| **Course Title** | **MSc Cyber Security Management** |
|---|---|
| Final Award | MSc Cyber Security Management |
| Interim Awards | Postgraduate Certificate in Cyber Security Management<br>Postgraduate Diploma in Cyber Security Management |
| Awarding Body | Ravensbourne University London |
| Teaching Institution | Ravensbourne University London |
| HECOS code (with Subject percentage Splits if applicable) | |
| QAA Subject Benchmark | Business and Management |
| External Accrediting Bodies | N/A |
| Apprenticeship Standard used to inform the development of the course (if applicable) | N/A |
| Accelerated Degree Option | N/A |
| Study Load | Full time and part time |
| Mode of study | 1 year Full Time, 2 years part time |
| Delivery Location(s) | Ravensbourne University London |
| Length(s) of Course(s) | 1 year Full Time, 2 years part time |
| Type (open/closed) | Open |
| Validation period | 5 years |
| Intended First Cohort Start Date | January 2024 |
| Date produced/amended | November 2023 |
| Course Leader | Dinesh Mothi |
| Course Development Team Members | Faisal Mustafa, Ajaz Ali, Philip Tokmark, Guido Dal Pozzo, Dinesh Mothi, Catherine Bedwei-Majdoub, Samantha Sandilands, |
| Course Administrative Contact | Charles Mullany |

**Course Description**

In an era dominated by digital innovation, creative industries are rapidly adopting the new technologies. The importance of securing sensitive information and systems from cyber threats has never been more critical for such industries. The demand for professionals who can navigate the complex landscape of Cyber Security and manage robust defence mechanisms is on the rise in all sectors.

The MSc Cyber Security Management is a taught Masters course which is designed to equip students with advanced Cyber Security Management skills. The course addresses the needs of a wide range of industries, including the media and creative arts. The course is designed to meet the demands of a wider audience whilst maintaining a strong alignment with Ravensbourne's ethos of creativity, innovation, and hands-on learning.

This course is informed by various frameworks from IT governance, UK Cyber Security Council, and CyBOK knowledge areas within the Human, Organisational and Regulatory aspects, which are widely recognised as leading practices in Cyber Security Management. Additionally, candidate will gain insights into the governance framework of Cyber Security Management and acquire skills to handle associated risks.

Through a blend of theoretical knowledge and practical applications, students will gain the expertise required to lead successful Cyber Security Management projects. The MSc Cyber Security Management course consists of 6 core modules and a final dissertation or project. The total credit value of the course is 180 credits, with each core module worth 20 credits and Final Project / Dissertation worth 60 credits.

The course offers an opportunity to develop skills in Cyber Security Risk Management, Strategic Cyber Security Management and Financial Aspects of Cyber Security. Cyber Security Management is a discipline which can be applied to Social Mobility, Government and non-government sectors, manufacturing, construction and any area related to creative art and media such as Fashion, Television and Film Production and Broadcasting to name a few.

Through a series of shared units with other postgraduate courses, the students are encouraged to expand their own practice by examining how the course intersects with other disciplines and how, from this intersection, innovative ideas emerge.

During this course, the emphasis is on practical applications and hands-on experiences, enabling students to develop required skills for their employability. Industry experts and practitioners will be involved in guest lectures and mentoring schemes to provide valuable insights into the various sectors such as finance, media, creative arts etc.

**Career Opportunities**
Upon successful completion of the MSc Cyber Security Management course, graduates will be able to pursue various career paths including setting up their own consultancy, working as a Cyber Security Manager, Director of Cyber `security or C-Level Executive.

| Course Aims |
| --- |
| • Provide students with a comprehensive understanding of Cyber Security Management principles, methodologies, and best practices within creative industries. |
| • Equip students with the knowledge and skills to protect intellectual property, digital content, and creative assets from cyber threats. |
| • Enable students to develop critical thinking, problem-solving, and decision-making skills necessary for effective Cyber Security Management. |
| • Encourage students to implement Cyber Security measures that support a culture of innovation, allowing for experimentation and creative exploration |
| • Foster leadership, communication, and teamwork abilities to manage diverse Cyber Security teams and stakeholders. |
| • Cultivate ethical, sustainable, and innovative approaches to Cyber Security management activities. |
| • Encourage students to apply theoretical concepts to real-world Cyber Security projects through practical assignments and industry placements.2 |
| • Develop effective leadership skills and practices in Cyber Security management, including the ability to inspire and motivate team members, resolve conflicts, and guide the Cyber Security towards successful completion. |
| • Develop and implement Cyber Security management strategies that leverage technologies to drive sustainable practices, reduce environmental impact, and enhance organizational resilience |
| • Develop a user-centric approach to Cyber Security, emphasising the importance of security awareness and training tailored to the unique needs of creative professionals. |
| • Prepare students to build resilient creative workflows that can withstand and recover from cyber incidents without compromising project timelines. |

