MSc in Computing

Programme Specifications

2021

AOU / OU-UK

Arab Open University

Faculty of Computer Studies

MSc in Computing

(Cyber Security and Forensics)

F66 (Adapted from UK OU)

Postgraduate Diploma in Computing (Cyber Security and Forensics) – *Exit award only*

E81 (Adapted from UK OU)

Programme Specification

May 2021

Programme specification

1. Overview/ factual information

Programme/award title(s)	• MSc in Computing (Cyber Security and Forensics) • Postgraduate Diploma in Computing (Cyber Security and Forensics) - *Exit award only*
Teaching Institution	The Arab Open University
Awarding Institution	The Arab Open University
Date of first OU validation	2009
Date of latest OU (re)validation	March 2021
Next revalidation	March 2026
Credit points for the award	180 points
UCAS Code	F66 / E81
HECoS Code	NA
LDCS Code (FE Colleges)	NA
Programme start date and cycle of starts if appropriate.	The MSc in Computing Programme was started in September 2011.
Underpinning QAA subject benchmark(s)	MSc in computing (Appendix-D)
Other external and internal reference points used to inform programme outcomes. For apprenticeships, the standard or framework against which it will be delivered.	NA
Professional/statutory recognition	NA
For apprenticeships fully or partially integrated Assessment.	NA
Mode(s) of Study (PT, FT, DL, Mix of DL & Face-to-Face) Apprenticeship	Blended Learning
Duration of the programme for each mode of study	2 Years (FT), and 5 Years (PT)
Dual accreditation (if applicable)	- The Open University (OU), United Kingdom - The Arab Open University (AOU), accredited from the Ministry of Higher Education
Date of production/revision of this specification	30/01/2020

2.1 Educational aims and objectives

2.1.1. Educational aims of the MSc programme in Computing

The MSc in Computing is an intensive programme of study designed specifically for graduates of computing and related disciplines, and for those with appropriate industrial experience. The qualification enables the students to develop their knowledge and skills in computing and to promote a professional attitude to the application of those skills.

The qualification will:

- Give students the knowledge and skills necessary to become an effective professional in the computing industry.
- Develop student's abilities in the critical evaluation of the theories, practices and systems used in a range of areas of computing.
- Provide students with selected specialised areas of study so that you can experience and develop the frontiers of practice and research in focused aspects of computing and its application.
- Encourage students, through the provision of appropriate educational activities, to develop study and transferable skills applicable to your employment and your continuing professional development.
- Enable students to develop a deeper understanding of a specialist area of computing
- Enable students to contribute to future developments in the field
- Provide the opportunity for students to develop and apply research skills, focused on a substantial practical project.

2.1.2. Educational aims of the Cyber Security and Forensics Pathway

The aims of the Cyber Security and Forensics Pathway is to provide students sufficient knowledge, skills, and competencies required for a career in the Cyber Security and Forensics specialization. Therefore, this pathway aims to provide sufficient high-level technological and thinking skills for students to be considered as cyber security and forensics professionals. In addition, in this pathway, several opportunities are provided for students to improve practical skills and theoretical methods. Students will acquire the required technical knowledge, analytical skills and organizational strategies to propose, analyse, develop and carry out a research project of their own. Moreover, students will work with real-world scenario simulations to develop higher-level thinking skills and train them for challenging problems in the field of cyber security and forensics. This allows them to learn the practical, technical, and ethical skills required by industry and gain a critical, analytical, systematic, and comprehensive understanding of the cyber security and forensics field.

- The pathway will provide students with advanced knowledge and understanding of Cyber Security and Forensics theory and concepts.
- The pathway will teach foundations and methods from several Cyber Security disciplines such as data security, network security, cryptography, formal security analysis, secure systems and web applications, multimedia security, digital forensics, privacy-enhancing technologies, and human-centered security.

- The pathway teaches students how to conduct investigations to correctly gather, analyze and present digital evidence to both business and legal audiences.
- It provides students with sufficient knowledge to be able to conduct digital investigation procedures, and skills including evidence handling, note taking and report writing.
- The pathway will teach students to apply their knowledge of scientific methods and gained Cyber Security and digital forensics skills in practice through lab sessions and individual dissertation projects where students will be offered an opportunity to analyze, evaluate and interpret existing Cyber Security and Forensics mechanisms and/or carry out their own research activities.
- The pathway will support students in carrying out their own scientific investigation under the guidance and advice of their supervisor. Students will be able to identify Cyber Security and Forensics problems and find suitable Cyber Security and Forensics mechanisms based on their skills and relevant literature sources.

