The London Institute of Banking & Finance

MSc Cyber Security

Programme Specification

1. General Information

UCAS Code	Award	Programme Title	Expected Duration	Study Mode
N/A	MSc	Cyber Security	1 year 1.5 years 2 years	Full-time Part-time 1 Part-time 2
		Programme Code		
		UK-LIBF-MACYS		
	Exit Awards	• Postgraduate Diploma • Postgraduate Certificate		

Credit Count	**180 FHEQ credits**
Awarding Institution	The London Institute of Banking & Finance
Teaching Institution	The London Institute of Banking & Finance
Delivery Modes	• Face-to-face • Blended • Online - Synchronous • Online - Asynchronous

Date of original production: November 2023	**Date of current version:** November 2023
Record of modifications:	

2. Programme Overview

Programme Summary

In the ever-evolving digital landscape, the need for professionals who can safeguard sensitive information and systems from cyber threats is paramount. The MSc Cyber Security programme is designed to equip you with the knowledge and skills to identify, prevent, and manage cyber threats, enabling you to safeguard critical information and systems.

The programme's core modules cover a range of topics that provide a comprehensive understanding of cyber security. These include Cyber Risk Assessment and Management, Theoretical Computer Science for IT Security, and Cyber Systems and Network Forensics. The seminar on Advanced Cyber Security and the Master Thesis will allow you to apply your theoretical knowledge to real-world scenarios and manage the complexities of cyber threats in a business context.

In addition to the core modules, the programme offers a range of elective modules, such as Secure Networking, Cryptology, and Secure Software Development. These electives allow you to delve deeper into specific areas of interest and align the programme with your career goals, providing a broader perspective on the field of cyber security.

Upon completion of the MSc Cyber Security programme, you will be well-equipped to pursue a range of careers in diverse business environments. You will have developed critical thinking, problem-solving, and decision-making skills tailored to the cyber security landscape, making you a valuable asset in any organisation.

Programme Aims

The MSc Cyber Security aims to

- develop an in-depth understanding of the theoretical and practical aspects of cyber security, including the principles, techniques, and tools used in the protection of IT systems and networks;
- equip you with advanced skills in identifying, preventing, and mitigating cyber threats in various IT systems and networks;
- provide you with a comprehensive understanding of the legal, ethical, and governance aspects of IT and cyber security;
- enable you to critically analyse current research, concepts, and practices in cyber security, and propose innovative solutions;
- provide you with the knowledge and skills required to protect organisations from cyber threats and breaches; and
- encourage continuous learning and professional development to stay abreast of the latest developments and trends in the rapidly evolving field of cyber security.

Employability & Graduate Outcomes

Graduates of this programme are likely to pursue careers in a number of areas in cyber security and IT-related fields including information security, penetration testing and cyber security analysis. This programme of study supports graduates in developing the following employability skills:

- Digital and technical proficiency
- Critical thinking skills
- Problem-solving skills
- Research skills
- Analytical skills

3. Intended Learning Outcomes of the Programme

This programme has been developed in accordance with the QAA Subject Benchmark Statement for Computing (C) (2022).

Please note: The programme's intended learning outcomes below are described at Master's level (Level 7).

On successful completion of this programme, you will be expected to:

LO1	Demonstrate a critical understanding of the key theories of cyber security, including cyber systems and networks, IT governance, compliance and law and their practical applications in various contexts.
LO2	Demonstrate a critical understanding of the key theories of computer science and cyber security, including proof techniques and mathematical logic.
LO3	Apply formal methods to address cyber threats, including proof techniques for program verification and mathematical logic.
LO4	Critically apply advanced preventive, detective and corrective cyber security controls, risk assessments, and cyber systems and network forensics.
LO5	Critically analyse information on network traffic and cyber system data to identify successful cyber attacks and implement effective cyber security measures.
LO6	Critically analyse key cyber security concepts for confidentiality, integrity, and availability, including authentication, cryptology and identity management, algorithm complexity, and machine and deep learning.
LO7	Critically evaluate concepts of cyber security, cyber attacks, and cyber forensics to address emerging challenges and cyber threats.

LO8	Apply advanced research skills to produce rigorous original empirical and theoretical research by critiquing current research, contribute to the field's body of knowledge, and address complex cyber security issues through systematic investigation and analysis using self-direction.

4. The Structure of the Programme

The MSc Cyber Security programme is offered as a 1-year full-time programme or in part-time mode over a 1.5 or 2-year period. In full-time mode you will complete 5 modules each semester, in part-time 1 mode you will complete 4 modules each semester, and in part-time 2 mode you will complete 3 modules each semester.

