ability to:

- develop policy, policing and strategic dimensions for organisations
- examine business and corporate dimensions of cyber security
- develop advanced technology and programming skills

Job Profile applicability:

- Cyber Outreach/Cyber Awareness Instructor
- Cyber Law/Cyber Policy Adviser
- Compliance Manager
- Information Security Officer
- Disaster Recovery Manager
- Cyber Risk Manager
- Auditor
- ICT/IT Manager
- Security Architect
- Security Consultant
- Cybercrime Investigator
- Security Analyst
- Cyber Intelligence Analyst
- Cyber Forensics
- CERT Operative
- SIEM Operator
- Firewall Administrator
- Forensic Analyst
- Intrusion Detection Specialist
- System Administrator
- Systems Engineer
- Security Administrator
- Security Engineer

Course Link: MCyberSec, Macquarie

Master Cyber Security, LA Trobe University

Sponsors/Provider:	**Proficiency Level:**
University of South Australia	Intermediate

Cost: $28,400 for 120 credit points

Delivery Method & Duration:
2 years full-time or part-time equivalent

Course Description:
LA Trobe University offers Master of Cyber Security specialising in the following streams:

- Business Operations
- Computer Science
- Law

These course is structured to focus on information security demands of business, government, defence, law enforcement and law firms**.** A total of 120 credit points of study must be completed for the degree irrespective of the discipline of choice.
The Master of Cyber Security) prepares graduates for a career as a Cyber Security professional with comprehensive range of technical and non-technical forensics skills.

Prerequisites:
Bachelor degree or its equivalent

Assessment: Assignments, practical assessments or examinations

Renewal Requirements:
N/A

Course Outcomes:
Depending on the stream of choice course provides proficiency in the ability to:

- develop business operations skills and techniques covering fundamentals of cybersecurity, core knowledge about communication networks, crisis communication, the mindset and motives of hackers, auditing and risk mitigation, as well as legal and ethical frameworks
- develop skills in cryptography, network security and digital forensics
- understand the relevant multidisciplinary skills by specialising in law
- implement surveillance and privacy policies
- understand about communication networks, crisis communication, the mindset, auditing and risk mitigation
- develop understanding of legal and ethical frameworks
- develop analytical skills to align business needs and deliver meaningful outcomes

Job Profile applicability:

- Cyber Outreach/Cyber Awareness Instructor
- Cyber Law/Cyber Policy Adviser
- Compliance Manager
- Information Security Officer
- Disaster Recovery Manager
- Cyber Risk Manager
- Auditor
- ICT/IT Manager
- Security Architect
- Security Consultant
- Cybercrime Investigator
- Security Analyst
- Cyber Intelligence Analyst
- Cyber Forensics
- CERT Operative
- SIEM Operator
- Firewall Administrator
- Forensic Analyst
- Intrusion Detection Specialist
- System Administrator
- Systems Engineer
- Security Administrator
- Security Engineer

Course Link: MCyberSec, LaTrobe

Master of Cyber Security, RMIT, Melbourne

Sponsors/Provider:	**Proficiency Level:**
RMIT, Melbourne	Intermediate

Cost: Approximately $ 23,040 AUD Annual indicative fee

Delivery Method & Duration:
2 years full-time or 4 years part-time

Course Description:
This program will give you the skills needed in an increasingly networked world, where the security of information is essential to the success of organisations. The information security and assurance master degree aims to equip you with the mathematical, technical and business tools to secure an organisation's information systems. Information security and assurance form a vital part of organisational responsibilities. In today's networked world it is more relevant than ever. From the latest internet worm to identity theft, the danger is no more than a mouse click away. You will learn about the Advanced Encryption Standard, RSA, elliptic curve cryptography, smartcards, biometrics and information systems risk management. There are opportunities for internships in the information security industry in the program.

Prerequisites:
Anyone of the following prerequisites are required

- An Australian bachelor's degree with a minimum GPA of 2.0 out of 4.0 with award title including computer, IT, software, electrical, electronics, communications, mathematics, physics or equivalent
- An Australian bachelor's degree with a GPA between 1.5 and 2.0 out of 4.0 in a scientific/ engineering/technical field with evidence of at least three years' work experience in the field of IT/ information security or equivalent

Assessment: Assignments, practical assessments or examinations

Renewal Requirements:
N/A

Course Outcomes:
Depending on the stream of choice course provides proficiency in the ability to:

- demonstrate understanding of Information Assurance and Security
- develop knowledge and skills in for offensive and defensive tactical Cyber Operations
- understand numerous cyber defence technologies and their effectiveness against modern threats
- understand the relevance of big data, decision analytics, and their use for decision making with an emphasis on security
- understand and evaluate the vulnerability of Critical Infrastructure
- develop and implement effective administrative and technical risk management plans to protect and secure process control systems

Job Profile applicability:

- Cyber Outreach/Cyber Awareness Instructor
- Cyber Law/Cyber Policy Adviser
- Compliance Manager
- Information Security Officer
- Disaster Recovery Manager
- Cyber Risk Manager
- Auditor
- ICT/IT Manager
- Security Architect
- Security Consultant
- Cybercrime Investigator
- Security Analyst
- Cyber Intelligence Analyst
- Cyber Forensics
- CERT Operative
- SIEM Operator
- Firewall Manager
- Forensic Analyst
- Intrusion Detection Specialist
- System Administrator

• understanding of the technical and policy used in computer and network defence	• Systems Engineer • Security Administrator • Security Engineer
Course Link: MCyberSec, RMIT Melbourne	

Master of National Security Policy, ANU

Sponsors/Provider:	**Proficiency Level:**
Australian National University	Intermediate

Cost: $30,096 annual indicative fee for domestic students

Delivery Method & Duration:
2-year full-time course.

Course Description:
This program offers a multi-disciplinary approach to understanding the current and emerging national security challenges facing the word. A total of 96 units of study must be completed for the degree over 2 years.
The Master of National Security Policy develops graduate's skills to implement and evaluate effective policy responses.

Prerequisites:
Bachelor degree or international equivalent with a minimum GPA of 5/7

Assessment: Assignments, practical assessments or examinations

Renewal Requirements:
N/A

Course Outcomes:
Course provides proficiency in the ability to:

- demonstrate a greater understanding of national security issues
- understand research principles and methods applicable to different disciplinary approaches to national security issues
- conduct independent research and understand aspects of professional practice within the field of national security
- apply relevant security frameworks, regulations, standards and legislation to enterprise environment

Job Profile applicability:

- Cyber Outreach/Cyber Awareness Instructor
- Cyber Law/Cyber Policy Adviser
- Compliance Manager
- Information Security Officer
- Disaster Recovery Manager
- Cyber Risk Manager
- Auditor
- ICT/IT Manager
- Security Architect
- Security Consultant
- Cybercrime Investigator
- Security Analyst
- Cyber Intelligence Analyst
- Cyber Forensics

Course Link: Master of National Security Policy, ANU

Master Cyber Security, University of South Australia

Sponsors/Provider:	**Proficiency Level:**
University of South Australia	Intermediate

Cost: Cost of course is provided to candidates upon request from university

Delivery Method & Duration:
2-year full-time course or part time
Full-time and part-time course available online

Course Description:
This course focuses on core studies of Cyber Security, with technical courses that cover cyber security aspects of a complex enterprise architecture and nontechnical the cover aspects of security principles, operations, planning, compliance and consultancy. A total of 72 units of study must be completed for the degree over 2 years.
The Master of Cyber Security prepares graduates for a career as a Cyber Security professional with comprehensive range of technical and non-technical skills to protect critical information.

Prerequisites:
Bachelor Degree in Information Technology or related or equivalent

Assessment: Assignments, practical assessments or examinations

Renewal Requirements:
N/A

Course Outcomes:
Course provides proficiency in the ability to:

- apply networking concepts to critically evaluate network infrastructure alternative
- plan, implement and evaluate of the operational aspects of security
- understand networking concepts to critically evaluate network infrastructure alternatives
- understand features of secure application development and implementation
- understand developing and/or selecting secure web technologies
- understand techniques for selecting appropriate data and services suitable for hosting on public cloud
- design, deploy and defend a secure information technology enterprise architecture
- apply relevant security frameworks, regulations, standards and legislation to enterprise environment
- managing cyber security projects and personnel, including vendors and other external parties
- accordance with Australian Cyber Law

Job Profile applicability:

- Cyber Outreach/Cyber Awareness Instructor
- Cyber Law/Cyber Policy Adviser
- Compliance Manager
- Information Security Officer
- Disaster Recovery Manager
- Cyber Risk Manager
- Auditor
- ICT/IT Manager
- Security Architect
- Security Consultant
- Cybercrime Investigator
- Security Analyst
- Cyber Intelligence Analyst
- Cyber Forensics
- CERT Operative
- SIEM Operator
- Firewall Administrator
- Forensic Analyst
- Intrusion Detection Specialist
- System Administrator
- Systems Engineer
- Security Administrator
- Security Engineer

Course Link: MCyberSec, Uni. SA

Master of Science Cyber Security & Forensics Computing, University of South Australia

Sponsors/Provider:
University of South Australia

Proficiency Level:
Intermediate

Cost: Cost of course is provided to candidates upon request from university

Delivery Method & Duration:
1.5-year full-time course or part-time

Course Description:
This course focuses on core studies of Forensic Computing (Electronic Evidence), Network and Device Forensics, ISO 17025 Forensic Laboratory Accreditation, Information Assurance and Security, Secure Software Development, Critical Infrastructure and Process Control (SCADA) system security, and two final thesis courses (including Research Methods). A total of 54 units of study must be completed for the degree.
The Master of Science (Specialising in Cyber Security) prepares graduates for a career as Cyber Security and forensics professional with comprehensive range of technical and non-technical forensics skills.

