Programme specification

1. Overview / factual information

Programme/award title(s)	BSc (Hons) Cybersecurity (Top-Up)
Teaching Institution	New College Durham
Awarding Institution	The Open University (OU)
Date of first OU validation	September 2019
Date of latest OU (re)validation	September 2024
Next revalidation	
Credit points for the award	120
UCAS Code	I140
HECoS Code	
LDCS Code (FE Colleges)	
Programme start date and cycle of starts if appropriate.	September 2024
Underpinning QAA subject benchmark(s)	Computing (2022)
Other external and internal reference points used to inform programme outcomes. For apprenticeships, the standard or framework against which it will be delivered.	The Quality Code for Higher Education benchmark statements for Computing (2022).
Professional/statutory recognition	None
For apprenticeships fully or partially integrated Assessment.	
Mode(s) of Study (PT, FT, DL, Mix of DL & Face-to-Face) Apprenticeship	FT/PT
Duration of the programme for each mode of study	1 Year FT / 2 Years PT
Dual accreditation (if applicable)	
Date of production/revision of this specification	October 2023

Please note: This specification provides a concise summary of the main features of the programme and the learning outcomes that a typical student might reasonably be expected to achieve and demonstrate if s/he takes full advantage of the learning opportunities that are provided.

More detailed information on the learning outcomes, content, and teaching, learning and assessment methods of each module can be found in student module guide(s) and the students handbook.

The accuracy of the information contained in this document is reviewed by the University and may be verified by the Quality Assurance Agency for Higher Education.

2. Programme overview

2.1 Educational aims and objectives

The aim of the award is to provide appropriate and guided learning opportunity for those students that wish to become professional computing practitioners within the IT sector but with a focus on the Cybersecurity sector.

The aims of the programme are as follows:

1. Provide our students with the fundamental knowledge, understanding and skills appropriate to the field of cyber security and related cyber physical technologies.

2. Ensure that our students have a developed awareness of the challenges, risks and impact that the cyber security domain, its pervasiveness, and its technologies, present in a wider global context.

3. Equip the students with the ability to perform critical analysis and apply learnt concepts, principles and practices of cyber security technologies, technique and associated risks to real world scenarios.

4. Develop a high level of judgement, critical thinking, research and problem-solving skills to create a computational artefact.

5. Produce graduates that can identify appropriate practices and perform work within professional, legal, regulatory, and ethical frameworks.

6. Promote a collaborative environment supporting equality, diversity, and inclusion (EDI) and sustainability and entrepreneurship.

7. Encourage and support the further development of interpersonal, team working, decision making skills that will help in the wider context of the cyber security industry.

2.2 Relationship to other programmes and awards (Where the award is part of a hierarchy of awards/programmes, this section describes the articulation between them, opportunities for progression upon completion of the programme, and arrangements for bridging modules or induction)
The FdSc in Cybersecurity was first validated by New College Durham (NCD) in 2017 followed closely by the BSc (Hons) Cybersecurity Top-up first validation in 2019. The NCD FdSc Cybersecurity programme provides students with a Foundation degree qualification and pathway that allows entry to the BSc (Hons) Cybersecurity Top-up, upon successful completion. The FdSc Cybersecurity programme provides the students with a wealth of knowledge, skills and behaviour in computer networking, network security, cyber security operations, emerging technologies, cryptography, security programming fundamentals and in the development of softer skills through work related learning and personal and professional development modules. Prior to entry to the FdSc, students need to have successfully completed a level 3 programme in an IT /Computing related subject and have met the minimum entry requirements of 48 UCAS points. This also includes relevant 'A' levels. Our department offers Level 3 BTEC programmes in IT, and we have recently expanded our portfolio to include the new T-Levels. Our T-Level offerings include Digital Production, Design and Development, as well as Digital Support Services. Each of these programmes are designed to provide a comprehensive curriculum that prepares students for entry into the FdSc. Each also has a stated cybersecurity element, mandated by ifATE standards, which the T-Levels follow. Successful completion of the BSc (Hons) Cybersecurity programme also provides students with the required knowledge, skills, and behaviour to progress to a level 7 qualification in a related subject or entry to employment in a junior position.

