UNIVERSITY OF LONDON

Programme Regulations 2022–2023

Cyber Security

MSc
PGDip
PGCert
Individual modules

Important document – please read
This document contains important information that governs your registration, assessment and programme of study

Contents

Important information regarding the Programme Regulations

Last revised 05 December 2022

As a student registered with the University of London you are governed by the current General Regulations and Programme Regulations associated with your programme of study.

These Programme Regulations are designed and developed by the University of London which is responsible for the academic direction of the programme. The Programme Regulations will provide the detailed rules and guidance for your programme of study.

In addition to Programme Regulations you will have to abide by the General Regulations. These regulations apply to all students registered for a programme of study with the University of London and provide the rules governing registration and assessment on all programmes; they also indicate what you may expect on completion of your programme of study and how you may pursue a complaint, should that be necessary. Programme Regulations should be read in conjunction with the General Regulations.

The relevant General Regulations and the Programme Regulations relating to your registration with us are for the current year and not the year in which you initially registered.

On all matters where the regulations are to be interpreted, or are silent, our decision will be final.

Further information about your programme of study is outlined in the Programme Specification which is available on the relevant Courses page of the website. The Programme Specification gives a broad overview of the structure and content of the programme as well as the learning outcomes students will achieve as they progress.

Terminology

The following language is specific to the Cyber Security programme:

Module: Individual units of the programme are called module. Each module is a self-contained, formally structured learning experience with a coherent and explicit set of learning outcomes and assessment criteria.

Core module: A compulsory 15-credit module that must be taken.

Optional module: A 15-credit module that is chosen from a number of options. This applies solely to students registered on the PGCert or PGDip.

Study session: There are four study sessions in a year, each lasting 10 weeks. Sessions begin in October, January, April and July. Each session is following by an assessment submission point.

Resitting the assessment of a failed module: When you resit a failed module you will not be allocated a tutor group but you will have access to the learning materials on the VLE and you will be required to resubmit your summative assessment.

Repeating a failed module: When you repeat a failed module you will be allocated a tutor group, you will have access to the learning materials on the VLE and you will be required to resubmit your summative assessment.

Throughout the Regulations, ‘we’ ‘us’ and ‘our’ mean the University of London; ‘you’ and ‘your’ mean the student, or where applicable, all students.

If you have a query about any of the programme information provided please contact us. You should use the *ask a question* button in the student portal.

Changes to the Cyber Security Regulations 2022–2023

This programme is offered for the first time in October 2022.

Update October 2022: The penalty for exceeding the word limit for coursework elements of assessment will also apply to online examinations where a word limit is given (see regulation 4.5).

1 Structure of the programmes

Appendix B gives the syllabuses and module outlines.

Qualifications

1.1

The following named qualifications are awarded under the Cyber Security programme:

- Master of Science (MSc) in Cyber Security
- Postgraduate Diploma (PGDip) in Cyber Security
- Postgraduate Certificate (PGCert) in Cyber Security

Qualification structure

1.2

The MSc Cyber Security consists of:

- ten core modules (15 credits each)
- one Project module (30 credits)

1.3

The PGDip Cyber Security consists of:

- one core module (15 credits); and
- seven optional modules (15 credits each)

1.4

The PGCert Cyber Security consists of:

- one core module (15 credits); and
- three optional modules (15 credits each)

Individual modules

1.5

Select modules from the MSc Cyber Security are available to study on a stand-alone basis, subject to module availability.

See the Programme page for information about the modules available for study on a stand-alone basis and when they run.

Exit qualifications

1.6

The PGDip in Cyber Security is an exit qualification that requires the passing of at least eight modules to the value of 120 credits, including one core module.

1.7

The PGCert in Cyber Security is an exit qualification that requires the passing of at least four modules to the value of 60 credits, including one core module.

2 Registration

Effective date of registration

2.1

Your effective date of registration will be either:

- 1 October, if you first register before the September registration deadline.
- 1 April, if you first register before the March registration deadline;

Date of first assessments

2.2

If your effective date of registration is:

- 1 October, you will take your first assessment(s) in December of the same year
- 1 April, you will take your first assessment(s) in June of the same year

Study sessions

2.3

The programme has two registration points in the year. There are four study sessions in a year, each lasting 10 weeks. Sessions begin in October, January, April and July. Each session is followed by an assessment submission point.

