Programme Specification

UNIVERSITY OF WESTMINSTER

Course record information

Name and level of final award	• Bachelor of Science with Honours - Cyber Security and Forensics • Bachelor of Science with Honours - Cyber Security and Forensics with Industrial Experience • Bachelor of Science with Honours - Cyber Security and Forensics with International Experience The award is Bologna FQ-EHEA first cycle degree or diploma compatible
Name and level of intermediate awards	• Bachelor of Science (BSc) - Cyber Security and Forensics • Diploma of Higher Education (Dip HE) - Cyber Security and Forensics • Certificate of Higher Education (CertHE) - Cyber Security and Forensics
Awarding body/institution	University of Westminster
Teaching institution	University of Westminster
Status of awarding body/institution	Recognised Body
Location of delivery	Primary: Central London
Language of delivery and assessment	English
QAA subject benchmarking group(s)	Computing
Professional statutory or regulatory body	British Computer Society (BCS) (Pending: Please refer to Page 12 for further information)
Westminster course title, mode of attendance and standard length	• Cyber Security and Forensics BSc, Full-time, September start - 3 years standard length with an optional year abroad or placement
Valid for cohorts	From 2023/4

Admissions requirements

There are standard minimum entry requirements for all undergraduate courses. Students are advised to check the standard requirements for the most up-to-date information. For most courses a decision will be made on the basis of your application form alone. However, for some courses the selection process may include an interview to demonstrate your strengths in addition to any formal entry requirements. More information can be found here: https://www.westminster.ac.uk/study/undergraduate/how-to-apply

Recognition of Prior Learning

Applicants with prior certificated or experiential learning at the same level of the qualification for which they wish to apply are advised to visit the following page for further information:

https://www.westminster.ac.uk/current-students/guides-and-policies/student-matters/recognition-of-prior-learning

Aims of the programme

Cyber security and forensics is an increasingly vital subject, given the impact of cyber incidents on businesses, governments, and individuals. The BSc Cyber Security and Forensics course is designed to meet the ever-growing demand for qualified experts. The course is developed with reference to QAA Subject Benchmark for Computing (March 2022) and the Engineering Council Accreditation of Higher Education Programmes (AHEP), fourth edition. Additionally, the course is designed to meet the requirements and expectations of the UK government strategic vision for 2030 to become a leading responsible democratic cyber power and to be able to protect itself from internal and external cyber-attacks. Therefore, the course is designed to be aligned with the key knowledge areas of National Cyber Security Centre (NCSC).

The course brings together a mix of several disciplines with the aim of producing a skilled, innovative, and confident problem solver who is able to produce a cyber resilient digital solution and detect and contain cyber-attacks before they do any damage to a system. This is achieved by enabling you, the student, to gain skills in key aspects of the cyber security and forensics and to be able to use tools and techniques both offensive and defensive in order to evaluate and identify risks and vulnerabilities and formulate countermeasures.

The cyber security and forensics domains are fast changing and dynamic due to ever evolving threats and the need for countermeasures, requiring companies to frequently change and improve their information systems security. You will be encouraged to solve cyber security and forensics problems with innovative solutions considering the global outlook and societal aspects of the prevailing environment in order to produce sustainable and adaptable solutions.

The programme aims to:

- Equip you, the student, with a solid knowledge in the fundamentals of cyber security, networks and digital forensics and other computer science topics relevant to the course.
- Develop an in-depth understanding of the theoretical and practical aspects of the current technologies that underpin cyber security, their limitations, threats and their impacts on real world cases and methods to mitigate them.
- Provide you with a good knowledge and awareness of the socio-economic, ethical, and legal aspects related to businesses, enterprise, and society.
- Encourage initiative and confidence in approaching cyber incidents and the adoption of digital forensics investigative approaches using both analytical and practical skills gained throughout the course.
- Provide an environment where you will be able to collaborate, develop transferable employability skills including project management, risk management, teamwork, leadership, entrepreneurship and written and oral communication.
- Be industry focused and relevant using industrial practice within teaching and extra curricula activities
- Support development of the wider skills and behaviours for professional communication, collaborative working and reflective practice that are respectful, accessible, and inclusive of all.
- Provide an exciting, enjoyable, and rewarding learning experience which will serve as a solid foundation for professional cyber security and digital forensics career.

The communication and interpersonal skills necessary for operation in a diverse and inclusive professional environment are an important part of the course and will allow you to adapt to future changes in technology. Alongside technical skills you will also develop a range of professional skills. There are three specific modules at each level which support the development of professional transferable skills through group and individual work: Trends in Computing in Year 1, work-based learning module Risk Management and IT Governance in Year 2 and the Final Year Project in Year 3. In other module you will also be encouraged to work collaboratively, manage your time successfully, work in teams in different roles and present and defend work to peers and tutors. Above all the course aims to inspire students of all backgrounds and genders to become a cyber professional developer.