2.3 For Foundation Degrees, please list where the 60-credit work-related learning takes place. For apprenticeships, an articulation of how the work based learning and academic content are organised with the award.
Not Applicable

2.4 List of all exit awards
Students who do not achieve 120 credits but do achieve at least 60 credits in any module excluding Computing Project at level 6, will be eligible for an Exit Award: Ordinary 'BSc. Cybersecurity (Top-up)'

3. Programme structure and learning outcomes

(The structure for any part-time delivery should be presented separately in this section.)

Programme Structure - LEVEL 6 Full Time				
Compulsory modules	**Credit points**	**Optional modules**	**Is module compensatable?**	**Semester runs in**
IoT Security	20	No optional modules	Y	1
Cybersecurity Landscape	20		Y	1
Open-Source Intelligence	20		Y	All Year
Principles of Digital Forensics	20		Y	2
Fundamentals of Ethical Hacking	20		Y	All Year
Computing Project	20		N	2

Programme Structure - LEVEL 6 Part Time (attend 1 day per week for 2 years)				
Compulsory modules	**Credit points**	**Optional modules**	**Is module compensatable?**	**Semester runs in**
Cybersecurity Landscape	20		Y	Year 1 - S1
Principles of Digital Forensics	20		Y	Year 1 - S2
Fundamentals of Ethical Hacking	20		Y	Year 1 – All Year
Open-Source Intelligence	20		Y	Year 2 – All Year
IoT Security	20		Y	Year 2 - S1
Computing Project	20	No optional modules	N	Year 2 - S2

2024 - 2025				
September FT 2024 Start + Year 1 PT - SEM 1				
Day 1	EH (AY)	FT PT	CSL	FT PT
Day 2	IoT Sec	FT	OSINT (AY)	FT
FT +Year 1 PT - SEM 2				
Day 1	EH (AY)	FT PT	PDF	FT PT
Day 2	CP	FT	OSINT (AY)	FT

2025 - 26				
September FT 2025 Start + Year 2 PT - SEM 1				
Day 1	EH (AY)	FT	CSL	FT
Day 2	IoT Sec	FT PT	OSINT (AY)	FT PT
FT + Year 2 PT - SEM 2				
Day 1	EH (AY)	FT	PDF	FT
Day 2	CP	FT PT	OSINT (AY)	FT PT

Intended learning outcomes at Level 6 are listed below:

Learning Outcomes – LEVEL 6	
3A. Knowledge and understanding	
Learning outcomes:	**Learning and teaching strategy/ assessment methods**
A1 – Demonstrate a systematic understanding of underlying principles, theories and concepts related to cyber security and related disciplines. A2 – Apply contextual knowledge and critical judgement in the utilisation of tools, techniques and procedures within cyber security and digital forensic context. A3 – Critically evaluate contextual digital technologies and techniques within the domain of cyber security and related fields. A4 – Critically evaluate, the global and national cybersecurity legislative culture and its impact upon organisations and the individual. A5 – Demonstrate the use of threat modelling, policy based risk assessment methodologies, and frameworks to mitigate potential cybersecurity incidents. A6 – Analyse a range of research techniques, theories, and methods. A7 - Integrate principles of project planning using appropriate methodologies.	**Teaching and Learning** The underpinning aims of the programme, is to provide students with a strong practical and theoretical knowledge, understanding and skills, preparing them for the professional world of work within the cybersecurity domain. Delivery is through a variety of remote and insitu lectures, seminars, tutorials, gamification, experiential and problem based practical sessions. Introducing gamification as a teaching and learning method further strengthens student knowledge and experience and introduces competitiveness. Any learning taking place online with this method is then easily transferable to the specialist in-house cybersecurity server lab facilities for further exploration. Guest speakers and industry specialists will be invited to provide a real-world view on some of the topics covered, or to deliver master classes furthering student knowledge and understanding. The VLE (Virtual Learning Environment) (MSTeams + Sharepoint) allows module-based resources and assessments to be stored and accessed by any learner 24x7.