Prerequisites:
Undergraduate degree from a recognised University in science, engineering or technology with an average of at least credit (65%) or Graduate Diploma in Science (Cyber Security and Forensic Computing), with an average of at least credit (65%) or equivalent

Assessment: Assignments, practical assessments or examinations

Renewal Requirements:
N/A

Course Outcomes:
Course provides proficiency in the ability to:

- protect the critical information stored on an organisation's computer systems
- understand the strategies, techniques and technologies used in attacking and defending networks
- design secure networks and protect against intrusion, malware and other hacker exploits
- present and present computer driven evidence in courtrooms
- apply security standards like NIST and ISO 17025 lab for validation and verification of evidence
- implement and manage, security throughout the software development lifecycle
- implement privacy and compliance policies in accordance with Australian Cyber Law

Job Profile applicability:

- Cyber Outreach/Cyber Awareness Instructor
- Cyber Law/Cyber Policy Adviser
- Compliance Manager
- Information Security Officer
- Disaster Recovery Manager
- Cyber Risk Manager
- Auditor
- ICT/IT Manager
- Security Architect
- Security Consultant
- Cybercrime Investigator
- Security Analyst
- Cyber Intelligence Analyst
- Cyber Forensics
- CERT Operative
- SIEM Operator
- Firewall Administrator
- Forensic Analyst
- Intrusion Detection Specialist
- System Administrator
- Systems Engineer
- Security Administrator
- Security Engineer

Course Link: MSc Cyber Sec &Forensic. Uni. SA

Cyber Security Roles

Cyber Outreach/Cyber Awareness Instructor

Entry Level

Qualification:
Bachelor/Master degree with a major in:

- Computer Science
- Cyber Security
- Information Technology

TAFE Certifications:

- Certificate II in Security Operations
- Certificate IV in Information Technology (specialising in Cyber Security)
- Graduate Diploma of Cyber Security
- Advanced Diploma of Network Security
- Cyber Security Essentials

Internship/Volunteer Work Experience and capabilities:
Trainer/Instructors roles are generally not offered to candidates with minimum work/internship experience.
At least 5 years of experience in a related field of IT security monitoring and analysis, cyber threat analysis, and vulnerability analysis along with teaching/training experience is required.

Intermediate/Advanced Level

Preferred Combination of Experience:

- Experience implementing multiple awareness and training activities, such as development and implementation of learning and awareness content
- Working knowledge of security standards and baselines
- Expertise regarding the latest security threats, trends, and prevention measures for both individuals and organisations
- Experience developing security solutions in an enterprise environment
- Experience handling and familiarity of business acumen and organizational issues and challenges

Certifications:

- CISA
- CISM
- CISSP
- CRISC
- GSLC
- GSNA
- IRAP
- ISO/IEC 27001 – LA/LI
- PCI-QSA
- Security +
- SSCP

Advantageous skills:

- Experience delivering training in both a traditional classroom setting and virtually
- PowerPoint skills
- Strong communication skills, both oral and written
- Ability to influence others and maintain strong relationships

Recommended Industry Engagement

- Security awareness blogs
- Security Podcasts
- Security conference

Lateral Career Transition

Suitable for:

- System/Network Administrator
- System/Network Engineer
- Systems/Network Analyst
- IT Analyst/Consultant
- Computer Science/ IT professors and teachers

*Note: Professional from various IT/Non-IT roles can transition to this role. The job titles listed are a few relevant examples.

Complimentary Skills:

- Teaching techniques and delivering technical training skills
- Presentation skills
- Technical awareness of common of security concepts

Cyber Law/Cyber Policy Adviser

Entry Level

Qualification:
Bachelor/Master degree with a major in:
- Cyber Security
- Law
- Cyber warfare Law
- Computer Science
- Information Technology

TAFE Certifications:
- Certificate II in Security Operations
- Certificate IV in Information Technology (specialising in Cyber Security)
- Graduate Diploma of Cyber Security
- Advanced Diploma of Network Security

Internship/Volunteer Work Experience and capabilities:
Internship or volunteer experience demonstrating understanding of policies, standards and regulatory requirements

Intermediate/Advanced Level

Preferred Combination of Experience:
- Experience working with Security Standards, frameworks and Compliance requirements such as ISO27XXX, COBIT frameworks, NIST and PCI DSS.
- Expertise and working knowledge of regulatory bodies such as ASD
- Understanding of security concepts related to cyber threats, DNS, routing, authentication, VPN, proxy services, and DDOS mitigation technologies
- Working knowledge of related legislative compliance and Government Acts like Freedom of Information Act 1982, the Privacy Act 1988, and regulatory reforms.
- Experience developing effective policy and planning methodologies, procedures and templates, and providing strategic and insightful policy advice
- Experience working across a range of policy, coordination, and processing work
- Experience working with IT processes, including; operations, security, configuration, change, incident, problem, and disaster recovery management

Certifications:
- CCFP
- CISM
- CISSP
- CRISC
- GSLC
- GSNA
- Security+

Advantageous skills:
- Critical thinking and problem-solving skills
- Strong influence and negotiation skills
- Stakeholder management
- Oral and communication skills
- Reporting skills

Recommended Industry Engagement
- Security communities
- Security podcasts
- Cyber security conferences

- Security blogs

Lateral Career Transition

Suitable for:

- Law practitioner
- System/Network Administrator
- System/Network Engineer
- System/Network Consultant
- IT support Specialists/Manager
- Quality Assurance Analyst
- IT Customer Support Specialists/ Manager

*** Note**: Professional from various IT/Non-IT roles can transition to this role. The job titles listed are a few relevant roles.

Complimentary Skills:

- Knowledge Security Standards, frameworks and Compliance requirements
- Technical understanding of inner-workings of your network, all of the subsequent threats, and how that relates to business risk

Compliance Manager

Entry Level

Qualification:
Bachelor/Master degree with a major in:
- Computer Science
- Cyber Security
- Information Technology

TAFE Certifications:
- Certificate II in Security Operations
- Certificate IV in Information Technology (specialising in Cyber Security)
- Graduate Diploma of Cyber Security
- Advanced Diploma of Network Security
- Cyber Security Essentials

Internship/Volunteer Work Experience and capabilities:
Auditing roles are generally not offered to candidates with minimal work/internship experience.
At least 5 years of experience in related field of IT security monitoring and analysis, cyber threat analysis, and vulnerability analysis is required, with minimum 3-5 years of experience in the field of information security.

Intermediate/Advanced Level

Preferred Combination of Experience:
- Experience working with IT strategy, security principles, enterprise architecture and security architecture
- Working knowledge of IT processes including operations, security, configuration, change, incident, problem, and disaster recovery management
- Experience executing projects with security concepts related to cyber threats, DNS, routing, authentication, VPN, proxy services, and DDOS mitigation technologies
- Experience working with ISO27XXX, COBIT frameworks
- Experience conducting compliance NIST, PCI DSS, IRAP assessments
- Experience conducting cloud risk assessments, third party audits, and gap assessment methodologies
- Experience working with various departments and management teams to manage risk, security compliance, and process effectiveness
- Experience implementing security awareness programs

Certifications:
- CISA
- CISM
- CISSP
- CRISC
- GSLC
- GSNA
- IRAP
- ISO/IEC 27001 – LA/LI
- PCI-QSA
- Security +

Advantageous skills:
- Leadership skills and mentoring experience (particularly mentoring technical staff)
- Efficient multitaskers with organisational skills
- Communication skills, both oral and written
- Interpersonal and relationship-building skills

Recommended Industry Engagement
- Security meetups
- C-level security conferences

- Security podcasts
- Security blogs

Lateral Career Transition

Suitable for:

- IT Consultant
- Network/System Administrator
- Quality Assurance Analyst

***Note:** Professionals from various IT workforces can transition to this role with experience and time in IT. The job titles listed are a few relevant roles.

Complimentary Skills:

- Working knowledge about IT principles, policies, standards and procedures
- Extensive knowledge, experience and technical expertise
- Awareness of updates to regulatory requirements and processes

Information Security Officer

Entry Level

Qualification:

Bachelor/Master degree with a major in:

- Computer Science
- Cyber Security
- Information Technology

TAFE Certifications:

- Certificate II in Security Operations
- Certificate IV in Information Technology (specialising in Cyber Security)
- Graduate Diploma of Cyber Security
- Advanced Diploma of Network Security
- Cyber Security Essentials

Internship/Volunteer Work Experience:

Manager positions are generally not offered to candidates with minimal work/internship experience.

At least 5 years of experience in related field of IT security monitoring and analysis, cyber threat analysis, and vulnerability analysis is required, with minimum 3-5 years of experience in the field of information security.