Further information about ratification of grades can be found in Section 6: Progression within the programme

2.4

Each 15-credit module will be taught over one 10-week session.

2.5

The Project is 30 credits and will be taught over two 10-week sessions, beginning in the April session.

Module availability

2.6

Where the learning experience may be compromised due to low student registrations, we may consider deferring the module to a later session.

Not all modules will run in every study session.

We will inform you of any such changes as early as possible and provide you with reasonable alternative arrangements.

Period of registration

See the Programme Specification for the minimum and maximum periods of registration applicable to this programme.

2.7

The minimum and maximum periods of registration to complete the programme are counted from your effective date of registration.

2.8

If you start by taking individual modules and then register for the PGCert/PGDip/MSc Cyber Security we will give you a new maximum period of registration for the PGCert/PGDip/MSc.

See Section 6: Progression within the programme for information on the maximum and minimum number of modules you can register for in a study session.

3 Recognition of prior learning and credit transfer

To be read in conjunction with the General Regulations, Section 3.

Recognition of prior learning

3.1

We consider applications for recognition of prior learning (RPL) on the basis of studies successfully completed at an appropriate level.

If you are registering on the MSc Cyber Security you may apply for recognition of prior learning for up to 120 credits (eight 15-credit modules).

3.2

If you are registering on the PGDip Cyber Security you may apply for recognition of prior learning for up to 75 credits (five 15-credit modules).

3.3

If you are registering on the PGCert Cyber Security you may apply for recognition of prior learning for up to 30 credits (two 15-credit modules).

4 Assessment for the programme

Summary table of assessment

See Appendix B for the specific assessment for each module.

4.1

Module	CYM010, CYM020, CYM030, CYM040, CYM050, CYM060, CYM070, CYM080, CYM090, CYM100	CYM500
Element weighting	100%	100%
Item of assessment	One unseen written end of term coursework/online examination	Project

Passing assessments

4.2

The pass mark for each module is 50%.

Invalid attempts

4.3

If you do not submit the assessment for a module, this will not count as a valid attempt at the module and there will be no academic penalty.

4.4

If you have not made a valid attempt at the module, you will need to re-register and make a new attempt at the module. You will be required to pay the **full module fee**.

See General Regulations for Rules for taking written assessments

See the website for information on the submission of mitigating circumstances.

Penalty for exceeding the word count

4.5

For coursework elements and online examinations with a given word limit, you should not exceed the word limit by more than 10%. If the word count is between 10% to 20% above the word limit, the assessment will receive a five mark penalty. If the word count exceeds the word limit by more than 20% you will receive a mark of zero for your work.

Late submission of coursework elements

4.6

You must keep to the deadlines given on the VLE. Coursework elements that are submitted after the deadline will not be marked and the attempt will be considered invalid.

See regulations 4.3 and 4.4 for information on invalid attempts.

5 Number of attempts permitted at an assessment element

5.1

The maximum number of attempts permitted for any element of assessment is two.

5.2

You will fail the assessment if your overall weighted mark for the module is below 50%.

5.3

You must make a second attempt at the assessment for a module you have failed, provided that you have not exceeded the maximum number of attempts at the assessment/s.

5.4

If you pass the module overall with a mark of 50% or above, you will not be permitted to make a second attempt at any assessment element.

Resitting the assessment of a failed module

If you resit the assessment for a module, you will have to pay a fee when you re-register for the module to resit the assessment. The fee payable is outlined in the fee schedule.

You will not be allocated a tutor group but will have access to the learning materials on the VLE and will be required to resubmit your summative assessment.

5.5

If you fail the assessment for a module held in the October session or the January session, your resit opportunity will be the July session of the same academic year.

5.6

If you fail the assessment for a module held in the April session or the July session, your resit opportunity will be in January of the following academic year.

5.7

If you do not make a second attempt at a failed module at the first opportunity, you will be required to repeat the module in full. **You will be required to pay the full module fee.**

Repeating a failed module

If you repeat a module, you will have to pay the full module fee when you re-register for the module. When you repeat a failed module you will be allocated a tutor group, you will have access to the learning materials on the VLE and you will be required to resubmit your summative assessment.