Learning Outcomes – LEVEL 6	
3A. Knowledge and understanding	
	There is an explicit expectation for independent study/learning using the VLE and collaboration with peers through group work/discussion groups/ forums to improve some of the softer skills often required by employers. **Assessment Strategies** All module learning outcomes will be assessed through multiple summative assessments allowing students to demonstrate knowledge and understanding of topics covered. Generally, this will comprise of two components per module and follow a contextualised real-world scenario adding realism to the taks. A variety of summative assessment tools will also be used, such as practical and theoretical assessments via oral presentations, viva's, student created digital artefacts, and written assessments in the form of reports. Each module will follow prior approved assessment and timing guidelines for workload balance. During the modules, students will be given the opportunity to demonstrate knowledge and understanding through supported formative assessment tools. These tools could include practical assessments methods, quizzes, design exercises, online learning tools (gamification) leading to college and global leaderboards.

Learning Outcomes – LEVEL 6	
3A. Knowledge and understanding	
	All feedback is constructive, providing the student with developmental advice on what they have done well and with points for improvement for future work. This is provided promptly following NCD approved guidelines.

3B. Cognitive skills	
Learning outcomes:	**Learning and teaching strategy/ assessment (TLA) methods**
B1 – Critically analyse, review and provide judgement on a given range of concepts and principles relating to cybersecurity technologies and techniques. B2 – Demonstrate judgement, critical thinking, research design, complex problem-solving skills to create a cybersecurity artefact within a computational context. B3 – Recognise and apply risk analysis, risk management techniques and mitigation techniques to a given scenario or problem.	Intellectual cognitive skills are developed through various TLA strategies and methods. These include online and in situ lectures, seminars, tutorials, and practical sessions. Students will be introduced to a range of tools and techniques to analyse research findings and apply risk management techniques. This will lead to the need to interpret and analyse both quantitative and qualitative data effectively. Students will demonstrate effective analytical skills in judging the reliability, validity, and significance of evidence to support their conclusions and/or recommendations Students will employ a range of tools and techniques to analyse cybersecurity technology-based solutions and apply structured problem-solving techniques to produce their proposed artefact. Students will be allocated a project supervisor who will provide 1-2-1 academic tutorials throughout the semester to offer guidance and support throughout systems development of the artefact and reflective evaluation.

3B. Cognitive skills	

3C. Practical and professional skills	
Learning outcomes:	**Learning and teaching strategy/ assessment methods**
C1 – Select, apply appropriate principles, standards, frameworks, tactics, tools, techniques and or procedures to a given cybersecurity scenario. C2 – Collect, analyse and evaluate resulting outcomes of a given problem scenario identifying key stages. C3 – Critically Identify appropriate professional practices, and perform work within a contextual professional, legal & legislative, and ethical framework. Include ethical data management and use, equality, diversity, and inclusion (EDI) along with sustainable practices in the work that they undertake. C4 – Conduct reflective evaluation of all academic and professional outputs. C5 - Develop practical skills by undertaking reflective problem identification and analysis to appropriately design, develop, test, integrate or deploy a cybersecure system and any associated artefacts.	**Teaching and Learning** Practical skills and proffesional skills, at this level, are embeded in every module and delivered through practical activities in the labs with results or findings reported in a professional manner. Students will learn how to apply specific principles, frameworks and standards to real-world problems using industry recognised tools and techniques and then reporting back in either a formal manner or through class group discussions. It is imperative that students gain professional skills and an understanding of the consequences of inaccurate reporting when dealing data acquisition and when dealing with the legal system. The programme will explore routes that will ensure that all assessment are contextually neutral for technical subjects, or will enhance EDI (ethnicy, diversity and inclusion) where case studies and cybersecurity scenarios explore diverse cultural and situational contexts. Students will be encouraged to explore sustainable and ethical practices, ensuring that their professional work will support these outcomes.

3C. Practical and professional skills	
	Assessment Formative and summative assessment strategies include a range of presentations, practical workshops, collaborative work, group discussions, reports and vivas. The project will provide a conduit for demonstrating several professional skills inclusive of project management, time management, design skills and practical artifact creation, concluding in a reflective evaluation.