Intermediate/Advanced Level

Preferred Combination of Experience:

- Knowledge and understanding of IT strategy, security principles, enterprise architecture and security architecture
- Technical knowledge of IT processes including operations, security, configuration, change, incident, problem, and disaster recovery management
- Familiarity and experience in security concepts related to cyber threats, DNS, routing, authentication, VPN, proxy services, and DDOS mitigation technologies
- Experience working with ISO27XXX, COBIT frameworks
- Experience conducting compliance NIST, PCI DSS, IRAP assessments
- Experience working with cloud risk assessments, third party audits, and gap assessment methodologies
- Experience working with various departments and management teams to manage risk, security compliance, and process effectiveness
- Experience implementing security awareness programs

Certifications:

- CISM
- CISSP
- CRISC
- GSLC
- GSNA
- IRAP
- PCI-QSA
- SSCP
- ISO/IEC 27001 – LA/LI
- Security +

Advantageous skills:

- Leadership skills and mentoring experience (particularly mentoring technical staff)
- Efficient multitaskers with organisational skills
- Communication skills, both oral and written
- Interpersonal and relationship-building skills

Recommended Industry Engagement

- Security meetups
- C-level security conferences

- Security podcasts
- Security blogs

Lateral Career Transition

Suitable for:

- Network/System Administrator
- ICT/IT Manager
- Data Quality Manager
- IT Project Coordinator

*__Note:__ Professionals from various IT workforces can transition to this role with experience and time in IT. The job titles listed are a few relevant roles.

Complimentary Skills:

- Working knowledge about IT principles, policies, standards and procedures
- Extensive knowledge, experience, and technical expertise
- Awareness of updates to regulatory requirements and processes

Disaster Recovery Manager

Entry Level

Qualification:
Bachelor/Master degree with a major in:
- Computer Science
- Cyber Security
- Information Technology

TAFE Certifications:
- Certificate II in Security Operations
- Certificate IV in Information Technology (specialising in Cyber Security)
- Graduate Diploma of Cyber Security
- Advanced Diploma of Network Security
- Cyber Security Essentials

Internship/Volunteer Work Experience and capabilities:
Manager positions are generally not offered to candidates with minimal work/internship experience.
At least 5 years of experience in related field of IT security monitoring and analysis, cyber threat analysis, and vulnerability analysis is required, with minimum 3-5 years of experience in the field of information security.

Intermediate/Advanced Level

Preferred Combination of Experience:
- Knowledge and understanding of current disaster recovery planning techniques and technologies
- Experience performing risk analyses and business impact analyses
- Experience planning, organizing, and leading the testing of emergency response, recovery support, and business resumption procedures
- Experience developing, implementing, and enhancing an enterprise-level DR strategy and solutions for critical application disaster recovery
- Understanding of current recovery solutions, high availability architectures and mainframe architectures and knowledge of crisis communication solutions.
- Ability to conduct post-implementation assessments, audits and reviews to evaluate outcomes of initiatives
- Experience interpreting data in order to develop and refine recovery processes
- Familiarity with business continuity program life cycle plans, source deliverables, and related disciplines
- Knowledge and understanding of IT strategy, security principles, enterprise architecture, and security architecture
- Technical knowledge of IT processes including operations, security, configuration, change, incident, problem, and disaster recovery management

Certifications:
- CISM
- CISSP
- CRISC
- GSLC
- ISO/IEC 27001 – LA/LI
- Security +

Advantageous skills:
- Project management skills
- Problem solving skills
- Organisational and planning skills
- Communication skills, both oral and written
- Reporting and presentation skills
- Interpersonal and relationship-building skills

Recommended Industry Engagement

- Security meetups
- C-level security conferences
- Security podcasts
- Security blogs

Lateral Career Transition	
Suitable for: • Network/System Administrator • Network/System Engineer • Network/ Systems Analyst • Application/Software Developer • Application/Software Tester ***Note:** Professionals from various IT workforces can transition to this role. The job titles listed are a few relevant roles.	**Complimentary Skills:** • Knowledge about disaster recovery planning techniques and technologies • Risk and Incident Management procedures • Experience and technical expertise

Cyber Risk Manager

Entry Level

Qualification:

Bachelor/Master degree with a major in:

- Computer Science
- Cyber Security
- Information Technology

TAFE Certifications:

- Certificate II in Security Operations
- Certificate IV in Information Technology (specialising in Cyber Security)
- Graduate Diploma of Cyber Security
- Advanced Diploma of Network Security
- Cyber Security Essentials

Internship/Volunteer Work Experience and capabilities

Manager positions are generally not offered to candidates with minimum work/internship experience.

At least 5 years of experience in a related field of IT security, Risk Management, Cyber threat analysis, and Vulnerability analysis is required, with minimum 3-5 years of experience in the field of IT.

Intermediate/Advanced Level

Preferred Combination of Experience:

- IT security experience focusing on security risk assessments, review of technical security requirements
- Knowledge and experience working with Information Security Governance and risk management programs and regulatory compliance
- Expertise and working knowledge of ISO27XXX, COBIT frameworks and conducting compliance NIST, PCI DSS, IRAP assessments
- Mature understanding of information security “best practices” including principles, security protocols, and standards
- Experience with policy and procedure interpretation and clarification and technical information security guidance to managers, data owners, project leads, application development teams, system operators, and user
- Knowledge and understanding of IT strategy, security principles, enterprise architecture, and security architecture
- Technical knowledge and experience in IT processes including operations, security, configuration, change, incident, problem and disaster recovery management
- Experience working with security concepts related to cyber threats, DNS, routing, authentication, VPN, proxy services, and DDOS mitigation technologies
- Experience working with various departments and management teams to manage risk, security compliance, and process effectiveness
- Working knowledge of business, finance, and management concepts

Certifications:

- CISM
- CISSP
- CRISC
- GSLC
- GSNA
- PCI-QSA
- SSCP
- ISO/IEC 27001 – LA/LI
- Security +
- SCCP

Advantageous skills:

- Project Management skills
- Leadership skills and mentoring experience (particularly mentoring technical staff)
- Efficient multitaskers with organisational skills
- Analytical and critical thinking
- Strong communication skills, both oral and written
- Interpersonal and relationship-building skills

Recommended Industry Engagement

- Security meetups
- C-level security conferences
- Security podcasts
- Security blogs

Lateral Career Transition

Suitable for:

- Risk Officer
- System Administrator
- System/Network Consultant
- System/Network Analyst
- IT/Business Consultant

* **Note:** Professionals from various IT workforces can transition to this role. The job titles listed are a few relevant roles

Complimentary Skills:

- Knowledge about Information Security Governance and risk management
- Working knowledge about IT principles, policies, standards and procedures
- Understanding of gap and risk assessment process
- Awareness of updates to regulatory requirements and processes

Auditor

Entry Level

Qualification:

Bachelor/Master degree with a major in:

- Computer Science
- Cyber Security
- Information Technology

TAFE Certifications:

- Certificate II in Security Operations
- Certificate IV in Information Technology (specialising in Cyber Security)
- Graduate Diploma of Cyber Security
- Advanced Diploma of Network Security

Internship/Volunteer Work Experience and capabilities

Auditing roles are generally not offered to candidates with minimum work/internship experience.

At least 2 to 6 years of experience in related field of IT security monitoring and analysis, cyber threat analysis, and vulnerability analysis is required.

Intermediate/Advanced Level

Preferred Combination of Experience:

- Experience and understanding of IT processes including operations, security, configuration, change, incident, problem and disaster recovery management
- Working knowledge of firewall and intrusion detection/prevention protocols, database management processes, and Windows, Linux, macOS, and other UNIX based operating systems
- Working knowledge of regulatory and industry data security standards (e.g. PCI, NIST and ASD)
- Experience working with IT risk and control frameworks, such as COBIT and ISO 27001/2
- Experience in planning and conducting audit engagements in accordance with compliance requirements such as PCI DSS
- Experience with data analytics, or possessing an analytical mindset
- Experience executing and documenting audit processes on a variety of computing environments and computer applications
- Experience providing consulting services to evaluate and assess new or significant business process or technology changes, and promotes the establishment of best practices
- Experience working with various departments and management teams to manage risk, security compliance, and process effectiveness

Certifications:

- CISA
- CISM
- CISSP
- CRISC
- GSLC
- GSNA
- IRAP
- PCI-QSA
- SSCP
- ISO/IEC 27001 – LA/LI
- Security +

Advantageous skills:

- Project Management Professional experience
- Ability to effectively process a large volume of information and/or uncertainty and draw meaningful and persuasive conclusions.
- Strong problem-solving and analytical skills
- Creative thinking

- Communication skills, both oral and written
- Interpersonal and relationship-building skills

Recommended Industry Engagement

- Security meetups
- Security podcasts
- Security blogs
- Security conferences

Lateral Career Transition

Suitable for:

- Quality Assurance Analyst
- IT Consultant
- Systems/Enterprise Architect
- IT Manager

***Note:** Professionals from various IT workforces can transition to this role with experience and certifications. The job titles listed are a few relevant roles.

Complimentary Skills:

- Working knowledge about policies, standards and procedures
- Audit and Assurance Experience
- Extensive knowledge, experience and technical expertise

IT/ICT Manager

Entry Level

Qualification:
Bachelor/Master degree with a major in:

- Computer Science
- Cyber Security
- Information Technology

TAFE Certifications:

- Certificate II in Security Operations
- Certificate IV in Information Technology (specialising in Cyber Security)
- Graduate Diploma of Cyber Security
- Advanced Diploma of Network Security
- Cyber Security Essentials

Internship/Volunteer Work Experience and capabilities:
Manager positions are generally not offered to candidates with minimal work/internship experience.
A minimum of 8 years of experience in related field of Information technology or communications is required.