Employment and further study opportunities

University of Westminster graduates will be able to demonstrate the following five Graduate Attributes:

- Critical and creative thinkers
- Literate and effective communicator
- Entrepreneurial
- Global in outlook and engaged in communities

- Social, ethically and environmentally aware

University of Westminster courses capitalise on the benefits that London as a global city and as a major creative, intellectual and technology hub has to offer for the learning environment and experience of our students.

The BSc Cyber Security and Forensics course has:

- Career development skills, embedded in all levels;
- Opportunities for placements and work-related learning activities;
- Staff membership which continues to widen and strengthen the University's links with employers in all sectors;
- A curriculum highly relevant to the current and future needs of industry;
- Career education and guidance activities that actively engage employers.

The University and the course team consider that employability is an important attribute of any successful graduate. Throughout the course from Year 1 onwards you will be offered a multitude of help and support to enhance your employability, find and secure placement opportunities and plan your career through regular workshops and events organised by the Career Development Centre and the course team.

This will be achieved by enhancing your employability skills in developmental sessions where you will, for example, practise job interview skills and CV writing skills. Extra-curricular activities will be offered to encourage you to further engage with the employability services of the university.

The course will focus on the development of practical know-how and broader transferable employability-related skills such as critical thinking, leadership, teamwork, communication, presentation, and report writing to ensure that you are prepared and ready to enter the world of work when you graduate.

Specific skills and knowledge required for students wishing to become cyber security and digital forensics professionals are developed in core modules. The optional modules in both Level 5 and 6 provide opportunities for further specialisation for specific careers in cyber security and forensics such as testing, information system security, and compliance.

Level 5 work-based learning module Risk Management and IT Governance is incorporated in the course in the form of a live project that is informed by the industry such as the production of a risk management report based on a real-world scenario. This module will provide you with an opportunity to work within a small team on a project that is informed by typical industry projects. In addition, the project-based module will allow you to put theory into practise and improve on transferable employability skills such as costing, project management, risk management, quality management, leadership, communication, time-planning and teamwork.

Many of the modules use scenario-based assessment to prepare you for working in a professional environment by utilizing real-world examples such as formulating protection against external attacks or whether company is compliant in the context of legal and regulatory constraints.

After completing the second year of your study you will have the opportunity to take a year in industry and gain work experience (work placement). This will increase your chances of employability after graduation and further develop broader skill sets such as time management often championed by employers.

Furthermore, you can choose to undertake an international experience year as part of your degree at one of our partner overseas institutions such as Institute of Informatics (IIT), Sri Lanka or Westminster International University in Tashkent (WIUT). You will study and reside in the country of a host institution during the year. The content of your study is agreed upon through a Learning Agreement between you, the home institution and the School of Computer Science and Engineering.

The technical and interpersonal skills you gain from your course shall prepare you for one of the many roles in cyber security and forensics. Examples of such roles are shown below:

- **Vulnerability assessors** - help companies to assess the strengths of their networks by using tools to identify if their networks are vulnerable to threats. They assess those vulnerabilities to recommend security solutions.
- **Computer forensics analysts** - investigate computer-based crime by using specialised methods and techniques to examine the data on digital devices. The findings from this analysis can be used as evidence in court.
- **Digital Forensics and Incident Responders (DFIR)** monitor and examine the system data continuously by using automated tools in order to determine if an attack or malicious act is in progress. If an attack is being carried out, they initiate their incident response plan to contain it, minimize its impact and bring back services and data to normal operation mode.

- **Information security risk managers** conduct risk assessments on information systems to identify any potential risks to the environment. They analyse risks, identify their potential impacts on the business and then identify changes needed to reduce or mitigate those risks by recommending security controls and measures.
- **IT security operations specialists** are responsible for the day-to-day security activities in an organization such as installing security software and patches, securing the network and prevent security breaches. They usually deploy and manage security software and tools across all organization infrastructure.
- **Penetration tester security officers** conduct offensive cyber operations across their organizations information systems to identify weaknesses in the systems. They do this in a managed and controlled way but using the same tools and techniques used by a malicious actor in order to stress test and discover any system's vulnerabilities.

Alternatively, you may wish to carry on to further study at Masters or Doctorate level. We offer many Master courses in computer science and data security. As a graduate of this course, you shall be capable and prepared for continuing your education at postgraduate level. We can offer you advice on this once you have completed your studies.

What will you be expected to achieve?