2.2 Relationship to other programmes and awards

- To gain an MSc in Computing (Cyber Security and Forensics), the student needs to complete the 90 points of compulsory modules and the 30 points of the elective modules for a total of 120 points of study in MSc in Computing (Cyber Security and Forensics).
- The student is also required to carry out research and study in a specialist topic by taking the 60-point course, which is the research project (T802). The student will need to select a research proposal topic which should be in the area of Cyber Security and Forensics. The student may choose a topic from a set offered by the supervisors, or a topic of his own choice that is linked to one or more of the courses offered in the programme.
- Students who fail the MSc Dissertation module T802 or cannot undertake the Dissertation work can obtain as an Exit Award, the Postgraduate Diploma in Computing (E81) - Cyber Security and Forensics Pathway. It can be provided to the students who have successfully completed the 120 points of study.

2.3 For Foundation Degrees, please list where the 60 credit work-related learning takes place. For apprenticeships and articulation of how the work based learning and academic content are organised with the award.

NA

2.4 List of all exit awards
Students who do not successfully complete the Research Project and Dissertation module (T802) can obtain as an Exit Award, the Postgraduate Diploma in Computing (Cyber Security and Forensics) – (E81), if they have successfully completed the 120 points of the pathway study (90 points of compulsory modules and 30 points of elective module). [Annexe 2]

3. Programme structure and learning outcomes for: MSc in Computing (Cyber Security & Forensics) – (F66)

Programme Structure - LEVEL 7					
Compulsory modules: Students need to take 90 points of compulsory courses:	**Credit points**	**Optional modules:** And 30 points from one of the following:	**Credit points**	**Is module compensatable?**	**Semester runs in**
Information Security: M811 (A & B)	30			No	Fall, Spring
Digital Forensics: M812 (A & B)	30			No	Fall, Spring
Network Security: T828 (A & B)	30			No	Fall, Spring
Research Project: T802 (A & B)	60			No	Fall, Spring, Summer
		Data Management: M816 A&B	30	No	Fall, Spring
		Machine Learning in Cyber Security: M818 (A&B); AOU module	30	No	Fall, Spring

Intended learning outcomes at Level 7 are listed below:

Learning Outcomes of the MSc programme in Computing – LEVEL 7	
3A. Knowledge and understanding	
Learning outcomes:	**Learning and teaching strategy/ assessment methods**
On completion of this degree, the students will be able to demonstrate knowledge and understanding of: **PA1:** A wide range of computing tools, techniques, development practices, and systems and their application to business, societal and personal requirements **PA2:** The application of a combination of computing theory and practice, with the ability to use theoretical considerations and practical constraints to guide application **PA3:** Computer systems their development, specification and use, allowing their evaluation against a range of criteria **PA4:** Computing and related standards, codes of practice, quality and evaluation frameworks and their application	The student will acquire knowledge and understanding mainly from the course texts, face-to-face tutorials with supporting material provided via reference texts, commercially available computing environments, specially developed computing environments, computer conferencing and web-based resources. Formal assessment of the taught courses is by way of continuous assessment in the form of the tutor-marked assignment (TMA), submitted at a fixed point in the course, and an examination for each course. Some courses use case study-based assignments where you will choose a project from your personal experience. Assessment of the final research project course is based on the production of a dissertation on a topic of the student's choice in the area of the pathway. Support and advice are delivered at all stages of the dissertation course by the supervisors.