Intermediate/Advanced Level

Preferred Combination of Experience:

- Experience overseeing the security of ICT systems, and creating a strategic plan for the deployment of information security technologies and program enhancements
- Experience directing ICT operations and setting priorities between system development, maintenance and operations
- Work with senior management to ensure that IT security protection policies are being implemented, reviewed, maintained, and governed effectively
- Expertise and knowledge of risk management programs and auditing experience, having conducted comprehensive risk assessments of IT systems
- Experience coordinating teams of specialist staff in the execution of complicated and inter-related activities within strict time frames, as well as identifying the critical path of workstreams and managing the inter-dependencies between components.
- Experience with resource allocation, coordinating teams and monitoring ongoing work progress
- Experience and knowledge of end-to-end ICT support functions and technologies including managing service desk ticketing and escalation processes
- Experience in managing, negotiating and maintaining service level agreements and vendor contracts, as well as evaluating supplier performance and relationships for ICT services, along with client and stakeholder management
- Experience and technical understanding of the following issues: managing complex Windows and VMWare platforms, disaster recovery, security, and networking
- Technical experience and understanding of IT operations practices and procedures including OS, LAN/WAN, and mainframe and PC hardware components

Certifications:

- CISM
- CISSP
- CRISC
- GSLC
- IRAP
- ISO/IEC 27001-LA/LI
- OSCP
- PCI-QSA
- Security +
- SSCP

Advantageous skills:

- Conflict resolution skills
- Negotiation skills
- Organisational and planning skills
- Process-oriented thinking
- Strong communication skills, both oral and written
- Reporting and presentation skills

Recommended Industry Engagement

- Business conferences
- Communities focusing on Information Technology
- Security blogs

Lateral Career Transition

Suitable for:

- IT Project Manager
- IT Project Coordinator
- IT Support Manager
- Technical Operations Officer

***Note:** Professionals from various IT workforces can transition to this role with experience and time in IT. The job titles listed are a few relevant roles.

Complimentary Skills:

- Knowledge of practices and methods of IT strategy, enterprise architecture and business requirements

Security Architect

Entry Level

Qualification:
Bachelor/Master degree a with major in:

- Computer Science/ Computer Science Engineering
- Cyber Security
- Information Technology

TAFE Certifications:

- Certificate II in Security Operations
- Certificate IV in Information Technology (specialising in Cyber Security)
- Graduate Diploma of Cyber Security
- Advanced Diploma of Network Security

Internship/Volunteer Work Experience and capabilities:
Generally, security architect roles are not offered to university graduates. Minimum experience of 2 years in related fields like Cyber Security, IT or administrative roles is required.

Intermediate/Advanced Level

Preferred Combination of Experience:

- Experience in architecting, designing, and building Security Architecture Frameworks
- Expert design skills in planning security systems by evaluating network and security technologies including local area networks (LANs), virtual private networks (VPNs), wide area networks (WANs), routers, firewalls, and related security and network devices
- Experience with planning and designing cryptographic systems, public key infrastructures (PKIs), including use of certification authorities (CAs) and digital signatures as well as hardware and software.
- Experience working with various security technologies and concepts encompassing enterprise solutions, and the ability to apply these in high-availability contexts within a demanding environment
- Experience performing threat modelling and value assessment techniques to regulate sound controls and architectural decisions
- Experience monitoring operational activities and projects to ensure compliance with security architectural blueprint and security strategies and providing analytical and technical security recommendations to respective stakeholders and business owner
- Experience working with Cloud Security, Cyber security (Malware, penetration testing, forensics, incident response), End point Security (McAfee, Symantec, Carbon Black, Trend), Security Incident and Event management (Splunk, McAfee, Symantec, Trend), Data Protection, network Security, Identity & Access Management
- Experience providing technical supervision for (and guidance to) a security team

Certifications:

- CISSP
- CRISC
- GSLC
- ISO/IEC 27001 – LA
- PCI-QSA
- Security +
- SSCP

Advantageous skills:

- Strategic thinking and problem-solving skills
- Stakeholder Management

- Project management skills
- Oral and communication skills
- Reporting skills

Recommended Industry Engagement

- Security conferences
- Security blogs
- Security meetups

Lateral Career Transition

Suitable for:

- Network/System Administrator
- Network/ System Engineer
- Database Administrator
- Application developer/Engineer
- Software Developer/Engineer

***Note:** Professionals from various IT workforces with technical expertise can transition to this role. The job titles listed are a few relevant roles.

Complimentary Skills:

- Strong technical knowledge in security architecture, design and infrastructure
- Knowledge of security and risk frameworks and security trends

Security Consultant

Entry Level

Qualification:

Bachelor/Master degree with a major in:

- Computer Science
- Cyber Security
- Information Technology

TAFE Certifications:

- Certificate II in Security Operations
- Certificate IV in Information Technology (specialising in Cyber Security)
- Graduate Diploma of Cyber Security
- Advanced Diploma of Network Security

Internship/Volunteer Work Experience and capabilities:

Entry-level experience and knowledge in:

- Latest Cyber Security Trends and attacks

Basic knowledge about:

- Information Security GRC policies
- Risk and Incident Management
- Networks and supporting systems

Intermediate/Advanced Level

Preferred Combination of Experience:

- Experience in an information security, information technology, ISMS development, operation or equivalent role
- risk management, audit or
- Experience working with information security best practice standards and guidelines governance and frameworks such as ISO27XXX, COBIT and CSA.
- Experience conducting compliance against NIST, PCI DSS, IRAP assessments
- Experience and knowledge about cyber security concepts such as: information security assessments/cyber risk assessments, gap assessments and recommendations, risk management frameworks (RMF), cyber-intrusion detection/incident handling and threat and vulnerability management
- Experience developing and maintain both new and existing security service processes, procedures, and knowledge management content relevant to security that requires understanding of common cyber threat terminology and methodologies, as well as possess basic understanding of cyber incident and response, and related current events.
- Experience conducting Information Security Risk and Gap Assessments based strategic business knowledge and be able to articulate risk in the context of business objectives
- Experience interpreting and analysing technical security reports for compliance to security policies
- Experience in designing and implementing assurance and security awareness programs

Certifications:

- CEH
- CISA
- CISM
- CISSP
- CRISC
- GSLC
- GSNA
- PCI-QSA
- SSCP
- ISO/IEC 27001 – LA/LI
- IRAP

- GSNA
- Security +

Advantageous skills:

- Customer Relationship Management
- Stakeholder Management
- Analytical and High attention to detail
- Negotiation skills
- Verbal and written communication skills
- Reporting skills

Recommended Industry Engagement

- Security Communities
- Security Podcasts
- Security Blogs
- Security Conference

Lateral Career Transition

Suitable for:

- Network/System Administrator
- Network/System Engineer
- Network/System Analyst
- IT Consultant/Analyst
- Technical Specialist
- Application Support Analyst

***Note:** Professionals from various IT workforces can transition to this role. The job titles listed are a few relevant roles.

Complimentary Skills:

- Knowledge about policies, standards and procedures
- Knowledge about business operations, risk management framework and risk assessment process

Cybercrime Investigator

Entry Level

Qualification:
Bachelor/Master degree with a major in:

- Computer Science
- Cyber Security
- Law
- Information Technology

TAFE Certifications:

- Certificate II in Security Operations
- Certificate IV in Information Technology (specialising in Cyber Security)
- Graduate Diploma of Cyber Security
- Advanced Diploma of Network Security
- Cyber Security Essentials

Internship/Volunteer Work Experience and capabilities:
Investigation roles require at least two years of experience in related field of IT security, Cyber threat analysis, and Vulnerability analysis.

Senior Level

Preferred Combination of Experience:

- Experience conducting both external and internal investigations
- Experience working with analytical tools, internet based research tools and relational databases
- Experience conducting review and documenting various forms of digital evidence such as: financial/transaction records, web traffic/IP address logs, audit logs and open source data for potential threats/subjects
- Experience conducting comprehensive subject interviews in high-stress environments
- Mature understanding and working knowledge of information security “best practices”, including principles, security protocols, and standards
- Experience working with security concepts related to cyber threats, DNS, routing, authentication, VPN, technologies
- Working knowledge technicalities of IT processes including operations, security, configuration, change and incident management
- Experience working with various departments and management teams to manage risk, security compliance, and process effectiveness.

Certifications:

- CCFP
- CEH
- CISA
- CISM
- CISSP
- CREST CCT
- CREST CRT
- CRISC
- GSLC
- GNFA
- GSNA
- IRAP
- OSCP
- OSCE
- PCI-QSA
- SSCP

- ISO/IEC 27001 – LA/LI
- Security +

Advantageous skills:

- Experience as a prosecutor or law enforcement officer would be a plus
- Analytical skills and critical thinking
- Strong communication skills, both oral and written
- Influencing and negotiation skills

Recommended Industry Engagements

- Security communities
- Security podcasts
- Business conferences

Lateral Career Transition

Suitable for:

- Network/System Engineer
- Network/System Architect
- Systems/Network Analyst
- Software Developer
- Program Analyst

***Note:** Professionals from various IT workforces with technical expertise can transition to this role. The job titles listed are a few relevant roles.

