Graduate Certificate in Cyber Security Governance and Risk Management

- Understand how to design and apply governance and compliance frameworks to cyber security risks and incidents. Advance your career in a high demand field and lead your organisation's cyber security management strategy.

INDUSTRY PARTNERS:

IBM

paloalto NETWORKS

RMIT Online

Who this program is for

Cyber security is no longer the responsibility of security managers of IT teams. Technological advancements have increased the sophistication and prevalence of cyber attacks, costing the global economy US$6 trillion each year (Cyber Security Ventures, 2020). Today, cyber security is critical to every organisation's success, and involves delivering value to sustain growth whilst maintaining a risk-based approach to mitigating the possibilities of a cyber attack.

Our Graduate Certificate in Cyber Security Governance and Risk Management is ideal for:

- Early to mid-career business professionals looking to transition into the industry who are interfacing with cyber teams or with cyber risks.
- Early to mid-career governance, risk, and compliance professionals looking to upskill and future-proof their career by taking advantage of growth in the cyber security industry.

KEY DETAILS

Duration:
9 months full time, 12 months part time. Expect 10–12 hours study per week, with each term comprising of 10 weeks.

Price:
$3,960 per course, $15,840 in total.*

*Plus a capped Student Services and Amenities Fee (SSAF) based on your credit point enrolment load.

FEE-HELP and other financial support may be available. Fees typically increase each year and may change without notice. Total fees are estimates and should only be used as a guide.

Prerequisites / level of study:
An Australian Bachelor degree or equivalent, or higher-level qualification, from a recognised tertiary institution plus 2 years relevant work experience, or at least 5 years continuous full-time experience working in business, information systems, or cyber security. These applicants will be required to submit a curriculum vitae (CV).

Enrolment:
Scheduled intakes are in January, April, July, and September.

Why study Cyber Security Governance and Risk Management?

Our Graduate Certificate in Cyber Security Governance and Risk Management, developed in collaboration with RMIT's Cyber Security Research and Innovation Centre, will equip you with the skills to develop and advise on cyber security risk and governance strategies.

You'll design and apply governance, compliance, and resilience frameworks, and learn how to respond to incidents and manage security governance teams, processes, and projects. You'll also gain the capabilities to interface with technical cyber teams across all levels of an organisation's hierarchy.

At RMIT Online, we have a suite of courses to provide you with the skills to tackle the world of cyber security.

- Our **Cyber Security Risk and Strategy** short course is designed for those looking to gain a foundational understanding of cyber security.
- For a more advanced understanding, our **Graduate Certificate in Cyber Security** will provide you with the technical skills to prepare yourself for an analyst role in the industry.
- Our **Graduate Certificate in Cyber Security Governance and Risk Management** explores governance and risk frameworks and strategies for you to successfully identify and mitigate a cyber attack and work effectively with cyber teams.

Australia's cyber security sector is **forecasted to 3x its revenue** over the coming decade due to increased demand for cyber security products and services

(AUSTRALIAN CYBER INDUSTRY ROADMAP, CSIRO, 2020)

By 2026, there are expected to be **31,600 cyber professionals in the workforce**, an increase from 19,500 in 2017.

(AUSTRALIAN CYBER INDUSTRY ROADMAP, CSIRO, 2020)