Learning Outcomes of the Cyber Security and Forensics Pathway – LEVEL 7	
3A.1 Knowledge and understanding	
Learning outcomes:	**Learning and teaching strategy/ assessment methods**
Students graduating from the Cyber Security and Forensics Pathway will be able to: **PWA1:** Have an understanding and a critical awareness of current problems and/or new trends in the area of Cyber Security and Forensics, much of which is produced by academic research and professional practice in the security field; **PWA2:** Have a comprehensive understanding of the tools, techniques and approaches of the design, development, implementation and updates of security systems; **PWA3:** Produce innovation and originality in the application of knowledge and available techniques for developing, designing, maintaining and implementing security systems; **PWA4:** Demonstrate critical awareness of the problems of the current research issue; **PWA5:** Participate and understand within the legal, professional and ethical framework as professionals in the domain; **PWA6:** Assess the risk posed by cybercrime within the society; **PWA7:** Construct and formulate new forensic analysis techniques and security strategies. **PWA8:** Compile novel solutions in different situations where Cyber Security systems are applied. **PWA9:** Identify the interaction of economic, social, historical, personal and political issues with networking security measures.	• Key concepts will be taught to the students through lectures, seminars, and tutorials. Furthermore, this learning will be reinforced by independent research. • Students will be evaluated in their knowledge and understanding by assignments, written submissions, and tests. Evaluations are designed to help tutors facilitate the continuous assessment of learning. • Students will also submit comprehensive written original short research papers to enhance their ability to do research and write it appropriately. Evaluations also include the opportunity to improve research skills that should demonstrate technical and theoretical expertise and critical awareness. • The courses will be given as face-to-face tutorials every week, where the tutors introduce the different concepts. The student will acquire knowledge and understanding mainly from the course texts, face-to-face tutorials with supporting material provided via reference texts, commercially available computing environments, specially developed computing environments, computer conferencing and web-based resources.

Learning Outcomes of the Cyber Security and Forensics Pathway – LEVEL 7	
3A.1 Knowledge and understanding	
PWA10: Recognise the main trends within Cyber Security and digital forensics technologies and identify their implications.	• A formal assessment of the taught courses is by way of continuous assessment in the form of the tutor-marked assignment (TMA), submitted in a well-defined time frame during the course delivery, and an examination for each course. TMA is a scientific report on a topic of the student's choice in the area of Cyber Security and Forensics. TMA might provide scientific results that can be published as a conference or a journal paper after making the proper extension. Support and advice are given at all stages of the dissertation course by Tutor. • Also, lab sessions will be offered to students in every course to provide them deep learning and enhance their practical skills in the domain. Every course will have a set of tools (hardware and software) that are required for this purpose.

Learning Outcomes of the MSc programme in Computing – LEVEL 7	
3B. Cognitive skills	
Learning outcomes:	**Learning and teaching strategy/ assessment methods**
On completion of this degree, the students will be able to: **PB1:** Integrate knowledge and skills from various sources into a coherent whole, making appropriate abstractions **PB2:** Deal with complex issues both systematically and creatively, using appropriate tools and techniques, notations and formalisms **PB3:** Pursue an original, independent, practical project involving an appropriate balance of research, development, evaluation and review and to communicate effectively the project aims, processes and outcomes.	Cognitive skills are also assessed in the assignments and examinations of the various courses. Assignments are carefully designed; complex pieces of work that require the skills of analysis, evaluation and integration. The students will also be provided practical activities to develop the cognitive skills, using dedicated software where appropriate. The Research project and dissertation (T802), mandatory for the award of MSc, provides an extended opportunity to further develop and be assessed on these skills.

Learning Outcomes of the Cyber Security and Forensics Pathway – LEVEL 7	
3B.1 Cognitive skills	
Learning outcomes:	**Learning and teaching strategy/ assessment methods**
On completion of the MSc in Computing (Cyber Security and Forensics) degree, the students will be able to: **PWB1:** Apply and critically assess forensic software and hardware tools; **PWB2:** Report digital forensic evidence in a systematic manner in a court of law; **PWB3:** Prepare and apply security policies; **PWB4:** Advise corporate clients on network security issues, analyse current systems and recommended where applicable; **PWB5:** Take decisions in complex and unexpected situations; **PWB6:** Develop independent learning capabilities that are essential for continued professional development; **PWB7:** Provide reasoned arguments on social, historical, economic, political and personal concerns as they relate to Cyber Security and digital forensics.	• Cognitive skills are developed via a range of activities including self-assessment exercises, multi-media tasks, tutor-led discussions, and the exploration of open and complex problems. Tutor-mediated online activities and interactive conference facilities provide an environment for critical discussion and peer interaction. Tutor feedback on formal exercises helps in the development of these skills. • Additionally, cognitive skills will be assessed by addressing problems requiring investigation, analysis and synthesis. These will be examined in TMAs and examinations, and TMAs and the project will offer opportunities to demonstrate integration of knowledge and skills from a range of topics. • The TMA will be dedicated to a unique scientific research problem in the scope of the course. The research problems are selected according to recent IEEE and ACM special issues. Each student should prepare a short paper that can contain a proposed solution to a specific issue (e.g., a lightweight IoT security solution) or it can present a literature review elaborated in a short survey study. This will provide an opportunity for the students to demonstrate their critical thinking and to explore the strengths, weaknesses, and limitations of specific research domains in each course. This will help student to start working and practicing on the preparation of a short research paper in every course. This consequently will help students to strengthen their