5.8

You may choose when you repeat a failed module. You do not have to take the assessment at the next available study session.

6 Progression within the programme

See Section 4: Assessment for the programme for method of assessment.

6.1

You must commence study of *CYM010 Cyber security foundations* before, or along with, any other modules. You must have passed 60 credits before you register for the *CYM500 Project*.

It is strongly recommended that you register on *CYM100 Research methods for cyber security* before registering for the *Project*.

Module selection

6.2

In any one study session, you may register for a maximum of 45 credits in a combination of new, failed and resumed modules, of which a maximum of 30 credits may be made up of new modules. A new module is a module you have not registered for previously or for which a previous attempt was invalid.

In a session where you are registered for the Project, this will count as 15 credits per session.

6.3

There are two exam boards a year, following the January and July sessions.

You will receive provisional results following the October and April sessions. These results will be formally ratified by the next available exam board. Provisional results should be used for the basis of progression.

Individual modules

See Section 1 for information about stand-alone individual module availability.

6.4

You may take three modules (45 credits total) on a stand-alone basis without being registered for the PGCert, PGDip or MSc. If you apply to progress to the PGCert, PGDip or MSc and this is approved, you may be credited with any individual modules successfully completed.

Progression between qualifications within the programme

6.5

If you are registered on either the PGCert or PGDip and want to transfer your registration to a higher qualification, you should notify us before you enter for your final assessments.

As the entrance requirements for the PGCert, PGDip and MSc are the same, you do not need to successfully complete the lower award to transfer to the higher award. However, transfer of registration cannot take place whilst a study session is live and before results for this session are ratified by the exam board.

Performance Based Admissions

There are two entry routes into the MSc: the Direct Entry route and the Performance Based Admission route. See the entrance requirements in the Programme Specification, and the requirements tab on the programme's web page for full details.

6.6

To enter the MSc via the Performance Based Admission (PBA) route, you must first register for and pass two of the 15-credit modules. Final results ratified at the Exam Board will be used for the basis of progression.

6.7

While registered on the PBA route you may register for a maximum of 45 credits in any session, of which 15 credits can be made up of new modules. Your total module registrations, including modules that you are waiting to repeat, may not exceed 60 credits.

Transfer from individual modules

6.8

A mark awarded for completion of an individual module may not be used to replace any mark for a degree, diploma or certificate already awarded.

6.9

If you are registered on standalone individual modules and you wish to transfer your registration to the PGCert, PGDip or MSc, you must meet the entrance requirements for Direct Entry or for Performance Based Admission (PBA).

6.10

If you only meet the entrance requirements for Performance Based Admission (PBA) but have already successfully completed two individual modules on a standalone basis (30 credits total), you will be permitted to transfer your registration directly onto the MSc, PGDip or PGCert via the Direct Entry route.

6.11

Only three modules (a maximum of 45 credits) may be counted as credit towards the MSc, PGDip or PGCert.

If you request to transfer from standalone individual modules to the MSc, PGDip or PGCert and are currently undertaking the study for these modules, transfer of registration cannot take place whilst a study session is live and before results for this session are ratified by the exam board.

7 Schemes of award

Marking criteria

See Appendix C for the Assessment Criteria.

7.1

All assessments will be marked according to the published Assessment Criteria.

Mark scheme

7.2

The following mark scheme is used for the MSc, PGDip and PGCert:

Mark range	Outcome
70% and over	Distinction
60% – 69%	Merit
50% – 59%	Pass
0% – 49%	Fail

7.3

To calculate the final grade for the qualification, the marks for modules are weighted equally, with the exception of the Project which is double weighted.

7.4

To be granted the qualification with Merit, your mean average mark for the 15 credit modules must be between 60% and 69%; your mark for the Project (if applicable) must be 60% or above.

7.5

To be granted the qualification with Distinction, your mean average mark for the 15 credit modules must be 70% or above; your mark for the Project (if applicable) must be 70% or above.

Date of award

7.6

The date of award will correspond to the year that the requirements for the award were satisfied.