Learning outcomes are statements on what successful students have achieved as the result of learning. These are threshold statements of achievement the learning outcomes broadly fall into four categories:

- The overall knowledge and understanding you will gain from your course (KU)
- Graduate attributes are characteristics that you will have developed during the duration of your course (GA)
- Professional and personal practice learning outcomes are specific skills that you will be expected to have gained on successful completion of the course (PPP)
- Key transferable skills that you will be expected to have gained on successful completion of the course. (KTS)

Level 4 course learning outcomes: upon completion of Level 4 you will be able to:

- LO4.1 Demonstrate knowledge and understanding of the core principles and the fundamental concepts of computer science. (KU GA)
- LO4.2 Explain the fundamentals of cyber security and digital forensics in aspects of networking, hardware, and data and the role of social engineering and its association with computer security. (KU KTS SS)
- LO4.3 Demonstrate a good understanding of a range of underlying mathematics theories related to computer science and cyber security. (KU GA KTS CS)
- LO4.4 Design and develop simple solutions and programs using a range of selected software engineering tools and techniques and programming languages. (GA KTS SS)
- LO4.5 Demonstrate a knowledge and understanding of current technology and trending future technology in computer systems, cybersecurity, design tools and techniques as taught (KU GA PPP)
- LO4.6 Gather and assimilate information, with some guidance, and apply it appropriately and then communicate technical information succinctly and accurately, by means of presentations, written reports, appropriate diagrams, and discussion (GA PPP KTS)
- LO4.7 Plan and coordinate work required for structured group tasks, keeping to set deadlines given direction and guidance. (GA KTS CS)

Level 5 course learning outcomes: upon completion of Level 5 you will be able to:

- LO5.1 Evaluate, compare, and contrast different auditing and monitoring techniques for various security threats and understand the legal aspects and the different standards companies can employ. (KU GA KTS SS)
- LO5.2 Analyse, evaluate and adopt a holistic approach to risk reduction strategies using appropriate risk management approaches and principles that comply to various standards and legislations. (KU GA PPP SS)
- LO5.3 Critically investigate complex digital forensic cases using practical tools, skills, methodologies and practices to identify computer crime and cyber incidents. (KU GA KTS SS)
- LO5.4 Concisely and accurately document findings in an appropriate and clear structure for technical and non-technical audiences that would be appropriate to use in legal context such as forming part of evidence in court. (GA KTS CS)
- LO5.5 Select and apply sustainable security control solutions and algorithms to secure complex network

environments in organizations and evaluate the societal and environmental impacts including any limitation to your solutions. (KU GA KTS SS)

- LO5.6 Work effectively either in a group or individually and be able to recognize development needs for the acquisition of new skills. (GA PPP CS)
- LO5.7 Adopt an inclusive approach to engineering practice and recognise the responsibilities, benefits and importance of supporting equality, diversity and inclusion. (GA PPP CS)

Additional Year course learning outcomes: upon completion of Additional Year you will be able to:

- IEY.1 Enable personal development by devising a programme of international study that complements the content of the home degree programme and/or develops other interests. (GA PPP KTS)
- IEY.2 Appreciate the challenges and opportunities of studying/ working in an international context. (GA PPP KTS)
- IEY.3 Demonstrate an understanding of, and respect for, the cultural norms and differences of the host country at a societal level as part of an inclusive, global outlook. (GA PPP KTS)
- IPY.1 Experience commercial application of engineering knowhow and identify the factors affecting products and services in IT industry. (KU GA PPP KTS)
- IPY.2 Demonstrate the acquisition of a range of professional, practical, and key-transferrable skills relevant to the fields of computing (KU GA PPP KTS)
- IPY.3 Take personal responsibility for directing your own learning and future career making the best use of the opportunities, experiences and people that were available to you during your placement year. (GA PPP KTS)
- IPY.4 Draw upon the diverse approaches, perspectives, knowledge and experience of a diverse workforce, treating all individuals with respect and recognising their contribution to the host organisation. (KU GA PPP KTS)

Level 6 course learning outcomes: upon completion of Level 6 you will be able to:

- LO6.1 Critically evaluate, design, and implement security measures on different technologies and evaluate their effectiveness against known attacks. (KU GA KTS)
- LO6.2 Select and apply advanced methods, principles, and concepts to identify cyber incidents and be able to forensically investigate, make decisions in complex and unpredictable contexts and interpret and analyse results obtained in a systematic manner. (KU GA KTS SS)
- LO6.3 Independently gather, assimilate, and critically evaluate information to a given cyber security or digital forensics issue, choose and formulate cost and effectiveness of a given set of solutions, and select and implement the most viable solution (KU GA PPP KTS CS)
- LO6.4 Select, analyse, and communicate complex technical information succinctly and accurately to expert and non-expert audiences, reviewing its reliability, validity, and significance by means of presentations, written reports, and discussion. (KU GA PPP CS)
- LO6.5 Undertake research tasks with minimum guidance and critically evaluate arguments, assumptions, and abstract concepts. Organise and present information concisely and correctly and manage project work, adhering to given timetables and targets (GA PPP SS CS)
- LO6.6 Recognise and assess risk limitations pertaining to a given problem including those related to the environment, sustainability, society, health and safety and regulation and suggest ways to mitigate this risk. (GA PPP SS CS)
- LO6.7 Practice life-long learning and entrepreneurial skills using independent and creative thought through the gathering and assimilation of information gained through practical work using logbooks, minutes of meetings, social media sites and other novel methods. (GA PPP KTS)

How will you learn?

Learning methods

The BSc Cyber Security and Forensics course uses a variety of teaching and assessment methods, to ensure that every student on the course is empowered to fulfil their full potential and achieve the best outcome they possibly can.

A principal aim of the course is to equip you for professional life, or higher study, relevant to your current programme of study. To this end the course is organised into a collection of learning opportunities (modules) at various levels which are directly related to the aims and learning outcomes of the course. These modules are the building blocks of your course.

Each module consists of learning activities which are delivered over a number of weeks. These learning activities are designed to help you achieve the knowledge and skills related to your subject area of cyber security and forensics.

A fundamental principle underlying the learning process and teaching methods used on this course is “learning-through-practice”. That is, to learn and understand the engineering skills and techniques required, students need to acquire skills through doing. This approach applies to both practical skills, which you will learn through project and laboratory work as well as to analytical skills, which you will learn by applying taught principles to problem-solving tasks.

Much of the learning is achieved through active participation in taught interactive practical sessions. At the end of these sessions feedback will be given. For example, laboratories typically form formative assessment components where you will be given support to complete the tasks described. At the end of these formative sessions, you will be given written, verbal, qualitative feedback, or a mixture of these to help you understand how well you have performed the task and how to improve it. These formative sessions are used as part of a teaching delivery framework aimed at developing your confidence and abilities to undertake the final summative assessment components for a given module. In general lecturers will provide written and/or verbal feedback on students’ work throughout the course and feedback may be given individually or to the class collectively.

In order to develop general and transferable skills you will undertake a number of different activities such as group work that will help develop team working, collaborative and interpersonal skills and time management, You will be required to present and defend your work which will allow you to critically reflect on your learning and also allow you to develop your ability to concisely and clearly present your work.

How is Equality, Diversity, and Inclusivity (EDI) addressed in your course

The principles of Equality, Diversity and Inclusivity lay at the heart of the BSc Honours Cyber Security and Forensics course. The course design ensures that you will have a learning experience that is flexible, respects diversity, encourages active participation and considers students varying needs. For example, the course will encourage and enable you to tailor your learning according to your career, cultural identity and individual aspirations by allowing you to choose a final year project specialisation within the broad area of cyber security, express your own unique evidenced based views of various societal and ethical issues, develop your own practical solutions to a given problem set and select option modules that will enable you to specialise or gain greater confidence in various application areas. Through this myriad of opportunities and choices the course will equip you with the technical and employability skills required to work in a changing and diverse world. Above all you should be reassured that the course team aims to eliminate all arbitrary barriers to your learning and to work with you to achieve your best outcome.

The learning methods employed by the BSc Cyber Security and Forensics course are underpinned by three key principles. These are:

- Provision of a learning environment, both physical and digital, that is equitable, diverse and inclusive which allows you to learn flexibly with materials that will be available to you in a number of learning context and at any time such as mobile and home environments;
- Provision of a supportive and safe learning environment, based on mutual trust and respect, where students are empowered to act as partners in their transformative learning experiences;
- Provision of a forward-looking course curriculum that is work-place relevant, current and authentic.

Practically, you will see this working in the following ways, for example:

- Teaching materials are, where possible, designed to be inclusive for all.
- Where possible, the assignment of students to groups will be done in such a way as to ensure there is a mix of abilities, gender and cultures within the group.
- The active development of mutual trust and respect between students and between staff and students;
- The celebration and encouragement of diversity through the core delivery of the course and extra-curricular activities;
- Emphasis on skill-based learning using a learn-by-practise approach; use of current and industry standard tools chains and methodologies; industry supported projects such as the WBL project;
- The teaching of broader concerns, concepts and skills such as the environment and project management that values inclusivity and diversity;
- A curriculum that is current, global in outlook and targeted at application areas that are address real-world challenges.