Complimentary Skills:

- Investigation skills
- Awareness Knowledge about Information Security Governance, laws, polices and requirements and processes

Security Analyst

Entry Level

Qualification:
Bachelor/Master degree with a major in:
- Computer Science
- Cyber Security
- Information Technology

TAFE Certifications:
Certificate II in Security Operations
- Certificate IV in Information Technology (specialising in Cyber Security)
- Certificate IV in Security and Risk Management
- Graduate Diploma of Cyber Security
- Advanced Diploma of Network Security

Internship/Volunteer Work Experience and capabilities:
Entry-level experience and knowledge in
- Networks and supporting systems
- Latest Cyber Security Trends and attacks

Basic knowledge about:
- Information Security GRC policies
- Risk and Incident Management

Intermediate/Advanced Level

Preferred Combination of Experience:
- Experience working in an IT and cloud security environment
- Experience working with physical computer components and architectures, TCP/IP, the OSI model, underlying networking protocols, and security hardware and software
- Working knowledge of information system accreditations, certification policies, standards, and governance
- Working knowledge in common cyber threat terminology, methodologies, possess basic understanding of cyber incident and response, and related current events
- Experience working with technical aspects such as network protocols, packet analysis tools, Data Loss prevention software and anti-virus/anti-malware
- Experience conducting Information Security Risk and Gap Assessments based strategic business knowledge and be able to articulate risk in the context of business objectives
- Experience conducting Cyber Intrusion Detection/Incident Handling and threat and vulnerability assessments
- Experience interpreting and analysing technical security reports for compliance to security policies
- Experience in designing and implementing assurance programs and security awareness programs

Certifications:
- CEH
- CISM
- CISSP
- CRISC
- GSLC
- GSNA
- OSCE
- PCI-QSA
- SSCP
- ISO/IEC 27001 – LA/LI
- IRAP
- Security +

Advantageous skills:

- Customer Relationship Management
- Verbal and written communication skills
- Reporting skills

Security Efforts

- Security communities
- Security podcasts
- Security blogs
- Security conferences

Lateral Career Transition

Suitable for:

- Network/System Administrator
- Network/System Engineer
- Network/System Analyst
- IT Consultant/Analyst
- Technical Specialist
- Application Support Analyst

***Note:** Professionals from various IT workforces with technical expertise can transition to this role. The job titles listed are a few relevant roles.

Complimentary Skills:

- Knowledge about policies, standards and procedures
- Knowledge about business operations, risk management framework and risk assessment process

Cyber Intelligent Analyst

Entry Level

Qualification:
Bachelor/Master degree with a major in:
- Computer Science
- Information Technology
- Cyber Security
- Cyber warfare Law

TAFE Certifications:
- Certificate II in Security Operations
- Certificate IV in Information Technology (specialising in Cyber Security)
- Graduate Diploma of Cyber Security
- Advanced Diploma of Network Security

Internship/Volunteer Work Experience and capabilities:
- Entry-level experience in IT
- Knowledge of basic intelligence strategies applied to the theories, principles, practices, and techniques of intelligence analysis
- Experience demonstrating research and analytical abilities

Intermediate/Advanced Level

Experience:
- Experience and expert knowledge of the intelligence cycle and the analytical process for all-source intelligence production
- Working experience of intelligence automated systems, including imagery analysis, database mining, network analysis, signals intelligence and exploitation tools and libraries
- Experience conducting research, creating, developing, and writing all-source intelligence assessments and RFI responses
- Experience in research, creation, development, and delivering of professional briefings, multimedia presentations, and written reports
- Experience working with current analytical tools such as, WEBTAS, Analytical Notebook, DCSG-A, GIS tools, and M3
- Working knowledge of networking (WAN, LAN, WLAN), network domains (Internet, intranet, DMZ), communication techniques/protocols (IP and others), their combined effects on network and host systems security, and physical and network based threat methodologies and tools
- Experience working with cloud Infrastructure and cloud Security

Certifications:
- CISM
- CISSP
- CRISC
- GSLC
- IRAP
- Security +

Advantageous skills:
- Military and tactical experience
- Strong negotiation skills
- Oral and communication skills
- Reporting skills
- Tactical and strategic thinking

Recommended Industry Engagement
- Security communities
- Security podcasts
- Cyber-intelligence conferences

Lateral Career Transition	
Suitable for: • Research Analyst • Network/System Engineer • Network/System Architect • Network/ Systems Analyst ***Note:** Professionals from various IT workforces with technical expertise can transition to this role. The job titles listed are a few relevant roles.	**Complimentary Skills:** • Knowledge about analytical tools • Technical understanding of inner-workings of your network, all of the subsequent threats, and how that relates to business risk

Cryptographer/Cryptanalyst

Entry Level

Qualification:
Bachelor/Master degree with a major in:
- Computer Science
- Computer Engineering
- Mathematics

Internship/Volunteer Work Experience and capabilities:
Entry-level experience in:
- Security/Network Administrator or
- Possess equivalent knowledge in areas such as:
- Symmetric and asymmetric cryptography

Intermediate/Advanced Level

Preferred Combination of Experience:
- Experience with the design, analysis, verification, and implementation of cryptographic algorithms and protocols
- Experience managing symmetric and/or asymmetric cryptographic keys and/or cryptographic hardware security modules
- Experience applying a quality management or process improvement framework such as Six Sigma, or an information security / operational risk management framework, i.e. ISO standards, NIST standards, and payment network compliance requirements
- Experience threat modelling and security requirements analysis
- Development experience with an object-oriented programming language, e.g., C++/Java/Python
- Experience developing code for Linux and Windows environments, as well as service-oriented and web-service architectures
- Experience developing statistical and mathematical models to analyse data and solve security problems

Certifications:
- CISSP
- Security +

Advantageous skills:
- Problem-solving and analytical skills
- Puzzle solving
- Research capabilities
- Oral and communication skills
- Creative thinking

Recommended Industry Engagement
- Security communities
- Security podcasts
- Capture the flag competitions
- Security conferences

Lateral Career Transition

Suitable for:
- Mathematics professionals
- Network/System Engineer
- Network/ System Administrator
- Software Developer

***Note:** Professionals from various IT workforces with technical expertise and mathematical skills can transition to this role. The job titles listed are a few relevant roles.

Complimentary Skills:
- Mathematical skills like probability theory and information theory
- Programming skills
- Knowledge about principles of cryptography (symmetric and asymmetric)

Cyber Forensic

Entry Level

Qualification:
Bachelor/Master degree with a major in:

- Forensic
- Cyber Security
- Law
- Cyber warfare Law

TAFE Certifications:

- Certificate II in Security Operations
- Certificate IV in Information Technology (specialising in Cyber Security)
- Graduate Diploma of Cyber Security
- Advanced Diploma of Network Security

Internship/Volunteer Work Experience and capabilities:
Entry-level experience in:

- IT security
- Digital forensics or law enforcement

Technical knowledge in:

- network skills
- operating systems
- hardware and software systems.

Intermediate/Advanced Level

Preferred Combination of Experience:

- Forensics analysis experience of operating systems and endpoints
- Work experience and knowledge of networking including, including TCP/IP-based network communications with network tracing knowledge
- Experience using digital forensics software applications such as EnCase, FTK, Sleuth Kit, Mandiant RedLine, and Sift Workstation.
- Experience using digital forensics analysis tools, threat analysis tools and eDiscovery tools (NUIX, Relativity, Clearwell, etc.)
- Experience working with forensics
- Experience providing expertise with a variety of digital forensics and threat analysis tools
- Experience leading client engagements and investigations including ability to effectively respond to client vulnerability/intrusions
- Assessment experience of intrusion signatures, tactics, techniques, and procedures associated with sophisticated cyber breaches
- Experience working with security software and document-creation applications
- Experience in hacking and intrusion techniques
- Prior experience with security testing and computer system diagnostics
- Experience with either internal/external audit, legal, or regulatory competencies

Certifications:

- CCFP
- CEH
- CISA
- CISM
- CISSP
- CERT CCT
- CERT CRT
- CRISC
- GSLC
- GNFA
- OSCE
- OSCP
- Security +

- SSCP

Advantageous skills:

- Good analytical skills
- Conceptual thinking and problem-solving skills
- Oral and communication skills
- Reporting skills

Recommended Industry Engagement

- Security blogs
- Security podcasts
- Security conferences

Lateral Career Transition

Suitable for:

- Network/System Administrator
- Network/System Engineer
- Network/System Architect
- Network/ Systems Analyst
- Technical Support Engineer

***Note:** Professionals from various IT workforces with technical expertise can transition to this role. The job titles listed are a few relevant roles.

Complimentary Skills:

- Knowledge about eDiscovery tools (NUIX, Clearwell, etc.)
- Understanding of forensic software applications (e.g. XRY, Encase, Helix, Etc.)