3D. Key/transferable skills	
Learning outcomes:	**Learning and teaching strategy/ assessment methods**
D1 – Demonstrate effective research skills when planning and gathering data from multiple sources and literature. D2 – Demonstrate the ability to provide valuable insight and be able to communicate the findings to an audience effectively and professionally. D3 – Demonstrate problem solving skills through the application of knowledge on known cyber security issues. D4 - Demonstrate a professional standard of fluency in written communications and an ability to articulate complex issues. D5 – Apply effective time management skills.	The key/transferable skills will be developed and fostered through online and in situ lectures, seminars, tutorials, and practical sessions. These would include effective time management skills, research skills, analysis of information sources, digital skills, meeting deadlines, problem solving and the ability to develop advanced communication skills through being able to articulate complex issues. At this level, students will also be expected to show more autonomy in their independent study and research practices. These transferable skills are learnt and developed across all modules and are assessed both formatively and summatively through presentations, practical workshops, collaborative work, group discussions, reports, and vivas. The project allows for further development of self-initiated project work and experimentation in the creation and formation of an artifact leading to greater confidence in professional practice.

4. Distinctive features of the programme structure

- **Where applicable, this section provides details on distinctive features such as:**
- where in the structure above a professional/placement year fits in and how it may affect progression
- any restrictions regarding the availability of elective modules
- where in the programme structure students must make a choice of pathway/route
- **Additional considerations for apprenticeships:**
- how the delivery of the academic award fits in with the wider apprenticeship.
- the integration of the 'on the job' and 'off the job' training
- how the academic award fits within the assessment of the apprenticeship

The programme offers two delivery modes – Full Time and Part Time (FT/PT).

The FT programme is delivered over two days a week for one academic year over two semesters. The PT programme is delivered over one day a week for two academic years across four semesters. All modules carry a weight of 20 credits including the computing project, totalling to 120 credits.

There are no elective modules or pathways available on the programme.

Fully qualified and experienced staff within the department provides a unique opportunity for the students to profit from up-to-date teaching and learning in the cybersecurity domain.

The programme is delivered in a brand-new state of the art building and with matching teaching facilities and three specialist rooms (network lab, cyber lab, and research & discovery lab).

Specialised resources

- Brand new dedicated servers for ethical hacking, computer forensics and for virtual machine and network deployment supporting any OS of choice.
- All labs (and computer rooms) have Dell Precision 7000 series with IntelCore 12th Gen I9, 16GB RAM and 34" curved monitors.
- Access to servers from anywhere on campus and this will be extended to remote access by September 2024.
- Industry standard Cisco networking equipment with the recent procurement of new switching, wireless and routing hardware to be housed in 4 cabinets in the network lab. This lab also provides direct access to both the curriculum network and a segregated internal Cisco network back the cabinets for hardware configuration.
- Utilisation of gamificaiton resources, such as Packet Tracer from Cisco and open resources from WorldSKills UK and EC-Council

- Range of ethical hacking hardware devices for pen testing for use in the cyber and research lab. These labs are also equiped with segregated networks to allow for ad-hoc network creation IE Raspberry Pi and IoT connection.
- Further plans are in place to facilitate the connection from the cyber lab and research & discovery lab back to the ethical hacking server for IoT pen testing.
- Range of Android and Apple tablets for use with IoT.
- We are currently building a range of IoT devices and components for security assessment and testing. These include Raspberry Pi's, Arduino development board, ESP3688Wifi and components in the first instance.

General resources

- General use computing suites including iMacs.
- 24 x7 access to the college network and associated application software.
- All computing facilities have new CTOUCH interactive screens for teaching and learning.

As a department all technology is reviewed periodically, and any new equipment deemed necessary to the programme will be submitted on a yearly capital bid. There is also a budget to permit the purchasing of non-capital items that would also benefit the programme.

5. Support for students and their learning
(For apprenticeships this should include details of how student learning is supported in the workplace)

The support mechanisms provided are both academic and pastoral support by nature. Quantitative and qualitative evidence is used to gauge the effectiveness and increased utilisation of these services, evidenced particularly in the responses from student questionnaires, and Advice Support and Careers (ASC) service student feedback and evaluation processes. Additional learning support is available to students who have learning difficulties and/or disabilities.