Teaching methods

We tailor our teaching methods to both the diversity of the subject matter as well as the diversity of our students' to ensure that we maximise the effectiveness of our teaching. We aim to make our students ready for employment by exposing them to tools and techniques relevant and practised by industry.

The range of teaching methods you will experience will include:

- Lectures, seminars, and workshop sessions
- Projects (small groups, large groups and individual)
- Laboratories and computer-aided engineering
- Formative assessment including online quizzes
- Problem sheets, investigations, and design problems
- Individual supervision
- Online learning material

Lectures are used to support your learning. Within the lecture sessions you will be introduced to fundamentals, concepts and development methodologies and strategies. Lectures also have the advantage of showing you how different topics and facts interrelate with each other. Within lectures there will be interactive and participatory work to help monitor and encourage active engagement.

Seminars are used to provide a firm grounding in the theory, methods and tools used for a given module. Within these seminars you will be encouraged to collaborate and/or work in groups. Typically, these seminars will be practical in nature and will help you develop skills and understanding of how to apply knowledge covered in lectures to solve real problems. For example, you may be given a task to write code for a particular problem. During the seminars the tutors will monitor your progress and provide feedback and guidance on your work.

Practical workshops maybe led by or informed by industry experts (alongside academic staff), these maybe onsite or online. In these sessions you will work alone or in groups, undertaking industry focused work or will be guided on how to complete a given milestone for a more long-term element of work such as a group project.

Laboratories are effectively a practical seminar session. In these laboratory sessions you will be using software tools, network equipment, to carry out practical tasks to solve real-world problems. Whilst in these sessions you will be actively encouraged to observe laboratory ethics and/or data security rules. In some instances, virtual or simulation tools maybe used within a laboratory to enable greater accessibility and flexibility by allowing work to be completed remotely as required.

To further support remote learning some modules will employ the use of online quizzes to test your understanding and provide automatic feedback. The key purpose of such online quizzes is to allow you to practise knowledge at home and to provide you with an understanding of how successful your learning has been. It also allows tutors to diagnostically verify your understanding and tailor teaching in order to address any gaps. Through this feedback you can identify where to focus your learning effort.

Throughout the course, authentic assessment is used to help you practise skills required by industry. This includes investigative research-based problems and more practical project led problems. Within the course you will be asked to produce solutions and artefacts based on requirements for a typical real-world scenarios and products.

The final year project module is designed to unify and integrate skills and knowledge gained in the taught learning modules. The final project module provides the opportunity to put into practise and extend what has been learnt to solve a broader more complex and significant engineering problem. To support you in successfully completing the project, you will be allocated a supervisor who is a member of academic staff.

To increase accessibility of the learning material and ensure that a diverse range of learners can participate on the course each module will provide the following online support: access to teaching materials, online reading lists, discussion boards, virtual study rooms for students to collaborate and where applicable, space for individual and group online meeting. Individual support for each module will be available from the modules teaching staff.

At key stages in your academic studies, the decisions you will need to make such as choice of option modules and choice of individual project will be guided when required by your personal tutor. Students will also be academically supported by module leaders and the course leader during their studies.

The teaching methods described above are more effective when coupled with independent study time where you take more control of your own learning. To help enable you to maximise the benefits of self-study we introduce, explain to you, and develop your understanding of concepts and skill sets required for continual professional development (CPD). This is achieved using group-based activities, a framework of taught content, extracurricular events and assessment styles that

encourage the planning and reporting of material that is self-learnt.

Assessment methods

Assessments and feedback are an integral part of the learning process and enable you to gauge your progress in relation to learning outcomes, reflect on what you have learnt, identify areas in which you are strong and areas in which you need to improve and help you make informed decisions on the pace and focus of your own independent learning.
The guiding principles of assessment design and its associated feedback within the BSc Cyber Security and Forensics course are Purpose, Progression and Personalisation.

Purpose:

- assessment is authentic, meaning that it provides the chance to apply knowledge and competencies required within industry to solve real-world problems;
- the assessment method(s) used are clearly relevant to the module's learning outcomes;
- consideration is given to the amount of effort and time required to complete the task(s) and to maintain a balanced assessment load.

Progression:

- the choice of assessment method(s) employed provides an opportunity for new learning and contributes to the learning process;
- assessments are clearly related to the overall pattern of the course, they are developmental and not unnecessarily repetitive;
- less familiar types of assessments are prepared for using formative work such as practise laboratories.

Personalisation:

- you are able to make the assessment you own through design and implementation choices;
- timely feedback is given for all assessments;
- guidance on how you can improve your performance in the future is given, either individually or as part of a group.

