

PROGRAMME SPECIFICATION

1.	Awarding Institution:	The University of Law
2.	Final Award:	Master of Science in Cyber Security Management
3.	Exit / Intermediate awards	Postgraduate Diploma in Higher Education Postgraduate Certificate in Higher Education
4.	Programme Title(s):	MSc Cyber Security Management
5.	Accredited by:	N/A
6.	Total Credits:	MSc Cyber Security Management – 180 credits Postgraduate Diploma in Higher Education in Cyber Security Management – 120 credits Postgraduate Certificate in Higher Education in Cyber Security Management – 60 credits
7.	Level:	MSc Cyber Security Management – Level 7 within the FHEQ Postgraduate Diploma in Higher Education in Cyber Security Management – Level 7 within the FHEQ Postgraduate Certificate in Higher Education in Cyber Security Management – Level 7 within the FHEQ
8.	Mode of Study:	Face-to-face; Full-Time and Part-Time Online; Full-Time and Part-Time
9.	Language of Study:	English
10.	Length of Programme:	Full-time: 12 months. Part-time: 24 months
11.	Criteria for admission:	2:2 or above from a UK Bachelor's degree, or equivalent qualifications. Non-standard routes:. ROUTE A: • Applicants must possess an undergraduate degree with a grade below that of a 2:2 (3rd or Ordinary); AND EITHER • A professional qualification at level 6 or above from a business professional body, e.g. CIM, CMI, CFA, ACCA, CIMA, CIPD, etc. OR • At least two years of proven professional work experience; ROUTE B: • Applicants must possess a professional qualification at Level 6 or above from a business professional body such as CIM, CMI, CFA, ACCA, CIMA or CIPD;

		<p>AND</p> <ul style="list-style-type: none"> • At least three years of proven professional work experience. <p>ROUTE C: Applicants possess no formal qualifications. Applicants will need to provide 5 years of proven professional managerial work experience along with a professional reference. Applicants may also be required to attend a formal interview.</p> <p>All applications for non-standard entry must be accompanied by a full CV.</p> <p>International Entry Requirements - an English language level equivalent to IELTS 6.5 or above with a minimum of 5.5 in each component.</p>
12.	UCAS code (if relevant):	N/A
13.	HECoS codes (if relevant):	100376 – Computer and Information Security 100755 – Data Management
14.	Date of Production/Revision:	November 2021

15. Aims and Rationale of the Programme

All ULBS Postgraduate degrees are organized into two hubs of programmes; Management Hub and Finance Hub. Programmes within each hub share certain modules, with additional modules that are specific to each programme. The shared modules give students the opportunity to network and liaise with students on other programmes, which they otherwise might not have done, offering invaluable networking opportunities that will benefit them in their work-life. The MSc Cyber Security Management degree is part of the Management Hub. The shared modules within the Management Hub are:

- Global Business Strategy
- Innovation Management in a Digital Age
- Success Through business Ethics

Additionally, all students will share the following two modules:

- Professional Development
- Business Project

The overall objective of master's level business and management degrees is to educate individuals as managers and business specialists, and thus to improve the quality of management as a profession. Master's degrees add value, for example to first (or bachelor's) degrees, by developing in individuals an integrated and critically aware understanding of management and organisations in a global context, and assist them to take effective roles within them.

The aim of this Programme (MSc Cyber Security Management) is to provide graduates with knowledge and understanding of the core aspects of cyber security management being adopted by the industry in the rapidly evolving technological landscape. The programme seeks to adopt a practical approach focussing on providing insights on how these concepts are applied in the industry.

It aims to achieve this goal through the learning experiences, skills and competencies offered which allow for effective managerial behaviour in today's complex organisations and turbulent business environments. Also, the aim of the programme is to educate individuals as cyber security and data science professionals; to address skill shortages in this area and to facilitate career advancement. In particular, the programme provides preparation for and/or development of a career in cyber security and/or data science management, or any management position where the assessment of risk and analysis of data plays a significant role.

The course content emphasises the practical application of cyber security concepts to solve practical problems and focuses on providing insight into how cyber security is implemented, managed and governed by organisations of differing sizes and industry focus. The programme is structured with a significant emphasis upon meeting professional and business development needs as well as enabling professionals and graduates to develop as:

- Professionals with a sound knowledge of the theoretical foundations that apply to modern technology being adopted by the industry. These are fast-evolving areas of specialisation and areas of strategic importance to businesses as they embrace digitalisation and technological change.
- Critically aware learners who can either pursue further studies in Data Science or Cyber Security at a Doctoral level or who wish to complete their professional papers and gain professional experience within that sphere. Some will wish to advance or change their careers or engage in businesses or entrepreneurial ventures.
- Managers and leaders who value lifelong learning so as to equip themselves with the ability to convert theory into practice from a critical and informed perspective so as to advance, in an ethical fashion, the effectiveness of employees and competitiveness of employing organisations.