Student Induction
All students joining the programme will undertake an induction programme at their point of entry. The aims of the induction are:

- To provide students with full details of the BSc. (Hons) Cybersecurity (Top-Up) degree programme, including its aims and objectives, modules, skills associated with their studies, its assessment strategy, awarding body regulations and its approach to learning.
- To induct students to the learning resources available to them whilst on the course, such as learning management system (student intranet and VLE) and Library
- To allow students the opportunity to identify issues which need to be resolved.
- To enable students to meet the tutors involved in delivering the programme.
- To meet and interact with fellow students.

- To introduce students to the code of conduct and regulations of the College.
- To make students aware of the relevant systems and structures available to support them, including the Advice, Support Careers Services (ASC), Personal Learning Coach, and the Students Union.

Overview of Support Arrangements

Students who are new to the college, and not previously known to the course team, are encouraged to engage with additional support via Personal Learning Coach (PLC) and Academic Support Tutor to ensure fluid transition into level 6 study.

- **Internal Students (Progressing from FdSc Level 5)**
  Designated personal tutor and 1:1 tutorial.
  Optional Personal Learning Coach (PLC) Support / continued support for those previously using PLC's.
  Access to Academic Support Tutor.

- **International Students**
  Designated personal tutor and 1:1 tutorial.
  Support from International Office.
  Personal Learning Coach (PLC) Support encouraged.
  Access to Academic Support Tutor encouraged.
  Prior access to English for IT resources, provided by Cisco and OpenEDG.

- **External UK Students**
  Designated personal tutor and 1:1 tutorial.
  Personal Learning Coach (PLC) Support encouraged.
  Access to Academic Support Tutor encouraged.

Personal Tutor System
A comprehensive personal tutor system is in place to make sure that students have a direct personal contact with an individual member of the course team to discuss academic and personal matters relevant to their learning.

All students are allocated a personal tutor when first registering to the course. It is intended wherever possible a student will have the same personal tutor for the length of their programme.

The personal tutor will be responsible for the induction programme to ensure students are comfortable with the programme. At the induction, the personal tutor will meet students to ascertain any individual learning or support needs and thereafter will meet with students on a regular basis to monitor progress and discuss any issues arising.

Academic Support
In addition to support from their personal tutor each student will receive academic support from their module tutors. Support is given to students via tutorials at set intervals during the academic year and there is likely to be opportunity within some workshop sessions for additional support. Further support is available within critique-based activities where both tutor and peers can give constructive advice as to the progress and development of group assignment work.

Students have access to a dedicated academic support tutor. This post has been acknowledged as being an invaluable resource enabling students who do not come from an academic background to achieve at a higher education level.

Access to HE (Higher Education) Academic Support Tutor
The HE Academic Support Tutor also supports students with a wide range of HE skills. The HEAST is invited to attend sessions at the beginning of the programme as an introduction to the support that can be offered and promote the links on the intranet. One to one sessions can also be booked which allow for personal feedback on any work that has been submitted.

Pastoral Support
The College is committed to providing high quality, confidential and impartial information, advice, and guidance service. This is provided by the comprehensive Advice, Support Careers (ASC) Service. All students receive induction on the ASC service at the start of their course. The ASC service is designed to provide effective and timely information, advice and guidance on funding and welfare, career planning and provides access to confidential personal counselling support. The ASC service offers appointments and a 'drop-in' service. ASC information is also available to download from the College website, student intranet or from the dedicated ASC area. The Student Development Co-ordinator, based in the Students' Union, also helps with social and health related issues.
The PLC service does not have any specific criteria for referral, and any student who may benefit from such support can access the service. Students can be referred by their tutor, lecturer, and external advisor, ASC or by themselves. This personalised referral system helps in identifying new students as well as continuing communication with progressing students. There is a dedicated page on the College internet and intranet. The service is also advertised via the College visual media system, allowing students in communal areas of college to become aware of the provision.