Choosing the right course for you

	FUTURE SKILLS SHORT COURSE (6 WEEKS)	POSTGRADUATE (9-12 MONTHS)	POSTGRADUATE (9-12 MONTHS)
	Cyber Security Risk and Strategy	Graduate Certificate in Cyber Security	Graduate Certificate in Cyber Security Governance and Risk Management
Objective	Providing a foundation in cyber security, learn how to formulate a cyber strategy for organisations to respond to incidents efficiently, limit damages caused, and recover information from any attacks experienced.	Develop a technical understanding of cyber security fundamentals and programming and prepare for a technical role in the industry.	Further develop business skills in information security fundamentals, governance, risk, and legislative requirements, and developing organisational strategies for cyber management.
Who this course is for	• Mid-senior managers looking to gain skills to implement a cyber strategy into their organisation • Consultants, IT professionals and entrepreneurs, who want to instill cyber practices into their teams or businesses	Ideal for students looking to be introduced to the technical skills and gain experience in order to transition into a career within cyber security. Areas you'll work in, but are not limited to are: Law, Marketing, Finance, Business. Healthcare, IT, Science, and Engineering.	• Early to mid-career business professionals looking to transition into the industry who interface with cyber teams or cyber risks • Early to mid-career governance, risk, and compliance professionals looking to take advantage of growth in the cyber security industry
What you'll learn	• Understand the fundamentals of cyber security risk • Comprehend why cyber security is important • Apply a cyber security risk mitigation strategy to your organisation • Communicate cyber security strategy to team members and organisational wide stakeholder engagement • Understand the commercial impacts of cyber security risk	• Demonstrate a strategic overview of complex issues in cyber security • Develop communication skills to engage effectively with technical and non-technical audiences • Demonstrate an ability to appreciate the ethical considerations that inform judgments and decision making • Work autonomously and effectively within a team	• Apply cybersecurity strategies, policies, and organisational structure to protect business information assets • Apply a risk management approaches to assess and quantify organisational exposure to cyber risk • Critically evaluate key legal, regulatory and compliance frameworks for application to organisational needs in cyber security risk management • Analyse cybersecurity governance frameworks and standards to assess security maturity in business contexts • Evaluate and develop cybersecurity program, security metrics and reporting in cybersecurity governance
Course outcome	With access to a specialised lab, you'll get hands-on with the tools and create your own cyber security strategy by the end of this course.	With a strong career focus, you'll also be exposed to thought leadership from a range of cyber security professionals and complete mock job applications.	You'll graduate equipped to develop, analyse and evaluate cyber security impacts, risks, practices, compliance frameworks and governance strategies and solutions for organisational settings.

Why study with RMIT Online?

Flexible online learning

The freedom of learning online means you can study, whenever and wherever you want.

Real world skills

Our project-based assessments mean you'll roll up your sleeves and create a project for real a world business scenario, allowing you see the immediate impact of your learning within your organisation.

Full time support

Our expert team of support advisors along with academic tutors and course coordinators are the best at what they do and are here to support you every step of the way.

Industry connected

We combine the forces of a leading technology university with high profile industry partners to ensure you're job ready, learning practical skills that align with industry best practice.

Propel your career

Online postgraduate programs receive the same qualification as on-campus – without putting your life on hold.

Future focused

With up to the minute content, RMIT Online courses are shaped by future of work needs, ensuring that you acquire the latest industry relevant skills for today's in-demand jobs.

Prerequisites

English language requirements

You must meet the University's minimum English language requirements to be eligible for a place in this program.

If you are a local student, refer to the English requirements for postgraduate coursework programs.

If you are an international student, refer to the English requirements and equivalency information. The program requires a minimum overall score of 6.5 with no band less than 6.0 in IELTS (Academic).

Australian student visas

RMIT Online's Graduate Certificate in Cyber Security Governance and Risk Management does not meet Australian student visa requirements. For an Australian student visa, you must have an on-campus place in a program of study. For more details on RMIT's on-campus programs visit rmit.edu.au

Entrance requirements

You must have completed an Australian bachelor degree or equivalent, or higher-level qualification, from a recognised tertiary institution plus two (2) years relevant work experience.

If you do not have these academic qualifications, you may be eligible for entrance into this program if you have at least 5 years continuous full-time experience working in business, information systems, or cyber security.

To have your professional experience considered, as part of your application you must submit a curriculum vitae (CV), and a statement that details your experience.

Credit pathways

At RMIT Online, we're committed to supporting your lifelong learning journey. Upon successful completion of the Graduate Certificate in Cyber Security Governance & Risk Management (GC196) you will be eligible to continue your studies in RMIT Online's Master of Business Administration (MBA) (MC199) with 48 credit points (4 courses) worth of credit.

Program overview

As part of your studies, you'll undertake three core courses in the program, before choosing an elective subject that can be aligned to your desired learning outcomes.

Students of this program are eligible to apply for work experience placements with the Australian Defence Force Cyber Gap Program. In order to apply, you must be studying an eligible 12-month program. Further details can be found **here**.

Our Graduate Certificate in Cyber Security Governance and Risk Management will provide you with the business skills to develop and advise on cyber security governance strategies. If you're looking for a technical understanding of cyber security, we recommend you undertake our Graduate Certificate in Cyber Security.

Program courses

01	Fundamentals of Cyber Security*
02	Cyber Security Governance, Risk and Compliance Management
03	Cyber Security Resilience and Incident Management
04	Electives

* We recommend that to complete this program, you undertake Fundamentals of Cyber Security first, before completing the remaining two core subjects and the elective.