The programme will share the vision and values associated with the University of Law Business School. Its emphasis on practice-based learning within a realistic, professional, international and contemporary context. Building on the practical nature of learning and high-quality teaching and assessment, links with employers and professional bodies. The aim of the programme with regard to teaching and learning is to produce postgraduates with excellent professional, intellectual and life skills.

The University prides itself on the depth and practical relevance of the knowledge delivered on its programmes and its teaching by academics with practical experience to ensure that research is melded with relevant real-life application. Students will apply these theoretical concepts to real-life case studies and their own workplaces, in a practice-based environment.

16. Programme Outcomes

Knowledge and understanding

Upon successful completion of the programme students should be able to:

- Critically evaluate the current technical language and practices of cyber security; provide integrated solutions in a global business context and a fast pace of change.
- Acquire knowledge about data functions and technologies across industries.
- Understand the distinctiveness and emergence of different technologies and paradigms when it comes to the application of data management techniques for traditional or digital businesses. This would include concepts and practices to do with analytics, and information and technology management.

- Reflect and understand data sources, data models, design, data analysis and implications for data managers businesses with a focus on improving the data experience.
- Develop an understanding of cyber security concepts and its practical application to solve common challenges in securing enterprises across different industry sectors.
- Understanding how to assess cyber security risks across new technologies and develop risk mitigating controls to manage the risks.
- Be familiar with emerging technology trends and the impact on traditional cyber security concepts.

Practice and Skills

Upon completion of the Programme students should be able to:

- Practice, conforming to the ethical expectations of the data management and cyber security profession.
- Engage with and critically view the key debates in data management in organisations and the professions.
- Apply the strategic skills required and operate effectively in the context of digital technologies in complex, changing environments.
- Work independently as well as effective members and /or leaders of teams;
- Develop independent research skills to solve strategically important and complex problems and communicate in an appropriate manner.
- Independently engage with and format appropriate primary and secondary information related to research in data management and cyber security and apply to a significant project or dissertation.
- Acquire technical and communication skills including the ability to present quantitative and qualitative information together with analysis argument and commentary
- Conduct data analysis and evaluation directed at answering specific questions having the ability to choose from a range of available tools and technologies

Relevant Subject Benchmark Statements and other reference points to inform programme outcomes

Subject Benchmark Statements for Master's Degrees in Business and Management, February 2015 (QAA)

The Frameworks for Higher Education Qualifications of UK Degree-Awarding Bodies (2014) The Revised UK Quality Code for Higher Education (QAA) March 2018.

17. Programme Structure, Levels, Modules and Credits

Programme Title – MSc Cyber Security Management	
<i>Module Titles</i>	<i>Credit</i>
Global Business Strategy	15
Innovation Management in a Digital Age	15
Success Through Business Ethics	15
Cyber Security Management & Compliance	15
Cyber Security for Business	15
Data Security	15
Data Design Management	15
Network & Cloud Management	15
Responsibility of Directors	15

Professional Development	Non Credit Bearing
Business Project	45

Students who obtain all the 180 credits from the modules above will receive the MSc in Cyber Security Management award and will achieve all the learning outcomes described in this document.

Students who obtain 120 credits from the modules above will receive the Postgraduate Diploma in Cyber Security Management award, and consequently the learning outcomes described in this document will be achieved just partially, on the basis of the modules passed.

Students who obtain 60 credits from the modules above will receive the Postgraduate Certificate in Cyber Security Management award, and consequently the learning outcomes described in this document will be achieved just partially, on the basis of the modules passed.

18. Programme Outcomes, Learning & Teaching and Assessment Strategies	
<p>A. Knowledge and Understanding</p> <p>Upon successful completion of the programme students should be able to:</p> <ul style="list-style-type: none"> • Critically evaluate the current technical language and practices of cyber security; provide integrated solutions in a global business context and a fast pace of change. • Acquire knowledge about data functions and technologies across industries. • Understand the distinctiveness and emergence of different technologies and paradigms when it comes to the application of data management techniques for traditional or digital businesses. This would include concepts and practices to do with analytics, and information and technology management. • Reflect and understand data sources, data models, design, data analysis and implications for data managers businesses with a focus on improving the data experience. • Develop an understanding of cyber security concepts and its practical application to solve common challenges in securing enterprises across different industry sectors. • Understanding how to assess cyber security risks across new technologies and develop risk mitigating controls to manage the risks. • Be familiar with emerging technology trends and the impact on traditional cyber security concepts. 	<p>Learning and Teaching Methods</p> <p>The learning and teaching methodology will be consciously constructed around ULaw's emphasis on critical practice based learning within a realistic, professional and contemporary context, and will fit with the Business School's agreed approach for teaching and learning sessions to be student led.</p> <p>The programme will also incorporate varied teaching and assessment methods, to the extent where this is useful, but also mindful of the need for students to practice different method of assessment. A balanced approach is achieved across subjects and programmes.</p> <p>Students will be taught by people who have substantial business experience, there will also be guest speakers and involvement from professional bodies.</p> <p>All students will benefit from identification of strengths and learning styles. Where necessary remedial provision will be put in place for numeracy and academic writing. Students will also have access to a personal tutor and reviews of their learning journey.</p> <p>In particular, the delivery of lectures and the student led nature of tutorials and workshops is designed to ensure active participation in the learning process. Methods such as experiential learning, active learning</p>

techniques, directed reading, critical reflection, personal research, applied research encourage engagement by students in their teaching and learning processes. In addition, case study analysis and discussion are used by students to contextualise the learning and the application of models, techniques and concepts.