The programme is divided into modules which include both compulsory and elective modules weighing 15 credits each and a thesis weighing 45 credits. All modules in the programme are assigned to Level 7.

To achieve the full Master's award, students need to complete modules with a combined weight of 180 credits, including the final thesis.

Table 1: Structure of the Programme

FT	PT 1	PT 2	Module Code	Module Name	Credit	Compulsory/ Elective
Semester 1	Semester 1	Semester 1	LIBFEXDLMIGCR-01_E	Corporate Governance of IT, Compliance, and Law	15	C
			LIBFEXDLMDSAM	Advanced Mathematics	15	C
			LIBFWAWADLMARM	Advanced Research Methods	15	C
		Semester 2	LIBFEXDLMCSECRAM_E	Cyber Risk Assessment and Management	15	C
	Semester 2		LIBFEXDLMCSETCSITS_E	Theoretical Computer Science within the context of IT Security	15	C
Semester 2			LIBFEXDLMCSECSNF_E	Cyber Systems and Network Analysis	15	C
		Semester 3	LIBFOARPDLMCSITSDP	Cyber Security and Data Protection	15	C
			LIBFWAREDLMCSSAITS	Seminar: Advanced Cyber Security	15	C
	Se me		Elective		15	E

		Semester 4	LIBFMTMMTHE	Master Thesis	45	C

Table 2: List of Electives

Module Code	Module Name	Credit	Subject Area
LIBFWAPRDLMCSEPCCCS_E	Project: Current Challenges of Cyber Security	15	n/a
LIBFOARPDLMCSC	Cryptology	15	n/a
LIBFEXDLMIMITSS_E	IT Systems: Software	15	n/a
LIBFEXDLMIMITSH_E	IT Systems: Hardware	15	n/a
LIBFEXDLMCSEEDSO1_E	Secure Software Development	15	n/a
LIBFWAPRPAIECPT	Project: AI Excellence with Creative Prompting Techniques	15	n/a
LIBFIRPFSINTER	Internship[1]	15	n/a

5. Teaching, Learning and Assessment

Information about teaching, learning and assessment can be found in the Teaching, Learning and Assessment Strategy.

Our programmes are designed to:

- integrate theory with practice,
- develop your ability to critique and challenge models and theoretical frameworks,
- stimulate debate, discussion, and research,
- foster a variety of academic skills,
- be accessible and inclusive,
- develop global citizens.

You are expected to undertake a considerable amount of independent study, including reading, industry-related research, and personal reflection.

[1] Check eligibility before booking the module.

Teaching Formats

The programme may be offered in various teaching formats, for example online or via blended learning.

You will have access to both asynchronous and synchronous teaching formats.

Via the Course Feed in the virtual learning environment, myCampus, you will be able to contact the module tutor in a flexible and accessible way.

This is also where Intensive Live Sessions are conducted synchronously with video-based elements. They serve to answer students' individual questions as well as to allow for group discussions.

Additionally, Learning Sprints[2] will offer a seven-week intense learning experience in which the lecturers guide students through the learning material in a very structured manner, with the goal of successfully preparing them to take the final assessment at the end. During this time, frequent synchronous online meetings are held, offering keynote speeches and interactive tasks.

Both the Intensive Live Sessions and Learning Sprints are recorded to further assist asynchronous learning.

In the blended format, teaching and learning combines online and in-person learning in a flipped classroom concept. Traditional classroom activities like lectures are conducted online via the learning platform, while in-class time is used for interactive work. On-campus elements like study groups and library study time complement this approach.

Learning Resources

You will have access to a wide range of resources, which may include the following:

- myCampus: This Moodle-based central information and digital learning platform is organized based on programmes and modules. On the respective module pages in myCampus, you can access all study materials (e.g., course books (i.e., text books), reading lists, practice exams, and video galleries) as well as the links to all related resources and databases (e.g., MS Teams, links to the library for further reading, contact details of lecturers, links to the booking tool for online exams, and the Turnitin submissions page). In the blended model you have access to the same learning platform, with slight adaptations made to accommodate, for example, differences in study sequence.
- Learnhub App: You can access your learning materials in a digital app and have all your notes and highlights synchronised. The app supports different learning formats, such as reading and annotating course books using different colour codes, assessing knowledge with interactive self-tests, or watching the latest videos of the current module.
- Our comprehensive online library is aligned with the study content and kept up to date. Compulsory and further reading is mentioned in the course and module

[2] Offered only when the minimum number of participants is reached.

descriptions available for the students and aims to provide them with unlimited access.

