

Master of Business Administration (Cybersecurity Management)

AQF Level 9 · 2 Years Full-Time · Face-to-face on campus · 160 Credit Points

Course Rationale

The MBA (Cybersecurity Management) (AQF Level 9) produces visionary leaders who integrate strategic business decision-making with advanced cybersecurity knowledge. It addresses increasing demands for professionals who can navigate digital risk. The course blends leadership, ethics, innovation, and real-world application through its Cybersecurity Leadership Capstone with Work-Integrated Learning. Delivered face-to-face on campus at ZII.

Career Pathways

Graduates will be prepared for roles directly related to IT and cybersecurity management, including:

- Chief Information Security Officer (CISO)
- Cybersecurity Manager
- IT Governance Manager
- Risk and Compliance Manager
- Business Continuity Strategist
- Management Consultant (Cybersecurity)
- Executive roles with technology/cybersecurity focus

Learning Time Period and Fees

Duration: 2 years full-time (4 semesters)

Total Workload: 2,616 hours

832

TIMETABLED

1,664

PRIVATE STUDY

120

WIL PLACEMENT

DOMESTIC STUDENTS

\$32,000 total

+ \$500 enrolment fee (non-refundable)

Admission Requirements

Domestic and International Applicants:

- Bachelor's degree (or Grad Cert / Grad Dip)
- Interview assessment with Course Coordinator
- Satisfy Genuine Student (GS) criteria
- Alternative: mature age, STAT, portfolio entry
- Educational disadvantage consideration available

Work-Integrated Learning (WIL)

The MBA includes a WIL component as a key feature:

- IT505 Cybersecurity Leadership Capstone includes WIL
- 120 hours work placement at approved industry partners
- All WIL placements are face-to-face at approved sites
- Prepares graduates for senior cybersecurity leadership roles

International Student Fee

INTERNATIONAL STUDENTS

\$48,000 total

+ \$500 enrolment fee (non-refundable)

Must satisfy Genuine Student (GS) requirement per Australian Government regs.

English Proficiency

International students must demonstrate proficiency:

- IELTS: 6.5 overall (no sub-score below 6.0)
- TOEFL iBT: 79 (minimum sub-scores 19)
- PTE Academic: 58 (no score below 50)

Alternative:

- Completion of prior studies in English or relevant English pathway programs

Entry and Exit Options

Entry:

- Australian Bachelor's degree or equivalent
- Graduate Certificate or Graduate Diploma
- Interview with Course Coordinator

Exit Pathway:

- Exit after 4 foundational units (MG400, MG401, IT400, IT401) with Graduate Certificate in Business Administration (Cybersecurity Management)

Credit and Recognition of Prior Learning (RPL)

- Credit Transfer for formal qualifications from other institutions
- RPL for work experience (assessed individually)
- Documentation: transcripts, resumes, reference letters, portfolios

Tuition Protection (TPS): Cannot deliver? You are entitled to an equivalent placement or TPS refund. Rights set out in your Letter of Offer. Further information: www.tps.gov.au

Master of Business Administration (Cybersecurity Management)

Course Structure · AQF Level 9 · 16 Units · 160 Credit Points · Face-to-face on campus

The MBA comprises 16 units (160 credit points): 13 core (130 CP) + 3 electives (30 CP). Year 1, Semester 1 units also form the Graduate Certificate in Business Administration (Cybersecurity Management)

#	Year/Sem	Code	Unit Title	Type	Prerequisite	CP
Year 1, Semester 1 — also constitutes the Graduate Certificate in Business Administration (Cybersecurity Management)						
01	Y1 S1	MG40...	Executive Leadership and Team Management	Core	—	10
02		MG40...	Strategies for Corporate Communication and Cri...	Core	—	10
03		IT400	Foundations of Cybersecurity	Core	—	10
04		IT401	Legal and Ethical Issues in Cybersecurity	Core	—	10
Year 1, Semester 2						
05	Y1 S2	MG40...	Strategic Marketing and Brand Management	Core	—	10
06		MG40...	Managerial Accounting and Financial Decision-...	Core	—	10
07		IT501	Systems Engineering and Design	Core	IT400	10
08		—	Elective Unit (choose from list)	Elective	—	10
Year 2, Semester 1						
09	Y2 S1	IT500	Design Thinking for Managers	Core	MG400	10
10		IT502	Risk and Change Management in Cybersecurity	Core	—	10
11		IT503	Contemporary Trends in Cybersecurity	Core	IT401	10
12		IT504	Project Management in Cybersecurity	Core	—	10
Year 2, Semester 2						
13	Y2 S2	IT505	Cybersecurity Leadership Capstone (WIL)	Core	IT504 + 8 Y1	10
14		IT511	Cyber Forensics and Incident Response Manag...	Core	—	10
15		—	Elective Unit	Elective	—	10
16		—	Elective Unit	Elective	—	10
Elective List (choose 3): IT411 Data Privacy · IT412 Ethical Hacking · IT512 Human Behaviour & Cybersecurity.						
Total Credit Points						160

Course Rules: To qualify for the award of MBA (Cybersecurity Management), the candidate must satisfactorily complete 13 core subjects (130 credit points) and 3 elective subjects (30 credit points). Total: 160 credit points.