Learning Outcomes of the Cyber Security and Forensics Pathway – LEVEL 7	
3B.1 Cognitive skills	
	writing communication skills and to explore new different research topics. • Such gradual development of research skills will allow the students to be well prepared for the master thesis where they should select a research topic, define the research questions, apply a research methodology, conduct experimentation for validating their contribution, and make the proper analysis of the results.

Learning Outcomes of the MSc programme in Computing – LEVEL 7	
3C. Practical and professional skills	
Learning outcomes:	**Learning and teaching strategy/ assessment methods**
On completion of this degree, the students will be able to: **PC1:** recognise and respond to opportunities for innovation in computing	Professional skills are covered specifically in some courses, implicitly as part of the continuous assessment on each taught course and are studied

Learning Outcomes of the MSc programme in Computing – LEVEL 7	
3C. Practical and professional skills	
PC2: recognise social, legal and ethical responsibilities and their appropriate application **PC3:** critically evaluate developments in computing including the identification of limitations and risks, legal issues, cultural and ethical impact and societal and business needs **PC4:** identify needs, articulate goals, locate and employ resources and to follow action plans in support of independent learning and professional development.	and assessed specifically in the Research project and dissertation. All teaching and assessment strategies will help you develop knowledge and skills that are transferable to your workplace, and the programme encourages a problem-solving approach to develop the professional skills through the assignments.

Learning Outcomes of the Cyber Security and Forensics Pathway – LEVEL 7	
3C.1 Practical and Professional skills	
Learning outcomes:	**Learning and teaching strategy/ assessment methods**
On completion of the MSc in Computing (Cyber Security and Forensics) degree, the students will be able to: **PWC1:** Create awareness, evaluate the social need and challenge of digital security; **PWC2:** Apply problem solving skills and knowledge from different techniques, to produce solutions to Computer Security problems;	• Practical and professional skills will be taught and developed throughout the qualification, with support from tutors and subject specialists. TMA, Lab and final reports will include assessment points related to the practical and professional skills.

Learning Outcomes of the Cyber Security and Forensics Pathway – LEVEL 7	
3C.1 Practical and Professional skills	
PWC3: Integrate Cyber Security and Forensics as an appropriate vehicle of postgraduate academic study; **PWC4:** Develop as confident digital security practitioners, to be independent worker aligned to professional standard; **PWC5:** Contribute in professional networking despite the rapid development within the Cyber Security and Forensics community; **PWC6:** Conduct research in the field of Cyber Security and Forensics, and to carry out further study and independent academic or application-based research; **PWC7:** Demonstrate professional attitudes, interpersonal and entrepreneurial skills that are part of a practitioner in the industry; **PWC8:** Be self-motivated and independent learners, self-aware and to reflect critically on your learning, and to embrace your own personal development and career planning.	• Students will be supported in developing a style of independent learning and reflective practice that encourages a professional engagement with the computing discipline, encompassing professional codes of conduct and legal, social and ethical concerns. Some aspects of professional practice will be taught and developed but may not be assessed. • The modules material exposes the students to practical case studies, whereby they have to apply what they have learned in real cases during course and lab sessions. Every course will have its own lab experiments/exercises. Moreover, every course will have a set of open source tools that will be installed in the computer labs. • Students will have to conduct the required experiments (or solve the exercises, depending on each module) during lab sessions, supervised by their tutors. Then, they have to deliver a short report about the results of the experiments. • In addition to the lab sessions, practical and professional skills are also formally assessed in the MTA and final exams. Students will have to answer some exam questions in a lab equipped with the required tools (course dependent) needed to demonstrate their ability to efficiently use them in the course context.