What you'll learn

- Apply cybersecurity strategies, policies, and organisational structure to protect business information assets.
- Apply a risk management approaches to assess and quantify organisational exposure to cyber risk.
- Critically evaluate key legal, regulatory and compliance frameworks for application to organisational needs in cyber security risk management.
- Analyse cybersecurity governance frameworks and standards to assess security maturity in business contexts.
- Evaluate and develop cybersecurity program, security metrics and reporting in cybersecurity governance.

PROGRAM COURSE 01

Fundamentals of Cyber Security

Course overview

This course is critical to understanding the complexity and nuances of cyber security as a technical discipline, and adequately interact with technical cyber security teams. This foundational course in Cyber Security will enable you to apply key concepts to cyber defence, identity and access management, network, communications and infrastructure security.

This course explores key concepts, principles and practices of cyber security. It will introduce you to security, concepts, and key security principles. You will develop insights into the types, anatomy and stages of cyber attacks with an overview of security tools and cyber defences. You will also be introduced to approaches to identity and access management (IdAM), network security concepts, applications and infrastructure security. Finally, you will engage with emerging cyber security issues.

Learning outcomes

- Analyse organisational drivers and business objectives to identify, prioritise and plan cyber security needs.
- Analyse key cyber security principles using cyber security tools, controls, and cyber defences.
- Critically evaluate security controls around identity and access management, network and communications security, applications and infrastructure security to identify vulnerabilities and propose defensive strategies against cyber threats.
- Formulate strategic advice and recommendations to implement security controls that adopt a risk-based approach and meet organisational strategy and business needs

Assessments

- Cyber threat identification plan including threat matrix plan
- Cyber vulnerability assessment and defense strategies report
- Cyber security proposal and presentation

PROGRAM COURSE 02

Cyber Security Governance, Risk and Compliance Management

Course overview

Understanding cyber security governance and risk is crucial to developing and maintaining cyber security in organisations in an age of increasing cyber threats and attacks. Cyber security governance enables organisations to develop and formulate strategies for risk and compliance management, and to respond to cyber security threats in an orderly and efficient manner.

This course builds the understanding of cyber security governance, risk and compliance (GRC) requirements and explores current and emerging cyber security GRC management practices and processes. You will evaluate risk management concepts, principles and key legal, regulatory and compliance frameworks for application in organisational contexts. You will assess and quantify cyber security risks and apply modelling to evaluate threats, and vulnerabilities. You will also develop risk mitigation strategies, policies, standards and procedures for risk metrics, operational management and board reporting.

Learning outcomes

- Analyse the concept of governance, principles of risk and compliance management in a cyber security context
- Apply a risk management approach to assess and quantify organisational exposure to cyber risk
- Critically evaluate risk management concepts, principles and key legal, regulatory and compliance frameworks for application to organisational needs in cyber security risk management
- Apply policies, standards and procedures and develop risk mitigation strategies for risk metrics and board reporting

Assessments:

- Complete a 1500 research report
- Complete a 2000 word prioritised threat matrix and risk assessment report
- Submit a risk mitigation report

Prerequisite: ISYS3442 Fundamentals of Cyber Security

PROGRAM COURSE 03

Cyber Security Resilience and Incident Management

Course overview

Developing cyber security resilience and the capability to manage security incidents is an increasingly urgent challenge for organisations operating in global digital environments.

This course explores current practices in cyber security resilience as a component of organisational management. You will develop insights and strategies to align cyber security management with organisational needs: assessing organisational cyber security maturity, incident management approaches, and crisis communication. You will also develop a strategic approach to the development of a security culture and awareness in an organisation, in the use of asset, resource and records management, roles and responsibilities for organisational cyber resilience (e.g. response), cyber security audits, and business continuity process and planning.

Learning outcomes

- Critically analyse organisational cyber security maturity in relation to cyber resilience and incident management
- Analyse asset and resource management practices to develop business continuity process and planning approaches
- Formulate strategic advice to promote and nurture a security culture and awareness in an organisation
- Develop an incident management response policy and plan

Assessments:

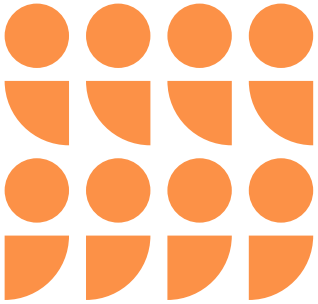
- Cyber security assessment
- Develop a security culture and awareness report
- Post-incident analysis and recommendations

Prerequisite: ISYS3442 Fundamentals of Cyber Security

PROGRAM COURSE 04

Elective bundles

For this course, choose one from the following three courses:



COURSE OPTION 1

Data and Privacy in the Digital Age

In this course, you will develop an advanced understanding of the key principles of Australian and international privacy laws. You will comprehend the value of personal and commercial data in an increasingly connected world and examine the obligations of organisations in relation to the collection, storage and use of customer data.