As well as ensuring that students have met the learning outcomes per module, assessment will, where possible and appropriate, be:

- demonstrative (helping students to learn – evaluation of current knowledge);
- rigorous (for correct and efficient solutions);
- challenging (requiring deep understanding and analytical ability);
- workplace relevant (tasks directly relating to industry and skills valued by employers);

On the BSc Cyber Security and Forensics course all assessments and feedback mechanisms are designed to form part of the learning experience and will take a variety of forms. The complexity and style of assessment for example will range from small tasks that might be completed within a seminar session to more complex and larger tasks which might be completed over an entire semester within a group. The challenge of an assessment will be varied, for example assessments may involve everything from risk analysis and mitigation given a typical scenario to using tools to analyse forensic data on hardware. Some assessments are designed to be completed individually whereas other assessments may require students to work as part of a team, emulating as closely as possible the environment students will face in a professional setting.

Each module has both formative and summative assessment types. Formative assessment does not contribute to your overall grades. Formative assessment helps you establish where you are in your learning journey, what you have learnt so far, and where you may have to improve. Formative assessment can be used diagnostically by tutors to enable them to dynamically target their teaching to address any gaps in knowledge. Formative assessment can take a form of test, quizzes, reflective sessions, group activities.

All summative assessments that contribute to final grades will be assessed against clear assessment criteria stated in module descriptors. These assessment criteria are directly linked to the modules learning outcomes, and they will be used to evaluate the submitted work and to produce written feedback. BSc Cyber Security and Forensics course provides inclusive, engaging and authentic assessment and feedback strategies to help provide equal opportunities, cater for different learning styles and to best support the student to successfully complete the course.

Examples of Summative assessments used in the course	
Practical Coursework / Practical based portfolio	You will be expected to complete lab tasks following lab guidelines and either answer specific questions about the labs (Coursework) or analyse your results based on a given scenario (Portfolio).
Group Presentation with/without Group Coursework	You will be working in a group, typically of 3 to 4 members, investigating a specific problem, or research a specific topic. You will be expected to give a presentation to demonstrate your group work. This is usually followed by a brief discussion and questions and answers with your peers and instructor. Generally, you will need to discuss in detail what the group has achieved, and how, and also how the work and the team member responsibilities were distributed.
ICT (exam conditions)	You will be expected to sit an in-class test under timed conditions. Typically, these in-class tests can be a closed-book or open-book where you will have access to certain materials. This type of assessment is used to assess your understanding of the fundamentals, theory, and paradigms. Tests help ensure you can demonstrate that you have developed a deep understanding of the subject which enables you to cope with complex problems that require deep inside in order to provide secure and optimal solutions. This time-constrained assessment is authentic in that it verifies that you will have sufficient depth and coverage of knowledge in order to successfully solve typical time-critical cyber security problems. It also helps you prepare for other professional exams and training.
Lab test	You will be expected to complete a specific lab task in the lab. This will be in most cases a timed activity where you are given instructions and a set of tasks to complete.
Coursework Case study	You will be required to work on a scenario that illustrates a specific problem. You will have to study this problem and assess it and take decisions or make recommendations. This will require research and analysis and potentially implementation in order for you to produce an assessment and recommendation. This type of assessment is used to assess your understanding of topics related to your module and how you can apply your knowledge to a given scenario.
Research essay	You will be expected to conduct in-depth research on a specific topic. This involves examining various resources, concepts and ideas about the topic you are researching.

Oral Assessment and/or Individual Presentation	You will be expected to present in a form of either a presentation or discussion on a given topic. This could also be a part of your dissertation where you will be expected to sit a viva voce assessment to defend your work.
Artefact	You will be expected to produce a product such as code implementation or a document containing a set of recommendation and guidelines that demonstrate your ability to innovate to provide solutions to a given problem.
Report	You will be expected to produce a document that outlines activities you have undertaken. This can be either for lab work that you have completed, a work experience and work placement that you undertook or your reflective comments about a specific topic.
Dissertation	This will probably be the biggest document you will have to produce for your entire studies. You will be expected to produce an extended piece of written work, that contains substantial evidence of research, investigations, and possibly implementation, all related to a specific problem you have chosen. Dissertations are the result of your independent work, carried out under the guidance of a supervisor.