Computer Emergency Response Team (CERT) Operative

Entry Level

Qualification:
Bachelor/Master degree with a major in:

- Computer Science
- Information Technology
- Cyber Security
- Forensics

TAFE Certifications:

- Certificate II in Security Operations
- Certificate IV in Information Technology (specialising in Cyber Security)
- Graduate Diploma of Cyber Security
- Advanced Diploma of Network Security

Internship/Volunteer Work Experience and capabilities:
Entry-level experience in: Security/Network Administrator
or
Possess equivalent knowledge in areas such as:

- Security methodologies and processes
- TCP/IP protocols and analysis

Intermediate/Advanced Level

Preferred Combination of Experience:

- Experience in monitoring, analysing, detecting, and responding to Cyber events and incidents within information systems and networks
- Experience providing cyber security operational services, including intrusion detection and prevention, situational awareness of network intrusions, security events, anti-virus and data spillage, vulnerability assessment tools and incident response actions
- Experience performing malware analysis and reverse engineering
- Experience testing, implementing, deploying, operating, maintaining, and administering the infrastructure hardware and software required to effectively manage the organization's cyber security operational services
- Experience operating and maintaining security toolsets to provide continuous monitoring and ongoing authorization programs
- Experience working with Security Information and Event Management (SIEM) solutions
- Experience composing security alert notifications and providing advice and assisting incident responders with steps to take to investigate and resolve computer security incidents
- Experience working with network and host-based security applications and tools, such as network and host assessment/scanning tools, and other security software packages
- Experience with scripting languages such as Bash, Perl, or Python
- Experience working with various log types (e.g. Windows Event, Web server, Firewall logs, etc.)
- Experience producing and presenting metrics supporting proactive identification of risk; escalating and providing recommended mitigations of issues and concerns

Certifications:

- CEH
- CISM
- CISSP
- CERT CCT
- CERT CRT
- CRISC
- GSLC
- ISO/IEC 27001-LA/LI
- OSCE
- OSCP

- SSCP
- Security +

Advantageous skills:

- Customer service and organizational skills
- Time management skills with ability to multitask and prioritise work
- Problem-solving and analytical skills
- Oral and communication skills
- Reporting skills
- Tactical and strategic thinking

Recommended Industry Engagement

- Security communities
- Security podcasts
- Capture the flag competitions
- Security conferences

Lateral Career Transition

Suitable for:

- Network/System Administrator
- Network/System Engineer
- Network/System Analyst
- IT Project Coordinator
- Technical/Data Center Support Specialist

***Note:** Professionals from various IT workforces with technical expertise can transition to this role. The job titles listed are a few relevant roles.

Complimentary Skills:

- Knowledge about system monitoring and vulnerability assessments
- Reverser engineering techniques and skills
- Knowledge about incident response and communication protocols

SIEM Operator

Entry Level

Qualification:
Bachelor/Master degree with a major in:

- Computer Science/ Computer Science Engineering
- Cyber Security
- Information Technology

TAFE Certifications:

- Certificate II in Security Operations
- Certificate IV in Information Technology (specialising in Cyber Security)
- Graduate Diploma of Cyber Security
- Advanced Diploma of Network Security

Internship/Volunteer Work Experience and capabilities:
Generally, SIEM Operator roles are not offered to university graduates. Minimum experience of 2 years in related areas like threat analysis or system administrator roles is required

Intermediate/Advanced Level

Preferred Combination of Experience:

- Experience of developing and improving services in a rapidly changing and expanding environment
- Experience working in an operational environment with SIEM technologies and security tooling
- Experience working in data analytics, with in-depth knowledge of principles and approaches in relation to data mining
- Experience maintaining SIEM platform stability and health, alongside providing regular and clear communication to the MTD team and relevant stakeholders
- Experience monitoring system capacity to ensure that the platform does not encounter resource issues
- Experience resolving any platform issues that may occur within SLA and ensuring that service impact is minimal
- Experience enabling and implementing new SIEM alarms from inception, through to tuning
- Experience with proactive and reactive tuning alarms and log sources for all clients on the platform
- Experience overseeing upgrades and changes on the SIEM platform
- Experience delivering and reporting SLA management
- Working knowledge of security technologies including: firewalls, IDS/IPS/HIDS, anti-virus, and vulnerability scanning

Certifications:

- CEH
- CISA
- CISM
- CISSP
- CERT CCT
- CERT CRT
- CRISC
- GSLC
- GSNA
- ISO/IEC 27001-LA/LI
- OSCE
- OSCP
- SSCP

- Security +

Advantageous skills:

- Good analytical skills
- Conceptual thinking and problem-solving skills
- Oral and communication skills
- Reporting skills

Recommended Industry Engagement

- Technical meetups
- Technical conferences
- Technical blogs

Lateral Career Transition

Suitable for:

- Network/System Administrator
- Network/System Engineer
- System/Software Engineer
- Quality Assurance Analyst
- IT Project Coordinator

***Note**: Professionals from various IT workforces with technical expertise can transition to this role. The job titles listed are a few relevant roles.

Complimentary Skills:

- Knowledge of SIEM technologies and platform
- Understanding of Standard Operating Environment and procedures

Firewall Administrator

Entry Level

Qualification:

Bachelor/Master degree with a major in:

- Computer Science
- Cyber Security
- Information Technology

TAFE Certifications:

- Certificate II in Security Operations
- Certificate IV in Information Technology (specialising in Cyber Security)
- Graduate Diploma of Cyber Security
- Advanced Diploma of Network Security
- Cyber Security Essentials

Internship/Volunteer Work Experience and capabilities:

Manager positions are generally not offered to candidates with minimal work/internship experience.

A minimum of 8 years of experience in related field of firewall architecture, design, testing, development, migration, and integration, with minimum 3-5 years of experience in the field of information security is required.

Intermediate/Advanced Level

Preferred Combination of Experience:

- Management experience providing oversight in the monitoring and management of an enterprise security perimeter
- Experience evaluating functionality, risk, and maintainability of perimeter security systems
- Experience in leading and managing a team of IT subject matter experts in planning, coordination, and execution of complex high visibility tasks essential to the security and operation of an enterprise
- IT network engineering support experience (Tier II, Tier III, network infrastructure implementation and maintenance) focusing on perimeter security
- Technical experience with firewall architecture, design, testing, development, migration, and integration
- Experience configuring firewall rule sets and objects in an enterprise environment
- Experience designing, implementing, and maintaining firewall security and service availability throughout the system life cycle
- Experience troubleshooting and resolving highly technical core service outages and other complex IT system issues
- Experience working with stakeholders - including program and project managers, end-users, and technical staff - to develop, test, implement, and sustain critical IT infrastructure and security architectures
- Hands-on experience and in-depth knowledge about firewall infrastructure technologies and management systems
- Experience understanding the areas of system and infrastructure design, operations and firewall engineering

Certifications:

- CEH
- CISA
- CISM
- CISSP
- CERT CCT
- CERT CRT
- CRISC
- GSLC
- ISO/IEC 27001-LA/LI

- OSCE
- OSCP
- SSCP
- Security +

Advantageous skills:

- Project management skills
- Problem solving skills
- Organisational and planning skills
- Client and vendor management skills
- Strong communication skills, both oral and written
- Reporting and presentation skills
- Interpersonal and relationship-building skills

Recommended Industry Engagement

- C-level security conferences and meetups
- Security podcasts
- Security blogs

Lateral Career Transition

Suitable for:

- Security/System Administrator
- Database Administrator
- Program Analyst
- Network/System Engineer
- Systems/Network Analyst
-

***Note:** Professionals from various IT workforces with technical expertise can transition to this role. The job titles listed are a few relevant roles.

Complimentary Skills:

- Knowledge about firewall and perimeter safety technologies
- Project Management and leadership experience

Forensic Analyst

Entry Level

Qualification:
Bachelor/Master degree with a major in:

- Forensic
- Cyber Security
- Law
- Cyber warfare Law

TAFE Certifications:

- Certificate II in Security Operations
- Certificate IV in Information Technology (specialising in Cyber Security)
- Graduate Diploma of Cyber Security
- Advanced Diploma of Network Security

Internship/Volunteer Work Experience and capabilities:
Entry-level experience in IT security, Digital forensics or law enforcement.

Technical knowledge including network skills, operating systems and hardware and software systems.

Intermediate/Advanced Level

Preferred Combination of Experience:

- Forensics analysis experience of operating systems and endpoints
- Work experience and knowledge of networking including, TCP/IP-based network communications with network tracing
- Experience using digital forensics software applications such as EnCase, FTK, Sleuth Kit, Mandiant RedLine, and Sift Workstation.
- Experience using digital forensics analysis tools, threat analysis tools, and eDiscovery tools (NUIX, Relativity, Clearwell, etc.)
- Experience providing expertise with a variety of digital forensics and threat analysis tools
- Experience leading client engagements and investigations, including ability to effectively respond to client vulnerability/intrusions
- Assessment experience with intrusion signatures, tactics, techniques, and procedures associated with sophisticated cyber breaches
- Experience working with security software and document-creation applications
- Experience in hacking and intrusion techniques
- Prior experience with security testing and computer system diagnostics
- Experience with either internal/external audit, legal or regulatory competencies
- Working programming knowledge in C, C++, C#, Java and similar

Certifications:

- CCFP
- CEH
- CISA
- CISM
- CISSP
- CERT CCT
- CERT CRT
- CRISC
- GSLC
- GNFA
- OSCE
- OSCP
- Security +

- SSCP

Advantageous skills:

- Good analytical skills
- Conceptual thinking and problem-solving skills
- Oral and communication skills
- Reporting skills

Recommended Industry Engagement

- Security communities
- Security podcasts
- Capture the flag competitions
- Security conferences

Lateral Career Transition

Suitable for:

- Network/System Administrator
- Network/System Engineer
- Network/System Architect
- Network/ Systems Analyst
- Technical Support Engineer

***Note:** Professionals from various IT workforces with technical expertise can transition to this role. The job titles listed are a few relevant roles.