You'll critically examine the legal, security and privacy issues that arise from the collection, storage and usage of such data and examine the response required from organisations in the event of a data breach. The ethical, social and regulatory implications of key privacy and data topics will be examined, while technology solutions for greater transparency, privacy and security will be explored.

COURSE OPTION 2

Digital Leadership & Digital Delivery with Agile

The digital leadership component will expose you to the leadership practices and mindsets required to build successful customer relationships and customer success teams. During this course, you will be introduced to a range of leadership frameworks and models, particularly within fast changing digital environments. You will gain an appreciation of evolving workforce needs and associated impacts on leadership practice, and how different leadership approaches can help address these challenges.

The agile delivery component will enable you to understand the depth and breadth of agile frameworks, methods, tools and techniques. You will learn how to select, blend and apply these broadly across business domains, helping people understand the benefits of focused work, identifying problems early, adapting to change, delivering early and often and the value of face-to-face communications.

COURSE OPTION 3

Law and Policy for Emerging Technologies

This course examines the emergence of new technologies and business models over the past decade and the impact that they have had on society, ethics, law, regulation and policy.

You will dissect the pressures emerging technologies place on current regulatory approaches and frameworks. Traditional approaches to regulation and policy development and key examples of current regulation will be examined. You will study a range of theories and approaches to developing fit-for-purpose regulation, and be equipped with the skills and knowledge to develop policy and regulation that can keep pace with technological change.

Why study online

Being 100% online, get 24/7 on demand access to the course content, ensuring you don't have to reduce your work or compromise your lifestyle.

Become industry connected as you learn from renowned academics with extensive industry experience. Our courses are designed with industry partners to ensure what you learn is up to date and aligns with best practice.

Get hands on through structured activities and build out your project portfolio to demonstrate your knowledge and practical skills.

Get personalised support that keeps you motivated on the road to success. Your support team includes the Student Success advisors who'll give you one-on-one assistance, an Online Facilitator, and a Course Coordinator.

Graduate with a globally recognised degree.

Who’s supporting you

RMIT Online works with leading experts at the forefront of their fields, multiplying the force of industry with a world-leading university.
By studying with RMIT Online, you can be sure you will be levelling up your skills and qualifications through work-connected, relevant learning.

INDUSTRY PARTNERS:

IBM is a leading cloud platform and cognitive solutions company. With over a century worth of history, IBM operates in a range of branches including machine learning, cloud and IT infrastructure, security, consulting services, and research.

Palo Alto Networks is a global cybersecurity company enabling teams and businesses to prevent cyberattacks with an automated approach that delivers consistent security across cloud, networks, and mobile devices.