Learning Outcomes of the Cyber Security and Forensics Pathway – LEVEL 7	
3C.1 Practical and Professional skills	
	• All teaching and assessment strategies will help the students to develop knowledge and skills that are transferable to the students' workplace, and the programme encourages a problem-solving approach targeting a set of professional tasks.

Learning Outcomes of the MSc programme in Computing – LEVEL 7	
3D. Key/transferable skills	
Learning outcomes:	**Learning and teaching strategy/ assessment methods**
On completion of this degree, the students will be able to: **PD1:** communicate effectively with technical and non-technical audiences, using appropriate channels and media and where appropriate incorporating research and practice from the forefront of the computing discipline and professional practice.	Key skills (many of which the students already have gained in their workplace) can be further demonstrated and developed by this programme through the course assignments and the Research project and dissertation.

Learning Outcomes of the MSc programme in Computing – LEVEL 7	
3D. Key/transferable skills	
PD2: make and articulate decisions, including collating appropriate evidence and opinions, even in the presence of incomplete information. **PD3:** independently apply problem solving principles; using appropriate underpinning knowledge and skills. **PD4:** review, evaluate, reflect on and critique your own work and the work of others, engaging in peer review processes that lead to innovation and improvement.	

Learning Outcomes of the Cyber Security and Forensics Pathway – LEVEL 7	
3D.1 Key/transferable skills	
Learning outcomes:	**Learning and teaching strategy/ assessment methods**
On completion of the MSc in Computing (Cyber Security and Forensics) degree, The students will be able to: **PWD1:** (a) Operate effectively within the organization, both as group leaders and/or group members; (b) explain tasks and make appropriate use of group members ' abilities; (c) discuss and manage conflict with confidence; and (d) engage effectively in the peer review process;	• Key skills are taught and developed throughout the teaching materials and TMA. In addition, key skills are supported by tutor feedback and guidance around formal activities and assessed exercises.

Learning Outcomes of the Cyber Security and Forensics Pathway – LEVEL 7	
3D.1 Key/transferable skills	
PWD2: Apply a full range of learning resources to perform literature reviews and participate in research; **PWD3:** Concentrate on own and others functioning; engage effectively in the peer review and analysis process and identify ways to enhance your practice; continue to advance your knowledge and understanding and recognize your development needs and develop new high-level skills; **PWD4:** Perform competently research tasks with limited guidance; Classify information to detect the relevant one in addition organize and effectively present information using different media; **PWD5:** Be autonomous and self-critical learner who can act autonomously in the planning and execution of tasks and direct learning for others; **PWD6:** Communicate confidently with other professional and academic contacts in addition to being effective, autonomous and competent during the incident; **PWD7:** Possess the independent learning skills required to continue professional research, making professional use of others where appropriate.	• You will undertake both direct and self-selected reading, and there is progressive development of your engagement and use of these materials. • Various types of assessment questions, project reports and some open-ended activity progress reports will be used to formally assess the targeted skills. • Students will be required to present their research work during classes, this will expose their colleagues (classmates) to different research topics in every course which will enrich their key skills in many research domains.

Learning Outcomes of the Postgraduate Diploma in Computing (Cyber Security and Forensics) - Exit award only	
Learning outcomes:	**Learning and teaching strategy/ assessment methods**
All of the aforementioned learning outcomes are covered EXCEPT for: A1. Knowledge and understanding of the conduct of research processes at MSc level, from problem definition through defining, planning and carrying out a research, to final academic writing, in a selected field relevant to the qualification sought.	The T802 has a Study Guide and 5 module booklets: Preparing for research; Literature reviewing and referencing; Methodology and techniques; Data presentation; analysis, interpretation and Writing skills. These cover research topic development, project planning and execution, the review of body of knowledge, the selection of appropriate methods and their application, collection and interpretation of results to develop conclusions which address the aim of the research, and writing skills to communicate effectively to an appropriate audience whilst demonstrating sufficient academic rigour. Formative assessment in the form of feedback on each TMA given by the supervisor. The TMAs are developmental, i.e. build towards the dissertation. Students will have to pass a viva-voce examination and will be given immediate feedback on the outcome of the examination.