Complimentary Skills:

- Knowledge about eDiscovery tools (NUIX, Clearwell, etc.)
- Understanding of forensic software applications (e.g. XRY, Encase, Helix, Etc.)

Intrusion Detection Specialist

Entry Level

Qualification:
Bachelor/Master degree with a major in:
- Computer Science
- Cyber Security
- Law
- Information Technology

TAFE Certifications:
- Certificate II in Security Operations
- Certificate IV in Information Technology (specialising in Cyber Security)
- Graduate Diploma of Cyber Security
- Advanced Diploma of Network Security
- Cyber Security Essentials

Internship/Volunteer Work Experience and capabilities:
Generally, intrusion detection roles are not offered to university graduates. Minimum experience of 2 years in related areas like threat analysis, SIEM operator or system administrator roles is required.

Intermediate/Advanced Level

Preferred Combination of Experience:
- Experience managing and performing network security monitoring functions
- Experience working with Intrusion Detection Systems (IDS), and other toolsets to identify and triage anomalies
- Experience with intrusion monitoring, cyber situational awareness, and reporting of suspicious events
- Experience conducting both external and internal security and vulnerability assessments
- Experience creating custom IDS/IPS signatures based on new threats and adversary tactics, techniques, and procedures
- Experience assisting IDS and Infrastructure management with maintaining equipment, including intrusion detection systems, SIEM technology, and log aggregators
- Experience establishing information assurance and security requirements based upon the analysis of user, policy, regulatory, and resource demands
- Experience conducting penetration tests on web-based applications, networks, and computer systems
- Experience with monitoring, compiling, and tracking vulnerabilities over time for metrics purposes
- Experience reviewing and defining requirements for information security solution
- Experience incorporating business considerations (e.g. loss of earnings due to downtime, cost of engagement, etc.) into security strategies

Certifications:
- CEH
- CISA
- CISM
- CISSP
- CERT CCT
- CERT CRT
- CRISC
- GSLC
- ISO/IEC 27001-LA/LI
- OSCE
- OSCP
- SSCP

- Security +

Advantageous skills:

- Analytical skills and critical thinking
- Hight attention to detail
- Strong communication skills, both oral and written
- Influencing and negotiation skills

Recommended Industry Engagements

- Security Communities
- Security Podcasts
- Business Conferences

Lateral Career Transition

Suitable for:

- Network/System Administrator
- Network/System Engineer
- Network/System Architect
- Network/ Systems Analyst
- Technical Support Engineer
- Software Engineer

***Note:** Professionals from various IT workforces with technical expertise can transition to this role. The job titles listed are a few relevant roles.

Complimentary Skills:

- Knowledge about intrusion detection software and principles
- Knowledge of SIEM technology and access and identity management principles

System Administrator

Entry Level

Qualification:

Bachelor/Master degree with a major in:

- Computer Science/ Computer Science Engineering
- Information Technology
- General Engineering

TAFE Certifications:

- Certificate II in Security Operations
- Certificate IV in Information Technology (specialising in Cyber Security)
- Graduate Diploma of Cyber Security
- Advanced Diploma of Network Security

Internship/Volunteer Work Experience and capabilities:

Entry-level experience in scripting, programming, networks and information systems.
Working knowledge of systems engineering concepts, principles, and theories.

Intermediate/Advanced Level

Preferred Combination of Experience:

- Experience providing hardware support for enterprise data centre servers, firewalls, switches, and VOIP phones
- Experience provide software application tier 1 and tier 2 support for core systems
- Experience with onsite and remote troubleshooting assistance and management for corporate users
- Experience in resolving incidents, managing problems, fulfilling user requests and performing systems maintenance
- Experience managing user account security and backups
- Reporting expertise on infrastructure status and capacity planning, including network health
- Experience reporting on current infrastructure status for capacity planning, as well as working and supporting various environments, such as Windows OS, Mac OS, antivirus, SharePoint, SCCM, ITAM, SQL, PL/SQL, and Oracle
- Prior experience planning and implementing software and hardware updates and patches
- Experience working with servers, storage, switches, routers, and firewall management as per business request
- Working experience in scripting technologies, Microsoft Active Directory, Exchange and networking protocols such as TCP/IP

Certifications:

- CEH
- CISA
- CISM
- CISSP
- CERT CCT
- CERT CRT
- CRISC
- GSLC
- GSNA
- IRAP
- ISO/IEC 27001-LA/LI
- OSCE
- OSCP

- PCI-QSA
- SSCP
- Security +

Advantageous skills:

- Good analytical skills
- Conceptual thinking and problem-solving skills
- Organizational skills
- Interpersonal skills
- Strong communication skills, both oral and written

Recommended Industry Engagement

- Technical meetups
- Technical conferences
- Technical Blogs

Lateral Career Transition

Suitable for:

- Software Tester
- IT Technician
- IT Customer Service
- Software Developer

***Note:** Professionals from various IT workforces can transition to this role. The job titles listed are a few relevant roles.

Complimentary Skills:

- Knowledge of networking, databases and active directories
- Working knowledge of configuration and operating systems

Systems Engineer

Entry Level

Qualification:

Bachelor/Master degree with a major in:

- Computer Science
- Cyber Security
- Information Technology

TAFE Certifications:

- Certificate II in Security Operations
- Certificate IV in Information Technology (specialising in Cyber Security)
- Graduate Diploma of Cyber Security
- Advanced Diploma of Network Security
- Cyber Security Essentials

Internship/Volunteer Work Experience and capabilities:

Entry-level experience in scripting, programming, networks and information systems

Working knowledge of systems engineering concepts, principles, and theories.

Intermediate/Advanced Level

Preferred Combination of Experience:

- Experience implementation and maintaining systems and hardware within an enterprise environment
- Experience working designing, implementation, and maintenance of managed desktop environment with a focus on automation, user satisfaction and security
- Experience with simulating, testing, and tuning of an infrastructure environment
- Experience implementing network and server environment changes across multiple data centres
- Experience with administering the infrastructure environment in line with operations policies and procedures
- Experience providing technical support using remote management and monitoring tools
- Experience managing support calls and tickets ensuring all system interactions are logged
- Experience diagnosing hardware and software issues to advise the end user on the appropriate resolution path
- Experience with installation and configuration of workstations, servers, and other physical and virtual IT equipment
- Prior experience researching unknowns and error checking configurations using available information resources
- Experience identifying, escalating, and responding to situations requiring urgent attention
- Experience maintaining and assisting in development of a Standard Operating Environment
- Implementing changes in production environments, maintaining and monitoring SLA's
- Working knowledge of networks and network protocols, including: TCP/IP, DHCP, DNS, VoIP, SMTP, SPF, DKIM, mail servers, and malicious networking activities

Certifications:

- CEH
- CISA
- CISM
- CISSP
- CERT CCT
- CERT CRT
- CRISC
- GSLC
- GSNA
- IRAP

- ISO/IEC 27001-LA/LI
- OSCE
- OSCP
- PCI-QSA
- SSCP
- Security +

Advantageous skills:

- Organizational skills
- Ability to work in teams
- Interpersonal skills
- Strong communication skills, both oral and written

Recommended Industry Engagements

- Technical meetups
- Technical conferences
- Technical blogs

Lateral Career Transition

Suitable for:

- Software Tester
- IT Technician
- IT Customer Service
- Software Developer

***Note:** Professionals from various IT workforces can transition to this role. The job titles listed are a few relevant roles.

Complimentary Skills:

- In-depth knowledge of computer science, networks and databases
- Understanding of programming languages, information systems and design

Security Administrator

Entry Level

Qualification:

Bachelor/Master degree with a major in:

- Computer Science/ Computer Science Engineering
- Cyber Security
- Information Technology

TAFE Certifications:

- Certificate II in Security Operations
- Certificate IV in Information Technology (specialising in Cyber Security)
- Graduate Diploma of Cyber Security
- Advanced Diploma of Network Security

Internship/Volunteer Work Experience and capabilities:

Generally, security administrator roles are not offered to university graduates. Minimum experience of 2 years in related fields like Cyber Security, IT or system administrator roles is required

Intermediate/Advanced Level

Preferred Combination of Experience:

- Experience establishing and implementing practices for monitoring of information systems' logical and physical security to minimise the risk of equipment/data loss, theft, or tampering
- Experience undertaking investigations and report on security breaches and incidents to guide the refinement of practices and processes in order to reduce the likelihood and impact of security related incidents
- Experience across information security and providing recommendations, and implementing changes to procedures and systems to enhance security
- Experience undertaking investigations and report on security breaches and incidents to guide the refinement of practices and processes and reduce the likelihood and impact of security related incidents
- Experience performing regular security reviews, compliance testing, vulnerability testing, risk analyses, and security assessments to ensure adherence to adopted security standards
- Experience monitoring network traffic and defending systems against unauthorised access

Certifications:

- CEH
- CISA
- CISM
- CISSP
- CERT CCT
- CERT CRT
- CRISC
- GSLC
- GSNA
- IRAP
- ISO/IEC 27001-LA/LI
- OSCE
- OSCP
- PCI-QSA
- SSCP
- Security +

Advantageous skills:

- Strategic thinking and problem-solving skills
- Project management skills
- Oral and communication skills
- Reporting skills

Recommended Industry Engagement

- Security conferences
- Capture the flag competitions
- Security blogs
- Security meetups

Lateral Career Transition

Suitable for:

- Network Administrator/Engineer
- System Administrator/Engineer
- Database Administrator
- Software Engineer
- System Analyst

***Note:** Professionals from various IT workforces can transition to this role. The job titles listed are a few relevant roles.