Assessment & Feedback

Regulations relating to progression and assessment, including information on late submissions, are as set out in The London Institute of Banking & Finance's General and Academic Regulations for Students.

Assessment strategies follow The London Institute of Banking & Finance's Higher Education Accessible and Inclusive Learning Policy.

Assessment consists of both formative and summative approaches, and feedback and feedforward are provided as outlined in the London Institute of Banking & Finance's Higher Education Assessing Learning & Feedback Policy. The different types of assessment used by the London Institute of Banking & Finance are described in the Higher Education Types of Summative Assessment Guidance.

Module assessment methods are included in Module Handbooks which are made available in myCampus.

6. Credit and Award

Credit Framework

The MSc Cyber Security is made up of 180 FHEQ credits. One credit approximates to 10 student effort hours; therefore, the total course requires an average of 1,800 hours effort. Typically, one ECTS credit is the equivalent to two UK credits, although this may vary depending on the individual European state's requirements.

Award

On successful completion of the full programme, you will be awarded the MSc Cyber Security.

Regulations

The London Institute of Banking & Finance's General and Academic Regulations for Students detail

- regulations governing the award of credit,
- how grades for awards are granted,
- time limits for completion of programmes of study, and
- capping of marks and regulations relating to the resitting of assessment components
- academic misconduct e.g., malpractice, and

- accreditation of prior learning (APL).

Exit Awards

In line with The London Institute of Banking & Finance's General and Academic Regulations for Students, the following applies:

Postgraduate Certificate (PgCert)	minimum of 60 credits, of which at least 40 credits must be at Level 7
Postgraduate Diploma (PgDip)	minimum of 120 credits, of which at least 90 credits must be at Level 7

Note: The London Institute of Banking & Finance does not award interim qualifications. For example, a student registered for the Master's degree will not automatically be awarded a Postgraduate Diploma or Certificate on completion of the required number of credits.

7. Professional Recognition

Credits gained via accreditation of prior learning (APL) into our awards may mean that students will not get certain exemptions from other institutions' higher education or professional awards that may recognise our programmes.

8. Criteria for Admission

Normally, successful applicants will possess a 2.2 Honours degree (or equivalent) from a recognised institution.

Applicants not possessing this requirement may be considered if they can demonstrate their ability to achieve at this level and contribute to the debates, discussions, and work of the learning set. In this case, applicants may be interviewed and / or required to submit a piece of written work in addition to their application to enable an assessment to be made of their suitability for the programme.

Applicants for whom English is not their first language would be expected to demonstrate their competence through achieving an IELTS score of 6.5 or above with no element below 6.0 (or equivalent). An online English test is offered (SPEEX) if IELTS not available. Alternatively, evidence you have previously studied in English at an appropriate level and at a recognised institution, may be accepted.

9. Benchmarks

External

- QAA UK Quality Code, including:
  - Subject Benchmark Statement for Computing (2022)
  - Level 7 descriptors in the Framework for Higher Education Qualifications in England, Wales and Northern Ireland

- Master's degree characteristics
- The Frameworks for Higher Education Qualifications of UK Degree Awarding Bodies (FHEQ)

Internal

- The London Institute of Banking & Finance Code of Practice
- The London Institute of Banking & Finance General and Academic Regulations for Students

In addition, research with the relevant sector has been undertaken to ensure that the learning outcomes of the programme addresses identified skills and knowledge gaps.

10. Links

Teaching, Learning and Assessment Strategy

The London Institute of Banking & Finance's General and Academic Regulations for Students

The London Institute of Banking & Finance's Code of Practice for Quality Assurance, Chapter 3: Accreditation of Prior Learning (APL)

Accessible and Inclusive Learning Policy

Types of Summative Assessment

Higher Education Assessing Learning & Feedback Policy

Subject Benchmark Statement for Computing

Framework for Higher Education Qualifications in England, Wales and Northern Ireland