Learning Outcomes of the Postgraduate Diploma in Computing (Cyber Security and Forensics) - Exit award only	
	Summative assessment is based on evidence within the final dissertation and extended abstract. The marking scheme requires students to reach a threshold within each section of the marking scheme. This ensures that a minimum standard is achieved in each essential aspect. The overall score indicates the award of merit and distinction result, thereby ensuring the recognition of compensating strengths within a dissertation.

4. Distinctive features of the programme structure

- **Where applicable, this section provides details on distinctive features such as:**

The MSc Programme will equip students with a set of analytical and Technical skills to work across the disciplines of Cyber Security and Forensics. This qualification meets the requirements of AOU frameworks and principles, such as the Quality Assurance guidelines for postgraduate qualification delivery and academic framework policies.

the programme has the following distinctive features:

- Tutorials are delivered by tutors with research and professional experience in Cyber Security in addition to their academic experience, which contributes to preparing our graduates for the industry.
- Elective modules will be offered to the students on demand as per the advising
- Boosted by the collective intelligence of multiple tutor teams at different branches.
- The programme will be offered by complying the local requirements of the higher education ministries in the offering countries.

The Industrial Advisory Board (IAB) members in each branch will update the demanding labour market skills and support in getting industrial training for the graduates.

5. Support for students and their learning.

Students will learn using online teaching materials posted on LMS, multi-media packages on CD/DVD, Web/OER resources, textbooks, research papers, videos recorded learning objects, and specialised software tools. The learning process involves also the following:

- Attending local workshops in collaboration with the industry (https://aou.edu.lb/ami-lab/News.aspx).
- Attending conferences such as International Symposium on Digital Forensics and Security (http://isdfs.org/), which will be hosted in AOU-Lebanon this year.
- Attending crash courses for acquiring practical skills in this domain such as:
  - Trends in Computer Networks
  - Ethical hacking, including Kali Linux and penetration testing taught by experts from Deutsch Telecom (Germany) and local cyber security experts.
  - Python programming
  - Latex for writing papers and reports

Students learning will be supported also with:

- Self-assessment questions and exercises

- Computer-based investigations, tasks/activities, and open-ended project
- Lab sessions
- Induction on research methodology
- Writing and presenting research work
- Feedback and guidance from tutors and other specialists
- Computer conferences and other online forums
- Study guides, information and guidance packs.

We will assess students learning by using the following:

- Tutor-marked assessments (TMAs)
- Formal examinations
- End of module assessments (EMAs)
- Progress and project reports.

There will be opportunities for student to:

- Apply learning in practical contexts, for example by reflecting on your own engagement with computing systems in a home, work or social setting
- Engage with fellow students, tutors, subject practitioners and academic specialists in online group and small group events
- Engage with research papers and industry white papers at the forefront of the discipline
- Gain exposure to the professional and employability discussions that are shaping the computing profession.
- Using the Digital forensics' lab equipped with software and hardware tools
- Using computer labs with advanced tools for information and network security

6. Criteria for admission

For admission to the programme, the candidate should have:

- BSc degree in:
  - Computing (or a related field) from the Arab Open University or another university recognized by the local ministry of higher education with at least a good average GPA, or
  - Other fields that are restricted to Math, Physics, and Business Computing. In this case, the candidate should have a professional experience in the computing field and have to register at least 12 credits of remedial courses (passing grade at least B). This is essential to confirm that the candidate has the necessary underpinning knowledge and understanding of the basic concepts required to undertake the MSc.

- English test score of:
  - 7.0 in the International English Language Testing System (IELTS), or

- 600 in the Test of English as a Foreign Language (TOEFL) in the Paper-Based Test (PBT) or the equivalent score 100 in the Internet Based Test (IBT).