Career Guidance
Students have access to a comprehensive range of relevant, up to date resources on learning and work via online ASC services and as hard copy which is available at the ASC facility. The ASC staff also provide on-programme support via class-based sessions on Careers Education, including careers management and finding employment both in the UK and abroad. Prospective and actual students are provided with detailed access to careers and funding services for general enquires. Lecturers may also provide useful career guidance during module lessons.

Support with Coursework
Students are supported in their preparation for assessments by their module tutor and where relevant other academic staff within the curriculum team. Students have access to additional academic support particular to assessment tasks from an independent Academic Support Tutor. The tutor offers specific study skills advice and guidance, on for example, Academic Writing, Assignment/Essay Planning and Structuring, The Harvard System (for references & bibliographies using "cite them right"), Online Information Retrieval, Literature Searching, Presentation Skills, Reading Efficiently, Report Writing, Revision and Examination Skills. Electronic advice and guidance booklets are available on the student intranet to download.

To protect students against unfair competition, the college may need to ensure that the students are not submitting assessments which have been copied or plagiarised or which are not the student's own work. The College supports academic integrity by using anti-plagiarism software to enable staff and students to check work for originality. Students can upload their assignments prior to submission for marking and get a report confirming their references. This

can be extremely effective in ensuring against plagiarism and providing a student and staff member with the confidence that the work is original. With the commonplace concerns regarding generative AI (Artificial Intelligence) and its impact on academic integrity, the programme team are currently monitoring the situation and exploring the use of AI review tools to assure standards. This is a continually evolving domain and will be monitored closely.

Module specific material is provided on the college VLE; this information is reviewed and updated annually to coincide with the nature and specific requirements of assignments being delivered each year. Documents include planners, programme handbook, module handbooks, PowerPoint presentations, and assignment briefs.

Self-directed study is an important aspect within the programme to provide students the opportunity to develop their assignments when resources are not available outside of the college campus. Students will have access computer rooms, specialist software, and printing facilities. This is to enable students to build on their practical skills independently to support the level individualised learning expected at level 6.

6. Criteria for admission

(For apprenticeships this should include details of how the criteria will be used with employers who will be recruiting apprentices.)

The College admissions policy is to encourage access to higher education through equal opportunity regardless of race, gender, disability, sexual orientation, religious belief, or age.

To gain entry to the programme a student must satisfy the standard or non-standard entry requirements to the programme. Candidates with non-standard entry applications will be considered based on relevant work experience and attainment of skills, which demonstrate an ability to study at this level.

Standard Entry criteria

- Applicants should have attained, a level 5 qualification (HND / FdSc. / International equivalent 120 ECTS Credits) in a related cybersecurity or computer networking discipline.
- All applicants must be interviewed by the curriculum team (international applicants via internet using Microsoft Teams).
- Must have Level 2 or equivalent in maths and English Language (or a minimum 5.5 IELTS in each band for international applicants).

Non-standard entry criteria:

- Evidence of appropriate cybersecurity or networking and IT experience or employment within the relevant sector.
- All applicants must be interviewed by the curriculum team (international applicants via internet using Microsoft Teams).
- Must have Level 2 or equivalent in maths and English Language (or a minimum 5.5 IELTS in each band for international applicants).

Admissions Process

Once an application has been received it is recorded and acknowledged by the college admissions team. The programme team then views the application.

The process for interview is as follows:

- Applications welcomed through UCAS and NCD Application Form.
- All applicants, progressing or external are interviewed by the curriculum team (International applicants via internet using Microsoft Teams) following a standardised set of questions.
- For external applicants, during the interview they will be asked questions to determine if they have satisfactory knowledge, skills, and behaviours that an internal student would expect to have on completion of the FdSc Cybersecurity programme.
- Whilst holding a level 5 qualification in a computing related area, external applicants would also be required to have, or provide, suitable academic or experiential evidence of knowledge and skills in computer networking, network security and in cyber operations.
- If there are gaps in knowledge, they will be provided with an action plan that will guide them to content that the student will need to study prior to the start of the programme. This could be for example resources from FdSc Cybersecurity programme or a short online training course or reading material from a recommended core text or website. Please see annex 3 at the end of this document for the mapping Process for the Admission of External Students.
- Acceptance or rejection via UCAS and NCD application process after interview.