Characteristics Statement: Master's Degree

Higher Education Credit Framework for England

11. Curriculum Map of Modules against Intended Learning Outcomes of Programme

Module Code	Module Name	Compulsory / Elective	Programme Learning Outcomes							
			LO1	LO2	LO3	LO4	LO5	LO6	LO7	LO8
LIBFEXDLMIGCR-01_E	Corporate Governance of IT, Compliance, and Law	C	X						X	
LIBFEXDLMDSAM	Advanced Mathematics	C		X			X			
LIBFWAWADLMARM	Advanced Research Methods	C								X
LIBFEXDLMCSECRAM_E	Cyber Risk Assessment and Management	C	X			X		X	X	
LIBFEXDLMCSETCSITS_E	Theoretical Computer Science within the context of IT Security	C		X	X			X		
LIBFEXDLMCSECSNF_E	Cyber Systems and Network Analysis	C	X	X	X	X	X		X	
LIBFOARPDLMCSITSDP	Cyber Security and Data Protection	C	X	X		X	X	X	X	
LIBFWAREDLMCSSAITS	Seminar: Advanced Cyber Security	C	X		X	X	X	X	X	X
LIBFWAPRDLMCSEPCCCS_E	Project: Current Challenges of Cyber Security	E	X			X		X	X	
LIBFOARPDLMCSC	Cryptology	E		X	X	X		X	X	
LIBFEXDLMIMITSS_E	IT Systems: Software	E	X			X	X			
LIBFEXDLMIMITSH_E	IT Systems: Hardware	E	X			X	X			
LIBFEXDLMCSEEDSO1_E	Secure Software Development	E				X		X		

LIBFWAPRPAIECPT	Project: AI Excellence with Creative Prompting Techniques	E					X	X		
LIBFIRPFSINTER	Internship	E				X	X	X	X	X
LIBFMTMMTHE	Master Thesis	C	X	X		X		X	X	X
This table shows the distribution of the programme's intended learning outcomes (as specified in the programme specification) across the programme modules.										

12. Mapping of Teaching Formats and Types of Media used in the Programme Modules

Module Code	Module Name	Compulsory / Elective	Type of Assessment[1]	Teaching Formats[2]			Types of Media[3]					
				CF	ILSE	LS[4]	CB	RL	OT	RB	V	PE
LIBFEXDLMIGCR-01_E	Corporate Governance of IT, Compliance, and Law	C	EX	X	X	X	X	X	X		X	X
LIBFEXDLMDSAM	Advanced Mathematics	C	EX	X	X	X	X	X	X	X	X	X
LIBFWAWADLMARM	Advanced Research Methods	C	WAWA	X	X	X	X	X	X		X	
LIBFEXDLMCSECRAM_E	Cyber Risk Assessment and Management	C	EX	X	X	X	X	X	X		X	X
LIBFEXDLMCSETCSITS_E	Theoretical Computer Science for IT Security	C	EX	X	X	X	X	X	X		X	X
LIBFEXDLMCSECSNF_E	Cyber Systems and Network Forensics	C	EX	X	X	X	X	X	X		X	X
LIBFOARPDLMCSITSDP	Cyber Security and Data Protection	C	OARP	X	X	X	X	X	X		X	
LIBFWAREDLMCSSAITS	Seminar: Advanced Cyber Security	C	WARE	X	X	X						
LIBFWAPRDLMCSEPCCCS_E	Project: Current Challenges of Cyber Security	E	WAPR	X	X	X		X				
LIBFOARPDLMCSC	Cryptology	E	OARP	X	X	X	X	X	X		X	
LIBFEXDLMIMITSS_E	IT Systems: Software	E	EX	X	X	X	X	X	X		X	X
LIBFEXDLMIMITSH_E	IT Systems: Hardware	E	EX	X	X	X	X	X	X		X	X

LIBFEXDLMCSEEDSO1_E	Secure Software Development	E	EX	X	X	X	X	X	X		X	X
LIBFWAPRPAIECPT	Project: AI Excellence with Creative Prompting Techniques	E	WAPR	X	X	X		X				
LIBFIRPFSINTER	Internship	E	IRP	X	X	X						
LIBFMTMMTHE	Master Thesis	C	MT									

This table shows the distribution of teaching formats and types of media used in the programme modules

[1]EX = Exam, WAWA = Written assignment, WACS = Case study, WARE = Research essay, WAPR = Project report, P = Portfolio, AW = Advanced Workbook, OARP = Oral Assignment + Reflection Paper, OPRRP = Oral Project Report + Reflection Paper, IRP = Internship Reflection Paper, BT/MT = Bachelor / Master Thesis

[2]CF = Course Feed, ILSE = Intensive Live Sessions, LS = Learning Sprints

[3]CB = Course Book, RL = Reading List, OT = Online Test, RB = Review Book, V = Videos, PE = Practice Exams

[4]Offered only when the minimum number of participants is reached.