7. Language of study
English

8. Information about non-OU standard assessment regulations (including PSRB requirements)
AOU assessment strategy is based on general principles and procedures aiming to organize and monitor the examinations at all AOU branches. AOU regulations include validation (pre-assessment moderation) of examination questions and answer keys by external examiners (EE), audit tutors' marking, post-assessment moderation; and 4 tiers of examination committees. Below is a brief about the major assessment principles, policies, and procedures adhered to by FCS. **1. Main principles underpinning the processes of assessment at AOU** AOU has explicit procedures for ensuring that student performance is properly judged and for evaluating how academic standards are maintained through assessment practice. The following are some of the procedures which FCS implements: ▪ All forms of assessment must aim to test the Learning Outcomes (LOs) associated with the module. ▪ The creation and administration of all types of assessment is a team work (e.g. branch module coordinators (BCCs), module chairs (GCCs), programme coordinators (PCs), Deanship team, and External Examiners (EEs)). ▪ All assessment components are reviewed and approved by EEs. ▪ Strict quality measures take place to guarantee fair/correct marking at all branches and across them through Cross branch marking (CBM) [Note: CBM takes place in case the module is offered in different branches] ▪ Sample of students' marked work/scripts from all the modules per branch as well as the CBM are review by EEs.

- There are four tiers of Examination Board structure to approve the final students' results at the end of each semester.

The FCS maintains contact with EEs throughout the semester, and informs them about any issues that arise concerning student assessment. The EEs and the OU Academic Reviewer are involved in establishing the quality of the academic delivery, academic material preparation, assessment and guidance throughout the semester.

2. Composition of the examinations committees

AOU has a four-tiered Examination Board structure consisting of the following:

- Branch Examination Committee (BEC)
- Module Assessment Committee (CAC)
- Faculty Examination Committee (FEC)
- Central Examination Committee (CEC)

All EEs are members of CAC and FEC. The Chief External Examiner is a member of CEC. The composition of all examination boards has been clearly spelled out in the AOU Examination Rules and Regulations. The composition of all examination boards is appropriately maintained by the AOU administration. Marks submitted by branches are considered at HQ by CAC, FEC and ultimately by the CEC. In this way, cross-branch review is achieved.

3. Assessment Components, Weights, and Criteria

The FCS follows the AOU's assessment policies, rules and regulations. The assessments at AOU comprise of 3 essential components with their relative weight as follows:

- Tutor Marked Assignment (TMA) → 20%
- Mid-Term Assessment (MTA) → 30%
- Final Exam → 50%

Weightages of Assessment Components for T802 Thesis module:

For the Thesis module T802 the assessment components and the associated weightages are as follows:

T802	
I Assessment	**Weight**
Presentation	10 %
TMA 01	20 %
II Assessment	**Weight**
Dissertation FX	35 %
Poster	10 %
Defence	25 %
Total	**100%**

Formative and Summative parts of Assessments:

The TMA and the MTA parts of the assessment form the Continuous Assessment component at AOU. The TMA assessment component is part of the Formative Assessment at AOU and detailed feedback is provided to students on their TMA work. The MTA and Final Examinations are part of the Summative Assessment at AOU.

Feedback on Assessment:

The students are provided detailed feedback on their TMA work and this is an essential part of learning at AOU. Tutors use a detailed form for this purpose in which marks for each part of the TMA are clearly distributed. The feedback form also has specific area for the tutors to provide feedback to students concerning their strengths, weaknesses and steps for improvement. The tutor uses this form to provide detailed feedback to students and to suggest corrective and improvement actions. Feedback is also provided to students during in class face-to-face tutorials and during laboratory and office hours maintained by the tutors.

4. Marking, and Cross Branch Marking.

The FCs adopts transparent and fair mechanisms for marking and for moderating marks. All tutors responsible for marking are provided with model answers (approved by EEs) to the questions they will be marking. In addition, grades given by branch tutors are audited by internal staff member to ensure correct marking process.

Cross Branch Marking (CBM) is performed in FCS to ensure uniformity of script marking. The Deanship collects scripts from branches for various modules and these are distributed to other selected branches for the purpose of CBM. CBM reports are generated by the concerned tutors and the Deanship ensures that marking across branches is standardised and uniform.