**Course Learning Outcomes**

| The course provides opportunities for students to develop and demonstrate knowledge and understanding, qualities, skills and other attributes in the following areas.<br>On completion of the MSc Cyber Security Management students will be able to: | |
|---|---|
| **Explore** | Select, apply and evaluate requirements gathering techniques, demonstrating a mastery in using a wide range of sources, providing visual, contextual case-study research as appropriate, and demonstrating and applying knowledge and understanding. |
| **Create** | Synthesise and demonstrate advanced research and practice in Cyber Security Management and recommend pathways towards implementation. Students will have the skills to validate their judgement using the most appropriate medium for successful execution of Cyber Security projects. |
| **Influence** | Develop a coherent narrative around their work and Cyber Security project, developing and demonstrating techniques of communication. Students will develop and demonstrate their expertise to instigate, manage and record/reflect on the issues around and affecting a chosen area of research or practice, applying both knowledge and understanding. |
| **Integrate** | Demonstrate how critical perspectives can be developed on Cyber Security Management research. Students will explore, apply knowledge and understanding of the desired outcomes across a range of appropriate processes, media, materials, and organisational models. |

| Where a student does not complete the full course, but exits with a Postgraduate Diploma, they will have had the opportunity to develop and demonstrate knowledge and understanding, qualities, skills and other attributes in the following areas.<br><br>On completion of the Postgraduate Diploma in Cyber Security Management students will be able to: | |
|---|---|
| **Explore** | Select appropriate information gathering techniques, using a range of sources, providing visual, contextual case-study research as appropriate, and demonstrating and applying advanced knowledge and understanding. |
| **Create** | Synthesise research and practice in Cyber Security Management, and identify possible pathways towards implementation. Students will have the skills to validate the development of their judgement in using the most appropriate medium for successful delivery to the marketplace. |
| **Influence** | Develop a considered narrative around their work and Cyber Security Management modules, developing and demonstrating techniques of communication. Students will develop their ability to manage and record/reflect on the issues around and affecting a particular area of research or practice, applying both knowledge and understanding. |
| **Integrate** | Students will explore risk, testing, prototyping and evaluation in order to determine, improve and apply knowledge and understanding of the desired outcomes across a range of appropriate processes, media, materials, and organisational models. |

| Where a student does not complete the full course, but exits with a Postgraduate Certificate, they will have had the opportunity to develop and demonstrate knowledge and understanding, qualities, skills and other attributes in the following areas.<br><br>On completion of a Postgraduate Certificate in Cyber Security Management students will be able to: | |
|---|---|
| **Explore** | Select appropriate information gathering techniques, using a range of sources, providing visual, contextual case-study research as appropriate, and demonstrating knowledge and understanding. |
| **Create** | Synthesise research and practice in Cyber Security Management and identify possible pathways towards implementation. Students will have the skills to attempt to validate the development of their judgement in using the most appropriate medium for delivery to the marketplace. |
| **Influence** | Develop a narrative around their work and Cyber Security Management, developing techniques of communication. Students will develop their ability to manage and record/reflect on the issues around and affecting a particular area of research or practice, applying both knowledge and understanding. |
| **Integrate** | Students will explore risk, testing, prototyping and evaluation in order to determine, improve and apply knowledge and understanding of the desired outcomes across a range of appropriate processes, media, materials, and organisational models. |

| Ravensbourne University Assessment Criteria | |
|---|---|
| **Explore** | Research and Analysis<br>Subject Knowledge<br>Critical Thinking and Reflection<br>Problem Solving |
| **Create** | Ideation<br>Experimentation<br>Technical Competence<br>Communication and Presentation |
| **Influence** | Social Impact<br>Ethical Impact<br>Environmental Impact |
| **Integrate** | Collaboration<br>Entrepreneurship and Enterprise<br>Professional Develpoment |

**Core Competencies**

Each module learning outcome should be aligned to at least one competency.