Exit qualifications

7.7

If you have exhausted your permitted number of attempts at module(s) and are unable to complete the MSc or PGDip, you may be considered for an exit qualification of PGDip or PGCert (respectively). In such circumstances, you will need to have achieved the credits required for a PGDip (120 credits) or PGCert (60 credits) and have successfully completed the required modules for the qualification concerned.

Exit qualifications will be classified according to regulations 7.4 and 7.5.

7.8

If you have not completed the required modules, but you have completed the required number of credits for a PGDip (120 credits) or PGCert (60 credits), the Board of Examiners may, at its discretion, consider you for an exit qualification.

7.9

The exit qualification of PGDip or PGCert will be with effect from the year in which you satisfied the requirements for that award. Your registration will cease once the exit qualification has been granted.

Appendix A – Structure of the programmes

A detailed outline of the module syllabus is provided on the Programme page, under structure

MSc Cyber Security

For the qualification of MSc Cyber Security you must pass

- The following core modules (each worth 15 credits):
  - CYM010 Cyber security foundations
  - CYM020 Security management and governance
  - CYM030 Cybercrime
  - CYM040 Applied cryptography
  - CYM050 Network and infrastructure security
  - CYM060 Computer systems security
  - CYM070 Software and application security
  - CYM080 Security and behaviour change
  - CYM090 Information privacy
  - CYM100 Research methods for cyber security
- One compulsory Project module (worth 30 credits):
  - CYM500 Project

PGDip Cyber Security

For the qualification of PGDip Cyber Security you must pass

- **One** core module (worth 15 credits):
  - CYM010 Cyber security foundations
- Any **seven** modules chosen from (each worth 15 credits):
  - CYM020 Security management and governance
  - CYM030 Cybercrime
  - CYM040 Applied cryptography
  - CYM050 Network and infrastructure security
  - CYM060 Computer systems security
  - CYM070 Software and application security
  - CYM080 Security and behaviour change
  - CYM90 Information privacy

PGCert Cyber Security

For the qualification of PGCert Cyber Security you must pass

- **One** core module (worth 15 credits):
  - CYM010 Cyber security foundations
- Any **three** optional modules chosen from (each worth 15 credits):
  - CYM020 Security management and governance
  - CYM030 Cybercrime
  - CYM040 Applied cryptography
  - CYM050 Network and infrastructure security
  - CYM060 Computer systems security
  - CYM070 Software and application security
  - CYM080 Security and behaviour change
  - CYM090 Information privacy

Appendix B – Module descriptions

Cyber security foundations [CYM010]

This preliminary module, which must be taken before any of the other modules in the degree programme, introduces the broad range of concepts, challenges and technologies that underpin the provision of cyber security. Students will gain an understanding of what cyber security is, why it is important, and of the principal techniques and technologies that are used to achieve cyber security.

Gaining an understanding of certain key elements of cyber security is necessary to be able to properly appreciate individual aspects of the subject in greater detail. This module is intended to give students this broad understanding so that they can set the ideas and skills developed in other modules into a broader context.

Assessment: One online examination (100%)

Security management and governance [CYM020]

This module aims to generate understanding and appreciation of the need for effective security management and the main currently used approaches to management in practice, including key standardised approaches and the fundamental importance of a risk-based approach. After completing the module, students will also understand key components of practical cyber security management, including the impact of law and regulation, the importance of auditing, and the key role of people in achieving cyber security. To help students understand the importance of effective security management, case studies of failures will be considered.

This module plays a fundamental role in binding together all the other modules of the degree programme; it will address the issue of how to integrate the wide range of possible technologies and techniques for information security into a real-world Information Security Management System for an organisation.

Assessment: One online examination (100%)

Cybercrime [CYM030]

Cybercrime is a complex topic which affects individuals, societies and nations. There is an increasing manifestation of various types of cybercrime, which are either new or evolving. In order to understand the cybercrime environment, this module synthesises its dynamically changing economic, technical, political and psychological components. We explore the types of cybercrime, their manifestations, and their underlying mechanisms. Legal measures and challenges are explored, in view of the global nature of cybercrime. The evolution and the trends of cybercrime are analysed along various models adopted by criminals. Students will gain an understanding of the tools and approaches used in digital forensics and analyse real-world cases of cybercrime.