Knowledge and understanding is developed through the teaching and learning methods outlined above. Each class, whatever its particular format, involves discussion of key issues, practice in applying concepts, both orally and in writing, analysis and interpretation of material, critical evaluation.

The online version of the programme will share the same aims and principles of the face to face version, with the specific approach that it will be delivered remotely through a virtual learning environment where written and multimedia materials will be provided. The modules will be taught by lecturers with a similar profile to the face to face version, while the delivery and access to the faculty will be adapted to the specific requirements of the online format.

Assessment Methods

A wide range of assessment methods will be used across all modules to ensure that programme outcomes can be demonstrated by students. The assessment methods are intended to underpin the learning process. There is both formative and summative feedback. Formative assessment of knowledge and understanding will take place through the regular activities within workshops.

These (both formative and summative) may include group reports, group presentations, individual oral presentations, individual assignments, coursework, project, reflective journals, and portfolio-based assessments. This variety of approaches to assessment supports diversity in learning.

All assessment will test the module and programme learning outcomes and will be designed to align with the relevant FHEQ descriptors.

	For the online version the assessment methods will be the same, and administered remotely.
<p>B. Practice and Skills</p> <p>Upon completion of the Programme students should be able to:</p> <ul style="list-style-type: none"> • Practice, conforming to the ethical expectations of the data management and cyber security profession. • Engage with and critically view the key debates in data management in organisations and the professions. • Apply the strategic skills required and operate effectively in the context of digital technologies in complex, changing environments. • Work independently as well as effective members and /or leaders of teams. • Develop independent research skills to solve strategically important and complex problems and communicate in an appropriate manner. • Independently engage with and format appropriate primary and secondary information related to research in data management and cyber security and apply to a significant project or dissertation. • Acquire technical and communication skills including the ability to present quantitative and qualitative information together with analysis argument and commentary. <p>Conduct data analysis and evaluation directed at answering specific questions having the ability to choose from a range of available tools and technologies.</p>	<p>Learning and Teaching Methods</p> <p>Within the learning model outlined above, the intellectual skills will be primarily developed both in preparation for, and through the activities taking part in, the workshops. Many of the activities will involve the performance of the intellectual skills of analysis, synthesis and the exercise of critical judgment, both individually, and in small groups of between 3-4 students. The length of workshops enables comprehensive feedback to be given.</p> <p>The programme is also designed to provide incremental and demonstrable progression over its duration.</p> <p>Assessment Methods</p> <p>A wide range of assessment methods, both formative and summative, will be used across all modules to ensure that programme outcomes can be demonstrated by students. The assessment methods are intended to underpin the learning process. Formative assessment of knowledge and understanding will take place through the regular activities within workshops. These can be in the form of</p> <ul style="list-style-type: none"> • workshop group activity, where students consider a case-study, issue, or problem, and report on towards the end of the session in an oral presentation • simulations and role-play activities • in-class debates • communication exercises • activities that confirm understanding <p>Other types of formative assessment may take place. Feedback will be given simultaneously and aimed at confirming and assisting students in building their communication, critical thinking and analysis, and problem solving skills.</p>

	<p>Summative assessments of each module will be one of the following:</p> <ul style="list-style-type: none"> • written reports (formative element in the form of lecturer giving guidance on structure and general content) • portfolio, where students compile a portfolio of activities, where they have applied critical analysis and assessment on issues/activities provided by the lecturer • presentation/poster, where students prepare communication piece responding to a brief, constructing a presentation with annotations for further details. <p>This variety of approaches to assessment supports diversity in learning.</p> <p>All assessment will test the module and programme learning outcomes and will be designed to align with the relevant FHEQ descriptors.</p> <p>For the online version the assessment methods will be the same and administered remotely.</p>
--	---

<p>19. Inclusive Considerations</p>	<p>Learning materials (examples, case-studies and other support materials) are sourced from as wide and diverse sources as possible, to reflect the demographics of the student population. Students are actively encouraged to share experiences from their own culture, providing opportunities for comparing and contrasting different behaviours, issues, and solutions. This exposes students to cross-cultural differences and enhances their cultural awareness. Students who appear not to keep up with the pace of the class, are signposted to ULaw’s student support services.</p>
--	---

<p>20. Prior Credits considered for RPL</p>	<p>As per the University’s RPL Policy.</p>
--	--

Document Version Control

Version No.	Amended by	Revision Summary	Date
V1.0	Head of Quality Assurance	First version – programme approval	November 2021