| Competency | Definition | Aligned Assessment Criteria |
|---|---|---|
| **Cognitive** | The ability to acquire, retain and use knowledge, recognise, pose and solve problems. Attributes may include:<br>• Evaluate their own beliefs, biases and assumptions such as waterfall over agile.<br>• Evaluate strengths, weaknesses, and fallacies of logic in arguments and information<br>• Apply lesson learned , acquired knowledge and skills to new situations<br>• Perform basic computations or approach practical problems by choosing appropriately from a variety of mathematical techniques<br>• Earned Value Analysis<br>• Devise and defend a logical hypothesis to explain planned vs observed phenomenon<br>• Recognise a problem and devise and implement a plan of action | **Explore, Create, Integrate, Influence** |
| **Creative** | The ability to generate new ideas, express themselves creatively, innovate and/ or solve complex problems in an original way. | **Create** |
| **Professional** | The ability to understand and effectively meet the expectations of industry partners, through outputs and behaviours. | **Integrate, Influence** |
| | | |

| | | |
|---|---|---|
| **Emotional, Social and Physical** | Emotional -The intrapersonal ability to identify, assess, and regulate one's own emotions and moods; to discriminate among them and to use this information to guide one's thinking and actions and where one has to make consequential decisions for oneself. Attributes may include:<br><br>• Self-awareness & regulation (including metacognition)<br>• Mindfulness<br>• Cognitive flexibility<br>• Emotional resilience<br>• Motivation<br>• Ethical decision- making<br><br>Social - The interpersonal ability to identify & understand the underlying emotions of individuals and groups, enhancing communication efficacy, empathy and influence. Attributes may include:<br><br>• Managing your audience<br>• Coordinating with others<br>• Negotiation<br>• Creativity<br>• People management<br>• Leadership & entrepreneurship<br>• Service orientation<br>• Active listening<br>• Coaching and mentoring<br><br>Physical - The ability to perceive and optimise physiological activity and responses to influence emotion, solve problems or otherwise effect behaviour. Physical intelligence engages the body to train neuron pathways to help change an inappropriate response to an appropriate response. Attributes may include<br><br>• Self-discipline & management<br>• Attention<br>• Reaction & response time<br>• Cognitive & muscle memory | **Explore, Influence, Integrate** |

| | | |
|---|---|---|
| | • Managing stress<br>• Physical resilience | |
| **Cultural** | The capability to relate to and work effectively across cultures including intercultural engagement, cultural understanding and intercultural communication. | **Influence, Integrate** |
| **Enterprise and Entrepreneurial** | The generation and application of ideas within a practical setting. It combines creativity, idea generation and design thinking, with problem identification, problem solving, and innovation followed by practical action. This can, but does not exclusively, lead to venture creation (UK Quality Assurance Agency, Enterprise and Entrepreneurship Education 2018). | **Create, Influence, Integrate** |
| **Digital** | The confident adoption of applications, new devices, software and services and the ability to stay up to date with ICT as it evolves. The ability to deal with failures and problems of ICT and to design and implement solutions (Jisc Digital Capabilities Framework) | **Explore, Create, Integrate, Influence** |
| **Ravensbourne Return** | Engagement with inhouse activities including mentoring other students, volunteering, acting as a student rep or ambassador.<br>Demonstrate a knowledge of current events and social issues<br>Identify their personal convictions and explore options for putting these convictions into practice<br>Engagement with the external community through (from) employment, volunteering, participation in a Professional Life or other course-based Cyber Security. | **Explore, Create, Influence, Integrate,** |

**Learning, Teaching and Assessment**

| Learning and Teaching methods | Assessment Strategy |
|---|---|
| A variety of learning methods and technologies are employed across all units. They include: Briefings, Lectures, Cyber Security workshops, Tutorials, Seminars, Group work, Field Trips, Online activity, Individual Presentations and critiques, Group presentations, and self-directed independent study.<br><br>Although you are individually assessed, you may also work in teams and collaborate with external partners and students from other courses. These collaborations, which will be supported by your course tutor, can stimulate a powerful mix of individual, team-based and interdisciplinary approaches to your understanding of the parameters of professional practice.<br><br>The course is underpinned by a mentoring scheme and throughout each unit students will be provided with the opportunity to have regular meetings and touchpoints with their course tutor and an industry expert.<br><br>There are several mechanisms for evaluating the effectiveness of learning methods including unit evaluation, staff student meetings, and personal progress reviews. | A variety of assessment methods are employed across all units. They include formative and summative assessments which may include presentations, portfolios, learning journals, reports, peer assessment and external reviews. These methods encourage you to critically reflect on and build your learning and progress.<br><br>Formative feedback is given at the end of each term and students will receive ongoing advice and guidance (feed forward) alongside a critique against learning outcomes and assessment criteria. At the end of the unit summative assessment will provide conclusive feedback in response to an online submission of the assessment requirements for the modular units for this course. |