Assessment: One online examination (100%)

Applied cryptography [CYM040]

Cryptography provides the core toolkit that underpins most digital security technologies. An understanding of what cryptography does, and its limitations, is critical to developing a wider appreciation of the security of everyday digital applications. Since cryptography provides tools for atomic security services such as confidentiality and data integrity, an appreciation of cryptography also equips students with a fundamental understanding of what security means in cyberspace. Note that this module adopts a non-mathematical approach to cryptography, very much considering it

from the perspective of what any good cyber security professional needs to know, and avoiding unnecessary technical details.

In this module students will explore the role of cryptography in supporting digital security for everyday applications such as the internet, mobile phones, wireless networks and cryptocurrency. Students will develop an understanding of the functionality and purpose of the main cryptographic tools we use today. Students will learn how to make decisions about which cryptographic tools are most appropriate to deploy in specific settings. Students will also explore the wider infrastructure surrounding cryptography and how this impacts the overall security of systems deploying cryptography.

Assessment: One online examination (100%)

Network and infrastructure security [CYM050]

Computer networking technologies and cyber-physical systems form the infrastructure of organisations and businesses, the internet and the web-based application ecosystem as well as critical national infrastructure. This module provides the foundations for us to understand the design and security of an organisations network, operational technologies, the internet and critical infrastructure. Computer networking provides the foundational connectivity services that are used for the world wide web, distributed computer applications and services, operations and manufacturing, and national infrastructure.

This module discusses vulnerabilities and the exploits that target computer networks and systems, the internet infrastructure and provides an introduction to modelling, assessing and testing networks and systems. Key aspects are explored through case studies and we complement the *Computer systems security* and the *Software and application security* modules.

Assessment: One online examination (100%)

Computer systems security [CYM060]

Computer systems form the infrastructure of organisations, the internet and the web-based application ecosystem. This module provides the foundations for us to understand the computer systems from the operating systems and security services. The module allows us to consider case studies from a wide range of deployments including the internet and cloud computing/infrastructure that provide the world wide web and distributed computing services.

Assessment: One online examination (100%)

Software and application security [CYM070]

Software and applications form the key business functionality in organisations. Building secure software is critical to the business and must be considered alongside secure computer systems and networks/infrastructure.

This module introduces the principles around software and applications, including security and the issues of malicious software. The module outlines techniques used for secure software development, principles of secure programming, most common software vulnerabilities that can be introduced during software development and concludes with discussion of the wider considerations and research direction for software and application security. Key aspects are explored through a number of topical case studies, such as web and cloud and this module complements the *Computer systems security* and *Network and infrastructure security* modules.

Assessment: One online examination (100%)

Security and behaviour and change [CYM080]

Security is heavily dependent on humans and their actions. These actions can either strengthen or diminish security levels. In this module students are introduced to the relationships between security and human behaviour, in multiple settings. We consider perceptions and practical implementations of security, on both individual and group/societal level. We utilise concepts from behavioural economics, decision-making and psychology, along with mechanisms to design and encourage changes in security behaviours. Finally, we examine the construct of a security culture and its relationships with norms, habits and awareness training.

Assessment: One online examination (100%)

Information privacy [CYM090]

This module will introduce students to the challenges facing any organisation in managing data privacy. Students will gain an understanding of the meaning of data privacy, and will examine the serious legal constraints facing all organisations which make data privacy a key issue for cyber security risk management. Students will examine key governance matters, including privacy impact assessments, and the role of technology in supporting privacy will also be considered, including de-identification techniques for datasets, homomorphic encryption, and other privacy enhancing technologies. Finally, a privacy case study, such as e-voting, will be described.

Assessment: One online examination (100%)

Research methods for cyber security [CYM100]

This module provides students with an introduction to research methods in cyber security such that they can choose and investigate a research or professional topic for their project.
The project topic can be from across the CyBOK Knowledge Areas and professional frameworks such as the CIIsec Knowledge and Skills frameworks. The output from the module is a report that describes the project, provides an initial literature review and a project plan.