Dr Aida Ghalebeigi,
Program Manager

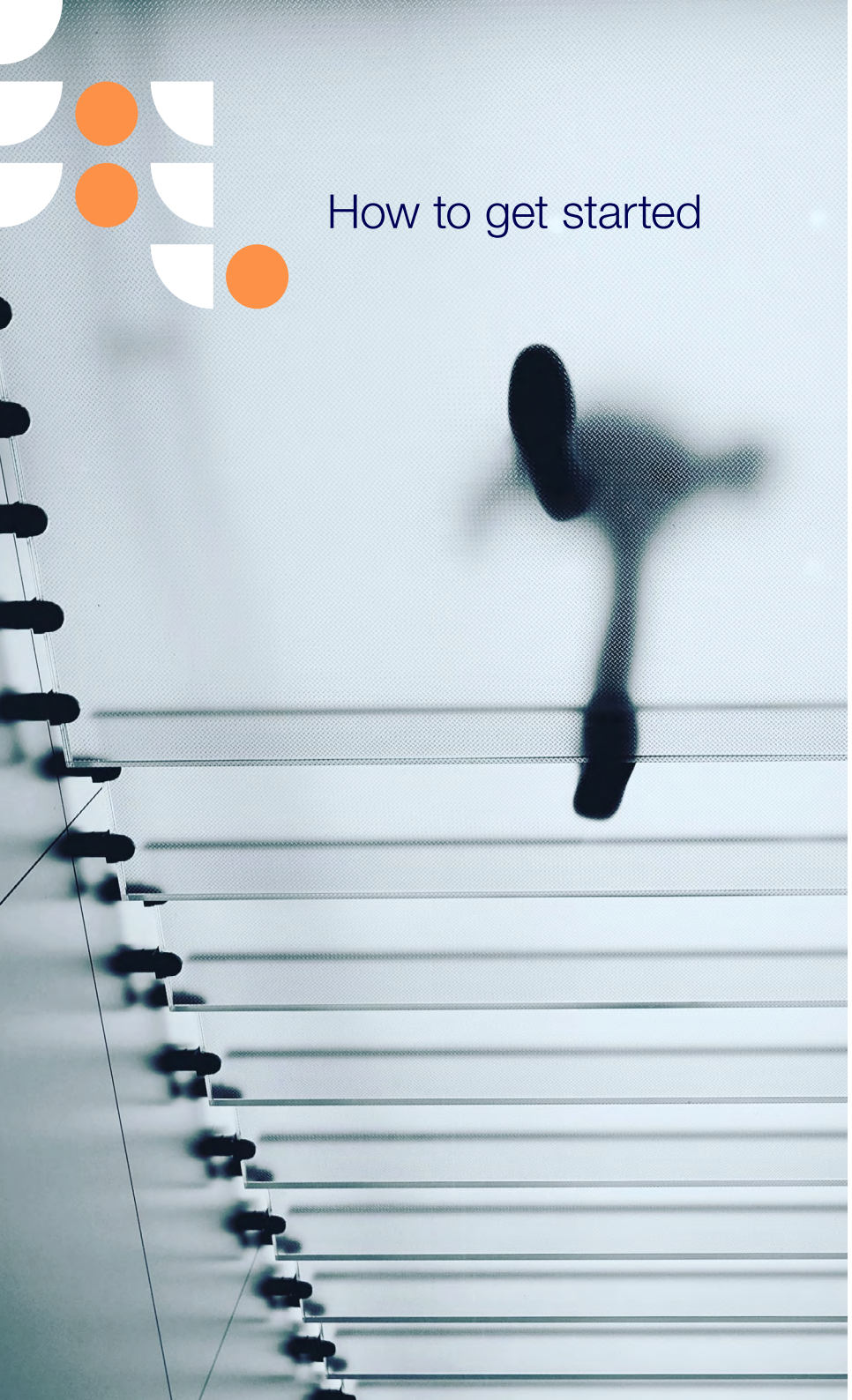
Dr Aida Ghalebeigi is the Program Manager for online programs in the School of Accounting, Information Systems, and Supply Chain. Aida has taught and developed courses online and face-to-face for both offshore and onshore programs, across undergraduate and postgraduate levels. In her research, she investigates gender equality in the workplace, especially in male-dominant industry sectors. Aida is continuously engaged with industry to design and create authentic learning experiences.

Matt Warren
Subject matter expert

Matt Warren is the Director of the RMIT Centre of Cyber Security Research and Innovation and a Professor of Cyber Security at RMIT University, Australia. Professor Warren is a researcher in the areas of Cyber Security and Computer Ethics.

Student success team, RMIT Online

Our student success team are here to help you with 1:1 coaching, tips on how to successfully study online, and any questions or concerns you may have.



How to get started

Enrolment in our graduate certificate is easy. Get in touch with one of our Student Enrolment Advisors today and we can get the wheels moving.

STEP 1 Chat to a Student Enrolment Advisor

Our Student Enrolment Advisor have all the information you will need to choose the best course for you. They can even coach you through the enrolment process over the phone. You can call our Student Enrolment Advisor during business hours on 1300 145 032. They'll be able to help with any questions regarding the application process, RMIT course fees, and how online study works.

STEP 2 Send us your documents

All you have to do is fill out and submit the relevant course application forms. Your RMIT Course Consultant can guide you through this process. It doesn't take more than a few minutes.

STEP 3 Wait to hear from us!

If there are any extra steps necessary, your Student Enrolment Advisor will let you know. Once you're enrolled, you'll also be able to access your course details via our Student Portal. For more information, visit **online.rmit.edu.au**

*Further information: Every effort has been made to ensure the information contained in this publication is accurate and current at the date of publishing. For the most up-to-date information, please refer to the RMIT Online website before lodging your application.

RMIT Online