**Course Structure**

| Module Code | Module Title | Shared Module | Mandatory / Elective | Credits |
|---|---|---|---|---|
| Level 7 | | | | |
| CYM23701 | Cyber Security Principles | No | Mandatory | 20 |
| CYM23705 | Strategic Cyber Security Management | No | Mandatory | 20 |
| CYM23704 | Financial Management for Cyber Security | No | Mandatory | 20 |
| CYM23702 | Cyber Security Risk Management | No | Mandatory | 20 |
| CYM23703 | Principles of Project Management | Yes | Mandatory | 20 |
| CYM23706 | Research Methods and Creative Thinking | Yes | Mandatory | 20 |
| CYM23707 | Dissertation /Cyber Security Management project | Yes | Mandatory | 60 |
| | | | | **180** |

**Learning Hours**

| **Learning Hours (per 20 credit module)** | | | |
|---|---|---|---|
| **Staff – Student Contact Hours** | | **Independent Study Hours** | |
| Formal Scheduled Teaching | 36 | Independent Study | 164 |
| **Total** | | | 200 |

## Course Regulations

### Entry Requirements

A minimum Lower Second-Class honours degree (or equivalent non-UK qualifications) in a relevant subject, or an equivalent professional qualification in a related discipline.

If you are applying directly from an undergraduate degree course without experience or professional practice you must be able to demonstrate a good knowledge of your chosen subject area.

In order to be eligible for a course, you will need to be a competent speaker and writer of English. This also applies if you are from the European Union, or if you are from a country outside the EU. You need to provide us with an IELTS or equivalent English language qualification demonstrating 6.0 overall with minimum 5.5 or CEFR Level B2 in each component.

### Accreditation of Prior Learning (if applicable)

Applications are welcomed from those who may not possess formal entry qualifications, mature students, those with work experience or with qualifications other than those listed above. Such applicants should demonstrate sufficient aptitude and potential to complete the course successfully. Applicants will be assessed at interview in accordance with Ravensbourne's Accreditation of Prior Learning Policy and Procedure.

APL will be applied on individual basis and candidates with proven experience and track record in Cyber Security Management may be exempt from 20 to 120 credits. The assessment of the exemptions will be carried out by the Course Leader on case to case basis.

### Conditions for Progression

Students will be deemed to have passed a module if they achieve a 40% for undergraduate students; or a 50% for postgraduate students.

A student who has passed all assessments to date but has not yet reached the end of a level (or stage) will be permitted to proceed into the following term by the Interim Assessment Board.

### Reassessment of Failed Elements

Failure or non-submission in any assessment will result in a Fail grade for the component and module.

A student shall be permitted three attempts at each assessment; one first sit and two resits.

Where a student successfully retrieves an assessment failure, the grade for the assessment will be capped at 40% (undergraduate) or 50% (postgraduate) (except where Extenuating Circumstances have been approved).

**Conditions for the Granting of Awards**

A student who completes an approved course of study, shall be awarded an MSc in Cyber Security Management.

Those students who exit the course without completing it may be entitled to exit with an award of either a:

1. Postgraduate Diploma in Cyber Security Management, provided they complete an approved course of modules and the learning outcomes for such award as set out in the Course Specification.
2. Postgraduate Certificate in Cyber Security Management, provided they complete an approved course of modules and the learning outcomes for such award as set out in the Course Specification.

**Any derogation(s) from the Regulations required?**

**N/A**

| | |
|---|---|
| Student Support | https://www.ravensbourne.ac.uk/student-services |
| Assessment Regulations | https://www.ravensbourne.ac.uk/staff-and-student-policies |

| Course Learning Outcomes | LO1 | LO2 | LO3 | LO4 |
|---|---|---|---|---|
| | | | | |
| Cyber Security Principles | LO1 | LO3 | | |
| Principles of Project Management | LO1, 2, 3, 4, 5 | LO 2, 4, 5 | | LO1, 3, 5 |
| Financial Management for Cyber Security | LO2, 3, 4 | LO 1 | | |
| Cyber Security Risk Management | LO1, 2, 3, 4 | | | |
| Research Methods and Creative Thinking | LO 1, 2, 3, 4 | LO 1, 2, 3, 4 | LO 5 | LO 5 |

| | | | | |
|---|---|---|---|---|
| Dissertation / Major Cyber Security Management Project | LO 1, 5 | LO 2, 3, 6 | | LO 4 |

**Course Diagram**

| Semester 01 | Semester 02 | Semester 03 |
|---|---|---|
| **Cyber Security Principles**<br>20 credits | **Financial Management for Cyber Security**<br><br>20 credits | **Dissertation/Major Cyber Security Management Project**<br>60 credits<br><br>(shared) |
| **Cyber Security Risk Management**<br><br>20 credits | **Strategic Cyber Security Management**<br>20 credits | |
| **Principles of Project Management**<br>20 credits<br>(shared) | **Research Methods and Creative Thinking**<br>20 credits<br>(shared) | |