Assessment: Project description and plan (100%)

Project [CYM500]

This module provides the student an opportunity to undertake an individual dissertation project in the discipline of cyber security. A project is a major individual piece of work. It can be of academic or professional nature and aimed at acquiring and demonstrating understanding and the ability to reason about some specific area of cyber/information security. The project may be academic in nature or document the ability of organisations or individuals to deal with a practical aspect of cyber/information security. The project represents the key difference between the Postgraduate Diploma, which is a taught qualification, and the award of an MSc which incorporates this substantial piece of individual work.

Assessment: One research project (100%)

Appendix C – Assessment criteria

This is an indicative description of expectations at each grade level. Overall grades will comprise qualitative and quantitative elements. The setting of questions, tasks and requirements and the accompanying marking scheme should take account of the criteria below.

% range	Grade Descriptor	Description
85 +	Outstanding Distinction	Work of outstanding quality, showing mastery of the subject matter with a highly developed and mature ability to analyse, synthesise and apply knowledge and theory. All objectives of the task are covered and work is free of errors. There is evidence of critical reflection and the work demonstrates originality of thought. Ideas are expressed with fluency and elegance. This work meets and exceeds the standard for distinction, as described in the 70-84 band, across all sub-categories of criteria: knowledge and understanding of subject; intellectual skills; capacity to solve more unusual or demanding scenarios involving application of deep understanding of the subject and its methods/techniques; research skills; use of research-informed literature and other scholarly practices.
70-84	Distinction	Produces work of exceptional standard, reflecting excellent understanding. Displays mastery of the subject matter, with notable critical awareness of current problems and/or new insights at forefront of the field. Shows excellent ability to select and apply appropriate and relevant methodologies/techniques/theories as well as the ability to evaluate methodologies critically. Deals with complex issues systematically and creatively, making excellent judgements. Conducts research highly effectively, using technical and/or professional skills as appropriate. Shows originality in application of knowledge and the ability to communicate at a very high level arguments, evidence and conclusions to diverse audiences.
60-69	Merit	Clear understanding of the subject area producing work with a well-defined focus. Shows some originality of ideas; appropriate use of analytical techniques; appreciation of methodology; critical analysis of data; evidence of independent reading; adequate referencing and professional bibliography; adequate structure and style; reasonably professional standard of presentation with some errors of spelling, punctuation or grammar. Shows understanding and critical awareness of current problems and/or new insights, much of which is at, or informed by, the forefront of the academic discipline, field of study or area of professional practice. Able to communicate very effectively arguments, evidence and conclusions to specialist and non-specialist audiences.
50-59	Pass	Demonstrates a sound general knowledge and understanding of material and subject area; Shows limited originality of ideas; straight forward application of analytical techniques; limited commentary on methodology; limited critical analysis of data; limited evidence of independent reading; adequate referencing and adequate bibliography; adequate structure and style; moderately professional standard of presentation with errors of spelling, punctuation or grammar. Able to communicate effectively with a given audience. Work shows a grasp of relevant concepts and material, but with some errors, gaps or areas of confusion. Only the basic requirements of the work are covered. There is a heavy reliance on course materials and little evidence of additional reading.

% range	Grade Descriptor	Description
40-49	Fail	Demonstrates limited understanding and lacks the core knowledge of the subject area; lacking originality of ideas; limited application of analytical techniques; lacking commentary on methodology; limited critical analysis of data, little evidence of independent reading; adequate referencing and adequate bibliography; adequate structure and style; poor to moderate standard of presentation with errors of spelling, punctuation or grammar. Offers some appropriate analysis, but with some significant inconsistencies which affect the soundness of argument and/or conclusions. Demonstrates very limited critical ability producing work that is too descriptive.
0-39	Fail	Demonstrates significant weakness in the knowledge base and understanding of the subject area; simply reproducing knowledge without evidence of understanding. Shows few original ideas; limited application of analytical techniques; limited understanding of methodology; lacks commentary on methodology; no critical analysis of data; poor, inconsistent analysis; very little or no evidence of independent reading; very poor referencing and poor bibliography; poor structure and style; poor standard of presentation with significant errors of spelling, punctuation or grammar.