Complimentary Skills:

- Strong technical knowledge in security architecture, design and infrastructure
- Knowledge of security and risk frameworks and security trends
- Technical knowledge in security principles such as physical security, social engineering, intrusion detection, prevention and response, firewalls, honeypots etc.

Security Engineer

Entry Level

Qualification:
Bachelor/Master degree with a major in:

- Computer Science/Computer Science Engineering
- Cyber Security
- Information Technology

TAFE Certifications:

- Certificate II in Security Operations
- Certificate IV in Information Technology (specialising in Cyber Security)
- Graduate Diploma of Cyber Security
- Advanced Diploma of Network Security

Internship/Volunteer Work Experience and capabilities:
Entry-level experience or working knowledge of security engineering concepts, networking fundamentals, and understanding of security analysis and skills

Intermediate/Advanced Level

Preferred Combination of Experience:

- Experience configuring, maintaining and reporting on intrusion prevention systems, and other network security devices
- Experience investigating potential security violations, threats and breaches, participating in incident response, and preparing reports on violations as necessary
- Experience conducting security assessments to ensure adherence to customer specific security policy, procedures, and industry standards
- Experience assisting with the review and definition of security requirements and review systems to determine if they are designed to comply with established standards
- Experience working with SQL database platforms
- Experience working with information and networking security practices
- Experience with networking and TCP/IP, UDP, IPSEC, HTTP, HTTPS, routing protocols, etc.
- Skilled in implementing and configuring networks and network components
- Experience working with computer programming and scripting
- Experience with application security and encryption technologies, as well as subnetting, DNS, VPNs, VLANs, VoIP and other network routing methods
- Experience with management of the LAN/WAN networking infrastructure, cloud-integration, video conferencing, and telecommunications.
- Experience ensuring data integrity and security whilst providing empowering functionality and systems access across traditional and emerging mediums

Certifications:

- CEH
- CISA
- CISM
- CISSP
- CERT CCT
- CERT CRT
- CRISC
- GSLC
- GSNA
- IRAP
- ISO/IEC 27001-LA/LI

- OSCE
- OSCP
- PCI-QSA
- SSCP
- Security +

Advantageous skills:

- Conceptual thinking and problem-solving skills
- Analytical thinking
- Oral and communication skills
- Reporting skills

Recommended Industry Engagement

- Security Conference
- Capture the Flag competitions
- Security Blogs
- Security Meet ups

Lateral Career Transition

Suitable for:

- Software Developer
- Systems Engineer
- IT Technician
- IT Customer Service
- Software Engineer
- System Analyst

***Note:** Professionals from various IT workforces can transition to this role. The job titles listed are a few relevant roles

Complimentary Skills:

- In-depth understanding of networking fundamentals
- Understanding of security fundamentals and principles such as physical security, social engineering, intrusion detection, prevention and response, firewalls, honeypots etc.

Penetration Tester

Entry Level

Qualification:

Bachelor/Master degree with a major in:

- Cyber Security
- Computer Science/Computer Science Engineering
- Information Technology

TAFE Certifications:

- Certificate II in Security Operations
- Certificate IV in Information Technology (specialising in Cyber Security)
- Graduate Diploma of Cyber Security
- Advanced Diploma of Network Security
- Cyber Security Essentials

Internship/Volunteer Work Experience and capabilities:

As most degrees do not specialise in ethical hacking and pentesting, hands-on experience is essential to develop technical skills. Participating in CTFs or bug bounties is appreciated.

Keen passion for security and networking skills is required

Intermediate/Advanced Level

Preferred Combination of Experience:

- Experience working with scripting languages such as Bash, JavaScript or PHP and programming languages such as Perl, Python, Ruby, Shell, VB, C/C++, C#
- Experience working with penetration testing tools such as Burp Suite and Metasploit
- Penetration testing or vulnerability identification experience, including web-app testing, infrastructure testing, wireless network testing, and mobile application testing (iOS, Android, and Windows)
- Experience and understanding of Windows and UNIX based operating systems
- Experience of working within compliance and governance frameworks such as PCI, HIPAA, GLBA, NIST or similar
- Having expertise in one or more of the following fields: mobile pentesting, thick clients, hardware, source code review, red teams, incident response, and forensic review
- Experience and understanding of software security principles, including both technical security and secure software design
- Experience writing technical documentation and reports

Certifications:

- CEH
- CREST CCT
- CREST CRT
- OSCE
- OSCP
- SSCP

Advantageous skills:

- Consulting skills
- Problem solving skills
- Creative ‘out-of-the-box’ thinking
- Strong communication skills, both oral and written
- Reporting and presentation skills

Recommended Industry Engagement

- Capture the flag competitions
- Security blogs

- Security podcasts
- Security conferences and meetups
- bug bounties
- Sites hosting virtual machines etc. for practising hacking skills

Lateral Career Transition

Suitable for:

- Software Developer
- Network/System Administrator
- Network/System Engineer
- Systems/Network Analyst

***Note:** Professionals from various IT workforces with technical expertise and networking can transition to this role. The job titles listed are a few relevant roles

Complimentary Skills:

- Understanding of security tools and applications
- Strong technical background with coding abilities
- In depth knowledge about operating systems, software, communications and network protocols

Software Developer (Security)

Entry Level

Qualification:
Bachelor/Master degree with a major in:
- Computer Science/ Computer Science Engineering
- Information Technology

TAFE Certifications:
- Certificate II in Security Operations
- Certificate IV in Information Technology (specialising in Cyber Security)
- Graduate Diploma of Cyber Security
- Advanced Diploma of Network Security

Internship/Volunteer Work Experience and capabilities:
Entry-level experience or working knowledge of software development, programming languages and design principals

Intermediate/Advanced Level

Preferred Combination of Experience:
- Experience designing and building software applications in line with business strategy
- Experience with test application logic, and resolving issues to ensure strong functionality and optimization
- Experience monitoring, maintaining and improving the performance of existing software
- Experience and board knowledge to recommend improvements to existing software programs and applications
- Working knowledge of main stream languages such as Java, .Net, PHP, Python etc.
- Experience working within the guidelines of the change management processes and provide impact assessment for change requests

Certifications:
- CEH
- CREST CCT
- CREST CRT
- OSCE
- OSCP
- SSCP

Advantageous skills:
- Analytical skills and problem-solving skills
- High attention to details
- Strong communication skills, both oral and written

Recommended Industry Engagement
- Technical meetups
- Technical conferences
- Open source software development
- Blogs

Lateral Career Transition

Suitable for:
- Software Tester
- IT Technician
- IT Customer Service

Complimentary Skills:
- Enhanced programming knowledge
- Secure programming knowledge (eg OWASP, WASC and related industry standards)
- Security testing techniques

- Programmer
- Software Engineer
- System Analyst

***Note:** Professionals from various IT workforces with coding expertise can transition with to this role. The job titles listed are a few relevant roles

Appendix – Recommended Industry Engagement

With the cyber security industry growing at an accelerated pace, breaking into the industry as a beginner or an experienced professional, you should have up-to-date knowledge and awareness of what is happening in the industry. A big part of achieving this is through industry engagement.

Listed below are few industry engagement and resources to enable both your knowledge and networking within the industry.

Security Communities

Australian Information Security Association AISA**:** Link
Information Security System Association ISSA: Link
Cyber Security Community – IET Engineering Communities: Link
ISACA Cyber Security Community: Link
Information Security Forum ISF: Link
Association of Information Security Professionals: Link
IEEE Cyber Security Community: Link
International Association for Cryptologic Research: Link

Conferences

CRIKEYCON: Link
Australian Cyber Security Centre (ACSC) Conference: Link
AusCERT Conference: Link
AISA National Conference**:** Link
ISACA Oceania CACS 2017: Link
Cyber in Business Conference: Link
RUXCON: Link
DEF CON: Link
Black Hat: Link
WAHCKON: Link

Blogs

Kerbs on Security: Link
Schneier on Security: Link
Dark Reading: Link
Security Bloggers Network: Link
CSO Online: Link
Zero Day Security Blog: Link
The Hacker News: Link
TechRepublic: Link
Active Directory Security: Link
The State of Security: Link

Podcasts

Security Weekly Podcast: Link

Risky Business Podcast: Link
Naked Security podcast by Sophos: Link
Threat post Podcast: Link

Security Meetups

SecTalks: Sydney, Perth, Brisbane, Melbourne, Canberra
CryptoAUSTRALIA: Sydney
Cryptoparty: Sydney

Capture the Flag competitions

Capture the Flag competitions are conducted as part of meetups, conferences and industry engagements. While CTFs varies widely from each other and cannot be ranked, they can be used as skill building and networking opportunities. Highly recognised CTF's are comparatively worth more upon completion.

A calendar of CTFs are available online at Ctftime.
Qualifier CTFs for conferences like DEFCON are available at legbit
Some of the CTFs conducted as part of security conference and Meetups in Australia are : Ruxcon, PlatypusCon, SecTalks

Sites Hosting Virtual Machines

Practical Pentest Labs
VulnHub