Graduate Attribute	Evident in Course Outcomes
Critical and creative thinker	IPY.1, IPY.3, LO4.1, LO4.2, LO4.3, LO4.4, LO4.6, LO4.7, LO5.1, LO5.2, LO5.3, LO5.5, LO6.1, LO6.2, LO6.3, LO6.4, LO6.5
Literate and effective communicator	IEY.1, LO4.5, LO4.6, LO4.7, LO5.2, LO5.4, LO5.6, LO5.7, LO6.2, LO6.3, LO6.4, LO6.5
Entrepreneurial	IPY.1, IPY.2, IPY.3, LO5.5, LO5.6, LO5.7, LO6.5, LO6.6, LO6.7
Global in outlook and engaged in communities	IEY.1, IEY.2, IEY.3, IPY.4, LO4.5, LO4.6, LO5.1, LO5.2, LO5.3, LO5.4, LO5.7, LO6.6
Socially, ethically and environmentally aware	IEY.2, IEY.3, IPY.4, LO4.5, LO5.1, LO5.2, LO5.3, LO5.4, LO5.6, LO5.7, LO6.2, LO6.4, LO6.6, LO6.7

Course Structure

This section shows the core and option modules available as part of the course and their credit value. Full-time Undergraduate students study 120 credits per year. Course structures can be subject to change each academic year following feedback from a variety of sources.

Modules are described as:

- **Core** modules are compulsory and must be undertaken by all students on the course.
- **Option** modules give you a choice of modules and are normally related to your subject area.
- **Electives**: are modules from across the either the whole University or your College. Such modules allow you to broaden your academic experience. For example, where electives are indicated you may choose to commence the study of a foreign language alongside your course modules (and take this through to the final year), thereby adding further value to your degree.
- Additional information may also be included above each level for example where you must choose one of two specific modules.

Modules

Level 4

Module Code	Module Title	Status	UK credit	ECTS
4ELEN010W	Applied Mathematics	Core	20	10
4CSEF001W	Introduction to Cyber Security and Forensics	Core	20	10
4NTCM002W	Introduction to Networks	Core	20	10
4NTCM004W	Programming Methodology I	Core	20	10
4NTCM005W	Programming Methodology II	Core	20	10
4COSC003W	Trends in Computer Science	Core	20	10

Level 5

Module Code	Module Title	Status	UK credit	ECTS
5NTCM006W	Applied Cryptography	Core	20	10
5CSEF001W	Digital Forensics	Core	20	10
5CSEF002W	Network Security	Core	20	10
5CSEF003W	Risk Management and IT Governance (WBL)	Core	20	10
5CSEF004W	Web Applications Security	Core	20	10
5BUIS021W	Agile Project Management and Professional Experience	Option	20	10
5DATA002W	Machine Learning and Data Mining	Option	20	10
5ELEN016W	Operating Systems	Option	20	10
		Elective	20	10

Additional Year

Module Code	Module Title	Status	UK credit	ECTS
5COSC028W	Computer Science and Engineering Industrial Placement	Option	120	60
5COSC027W	Computer Science and Engineering International Year	Option	120	60

Level 6

Module Code	Module Title	Status	UK credit	ECTS
6CSEF002W	Cyber Security and Forensics Final Year Project	Core	40	20
6CSEF004W	Incident Response and Malware Analysis	Core	20	10
6CSEF005W	Wireless Networks Security	Core	20	10
6COSC020W	Applied AI	Option	20	10
6CSEF001W	Cyber Security Threats and Counter Measures	Option	20	10
6CSEF003W	Defensive Programming Techniques	Option	20	10
		Elective	20	10

Please note: Not all option modules will necessarily be offered in any one year. In addition, timetabling and limited spaces

may mean you cannot register for your first choice of option modules.

Professional body accreditation or other external references

The course has been designed with reference to:

- QAA Subject Benchmark for Computing
- Engineering Council Accreditation of Higher Education Programmes (AHEP), fourth edition
- QAA Guidelines for Preparing Programme Specifications
- SEEC Credit Level Descriptors for Further and Higher Education

The British Computer Society (BCS) professional accreditation ensures independent validation that the course meets high standards set by the profession. It also benchmarks the course against those of other institutions both nationally and internationally and supports the continued improvement of the course, highlighting areas of best practice across institutions. For you as a student being on an accredited course provides a pathway to professional registrations such as Chartered IT Professional (CITP), Chartered or Incorporated Engineer (CEng/IEng) and Registered IT Technician (RITTech).

BSc Cyber Security and Forensics is intended to fulfil the educational requirements of BCS for the CITP and partial CEng. Due to the 5-year accreditation timeline the course will be considered for the accreditation in 2027. The accreditation will be backdated to include the first intake from September 2023. On successful completion of this process your course will become accredited in 2027.

The National Cyber Security Center (NCSC) is the UK government organisation dedicated to supporting organisations providing effective cyber security. The NCSC provides a single point of contact for SMEs, larger organisations, government agencies, the general public and departments. They also work collaboratively with other law enforcement, defence, the UK's intelligence and security agencies and international partners. NCSC certification identifies bachelor's, master's and integrated master's degree with well-defined and relevant content delivered to an appropriate standard. BSc Cyber Security and Forensics course will be submitted for provisional NCSC certification in 2024.