Entry to the programme is at the discretion of the course team and based upon the combination of successful interview and achievement of 240 credits from previous relevant study that illustrates an ability to meet level 6 course learning outcomes.

7. Language of study

The programme is conducted using English language.

8. Information about non-OU standard assessment regulations (including PSRB requirements)

N/A

9. For apprenticeships in England End Point Assessment (EPA)
(Summary of the approved assessment plan and how the academic award fits within this and the EPA)

N/A

10. Methods for evaluating and improving the quality and standards of teaching and learning

Quality and Performance is embedded across the School. Quality reviews take place at systematic intervals throughout the year at programme level and at area level. These reviews are led by the Teaching and Learning Quality Department which identify any potential performance issues at an early stage.

The Head of School has four Performance Management meetings throughout the year to monitor quality and performance across all areas of the School.
To ensure consistent standards in teaching and learning, Curriculum Managers carry out learning walks across a range of staff covering themes such as maths and English, employability, stretch and challenge and personalised learning. All curriculum staff also have a yearly lesson observation observed by a member of the TLA team.

All curriculum staff engage in staff development activities at least three times a year and are responsible for managing an individual Teaching Learning and Assessment Development Plan to identify areas for improvement and strategies to share best practice. The TLA team within the college are available to support curriculum staff in their development and deliver twilight development and/or bespoke sessions to curriculum areas upon request.

11. Changes made to the programme since last (re)validation

No changes have been made to the OU BSc. (Hons) Cybersecurity (Top-Up) since the original validation in 2019.

Annexe 1: Curriculum map

Annexe 2: Curriculum mapping against the apprenticeship standard or framework (delete if not required.)

Annexe 3: Notes on completing the OU programme specification template

Annexe 1 - Curriculum map

This table indicates which study units assume responsibility for delivering (shaded) and assessing (✓) particular programme learning outcomes.

Level	Study module/unit	A1	A2	A3	A4	A5	A6	A7	B1	B2	B3	C1	C2	C3	C4	C5	D1	D2	D3	D4	D5
	Cybersecurity Landscape	✓		✓	✓	✓			✓		✓	✓			✓			✓	✓		✓
	IoT Security	✓		✓		✓					✓	✓	✓						✓	✓	✓
	Open-Source Intelligence	✓	✓				✓		✓			✓		✓			✓	✓			✓
	Principles of Digital Forensics	✓	✓				✓		✓			✓	✓	✓			✓	✓	✓	✓	✓
	Ethical Hacking	✓	✓	✓	✓		✓		✓			✓		✓			✓	✓	✓		✓
	Computing Project						✓	✓		✓					✓	✓	✓			✓	✓

Annexe 3: Notes on completing programme specification templates

1 **-** This programme specification should be mapped against the learning outcomes detailed in module specifications.

2 – The expectations regarding student achievement and attributes described by the learning outcome in section 3 must be appropriate to the level of the award within the **QAA frameworks for HE qualifications**: http://www.qaa.ac.uk/AssuringStandardsAndQuality/Pages/default.aspx

3 – Learning outcomes must also reflect the detailed statements of graduate attributes set out in **QAA subject benchmark statements** that are relevant to the programme/award: http://www.qaa.ac.uk/AssuringStandardsAndQuality/subject-guidance/Pages/Subject-benchmark-statements.aspx

4 – In section 3, the learning and teaching methods deployed should enable the achievement of the full range of intended learning outcomes. Similarly, the choice of assessment methods in section 3 should enable students to demonstrate the achievement of related learning outcomes. Overall, assessment should cover the full range of learning outcomes.

5 - Where the programme contains validated **exit awards** (e.g. CertHE, DipHE, PGDip), learning outcomes must be clearly specified for each award.

6 - For programmes with distinctive study **routes or pathways** the specific rationale and learning outcomes for each route must be provided.

7 – Validated programmes delivered in **languages other than English** must have programme specifications both in English and the language of delivery.