Course management

BSc Cyber Security and Forensics course is under the School of Computer Science and Engineering and the management structure supporting the course is as follows:

- the Course Leader is responsible for day to day running and overall management of the course and development of the curriculum.
- the Head of School holds academic responsibility for the course and other courses within the School.
- the Head of the College of Design, Creative and Digital Industries, holds overall responsibility for the course, and for the other courses run by the College.

Academic regulations

The current Handbook of Academic Regulations is available at westminster.ac.uk/academic-regulations.

Course specific regulations apply to some courses.

Academic Support

Upon arrival, an induction programme will introduce you to the staff responsible for the course, the campus on which you will be studying, the Library and IT facilities, additional support available and to your Campus Registry. You will be provided with the Course Handbook, which provides detailed information about the course. Each course has a course leader or Director of Studies. All students enrolled on a full-time course and part time students registered for more than 60 credits a year have a personal tutor, who provides advice and guidance on academic matters. The University uses a Virtual Learning Environment called Blackboard where students access their course materials, and can communicate and collaborate with staff and other students. Further information on Blackboard can be found at https://www.westminster.ac.uk/current-students/studies/your-student-journey/when-you-arrive/blackboard

The Academic Learning Development Centre supports students in developing the skills required for higher education. As well as online resources in Blackboard, students have the opportunity to attend Study Skills workshops and one to one

appointments. Further information on the Academic Learning Development Centre can be found at westminster.ac.uk/academic-learning-development.

Learning support includes four libraries, each holding a collection of resources related to the subjects taught at that site. Students1 can search the entire library collection online through the Library Search service to find and reserve printed books, and access electronic resources (databases, e-journals, e-books). Students can choose to study in the libraries, which have areas for silent and group study, desktop computers, laptops for loan, photocopying and printing services. They can also choose from several computer rooms at each campus where desktop computers are available with the general and specialist software that supports the courses taught in their College. Students can also securely connect their own laptops and mobile devices to the University wireless network.

Support Services

The University of Westminster Student and Academic Services department provide advice and guidance on accommodation, financial and legal matters, personal counselling, health and disability issues, careers, specialist advice for international students and the chaplaincy providing multi-faith guidance. Further information on the advice available to students can be found at https://www.westminster.ac.uk/student-advice

The University of Westminster Students' Union also provides a range of facilities to support students during their time at the University. Further information on UWSU can be found at https://www.westminster.ac.uk/students-union

How do we ensure the quality of our courses and continuous improvement?

The course was initially approved by a University Validation Panel. University Panels normally include internal peers from the University, academic(s) from another university. a representative from industry and a Student Advisor.

The course is also monitored each year by the College to ensure it is running effectively and that issues which might affect the student experience have been appropriately addressed. Staff will consider evidence about the course, including the evidence of student surveys, student progression and achievement and reports from external examiners, in order to evaluate the effectiveness of the course and make changes where necessary.

A Course revalidation takes place periodically to ensure that the curriculum is up-to-date and that the skills gained on the course continue to be relevant to employers. Students meet with revalidation panels to provide feedback on their experiences. Student feedback from previous years is also part of the evidence used to assess how the course has been running.

How do we act on student feedback?

Student feedback is important to the University and student views are taken seriously. Student feedback is gathered in a variety of ways.

- Through student engagement activities at Course/Module level, students have the opportunity to express their voice in the running of their course. Course representatives are elected to expressly represent the views of their peers. The University and the Students' Union work together to provide a full induction to the role of the course representatives.
- There are also School Representatives appointed jointly by the University and the Students' Union who meet with senior School staff to discuss wider issues affecting student experience across the School. Student representatives are also represented on key College and University committees.;
- All students are invited to complete a questionnaire before the end of each module. The feedback from this will inform the module leader on the effectiveness of the module and highlight areas that could be enhanced.
- Final year Undergraduate students will be asked to complete the National Student Survey which helps to inform the national university league tables.

This programme specification provides a concise summary of the main features of the course and the learning outcomes that a student might reasonably be expected to achieve and demonstrate, if they take full advantage of the learning opportunities that are provided. This specification is supplemented by the Course Handbook, Module proforma and Module Handbooks provided to students.

Additional Details

When CS&E Industrial Placement Year is taken the award of BSc Cyber Security and Forensics with Industria Experience is available. When CS&E International Study Year is taken the award of BSc Cyber Security and Forensics with International Experience is available.