5. The Assessment Procedures

The assessment procedures are secure and we have full confidence in their integrity and trustworthiness. The following steps are implemented to ensure the security and integrity of the assessment procedures:

- A secured web-based framework is created and organized by the Deanship at the beginning of each semester to exchange the assessment documents. Through such framework, the Deanship centrally control and organize the whole flow of the assessments and documents with all the members involved in the assessment process, where a personal account is created for each GCC, EE, Exam officer of each branch.
- Each GCC prepare the assessment components of his/her module (i.e., TMA, MTA, Final with the model answers and marking guide) and submit them through the aforementioned framework.
- The FCS Deanship communicates the EEs to start their review/feedback on examination papers (through the framework).
- Once the examinations are finalised the Deanship sends them to the Exam Officer at each branches (through the framework)
- The examinations officer prints and keeps them in sealed envelopes under lock and key in a safe storage place at his/her branch.
- The examination officer takes out the examination papers about half-an-hour prior to the start time to give them to invigilators.
- All examinations across all branches are time-synchronized to avoid students of one branch leaking exams to students of other branches.
- Branch directors and branch programme coordinators supervise the administration of the examinations.
- All stages of test administration, the marking of scripts, and the recording of marks are regulated by explicit written instructions and monitored by concerned bodies (programme coordinators, course coordinators, examination committees).
- To guarantee objectivity in marking, students' names and registration numbers do not appear on final examination scripts. Furthermore, in courses taught by more than one tutor, the principle of 'group marking' is applied in the marking of all scripts
- For TMAs, the integrity of the solutions is ensured by providing the solutions to tutors very close to the cut-off date to avoid leakages of solutions due to intentional or unintentional means.
- Plagiarism on TMAs is an issue which all education institutions are grappling with. We now have Turnitin plagiarism detection software to address the issue.

- Once each assessment is marked at each branch, samples of students marked work/script is uploaded along with the audit-trail forms (for finals and MTAs), similarity report (for TMAs), feedback forms (for TMAs) on a secure shared space in order to be reviewed by the EEs.
- The samples of the final exams are subject for Cross branch marking to ensure the fairness of the marking process. The output of the CBMs are made available for the EEs.
- The final results for each course are reviewed by the course assessment committee (CAC), then by the faculty examinations committee (FEC), and finally by the central examination committee (CEC)..

The assessment process is objective in nature since the entire process is open and accessible to EEs' scrutiny.

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)

NA

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

AOU has a continuous monitoring process that aligns with OU. In addition to having a conversation directly with module leaders, students are also invited to feedback on all aspects of the programme to evaluate and improve the quality and standards of teaching and learning.

- **Meeting dates**: Staff / Student Program Forums are held once per semester to ensure that the previous issues raised have been addressed within the programme team and planning for future actions based on feedbacks from those meetings.

- **Programme Feedback Surveys**: Every semester, student assessment surveys occur on a term basis with a different focus, Activities, Assets, and Module and Program. The aim of this feedback process is to provide an opportunity for students to express their views on all aspects of the quality of the program, resources and the institution as a whole. Students are encouraged to complete these surveys because it helps AOU to identify what is going well and what the university needs to fix to continue improving student experience. Feedback from student surveys is considered as part of the Annual Institutional Review of the university, which aims to identify areas of excellence and areas that need to be improved.

- **Continuous Feedback**: AOU also encourages students to provide continuous feedback through conversations with the module and subject leaders.

- **Periodic review and revalidation of programme** by an external panel (Revalidation every 5 years)

- **External Examiner and Academic Reviewer**: to monitor the quality of the learning material and delivery on a regular basis. External examiners should confirm that standards are comparable to similar programmes in the UK, and in line with the Computing Subject Benchmark as well as the UK Higher Education Qualification Framework.

Student views on teaching and learning provisions, is imperative to enhancing student-learning experience therefore student feedback is an important input to quality enhancement. At AOU, student feedback is collected through a structured online student survey wherein student perception is elicited through a satisfaction rating on courses, tutors and tutorials, assessments, academic support and resources. The survey is administered through the online student system, wherein students are encouraged to participate. The survey has been scientifically designed and tested for validity.

The students' perceptions are quantitatively rated to a degree using the psychometric Likert scale as follows:

- Tutors with high academic profile are recruited in the MSc programme. Tutors' performance is followed up by the course coordinator who attends tutorials and provides them with the necessary support and guidance.

- The student feedback questionnaire is the most detailed and structured method for collecting student feedback. Feedback is collected on a semester basis. The questionnaire includes questions on Tutors and Tutorials, Courses and Assessments, Academic Support, and Learning and Physical resources. The last two weeks of each semester, the survey questionnaire dedicated to postgraduate students is posted electronically on LMS (Learning Management System) in an enforced mode. Then, the postgraduate students have to complete the surveys to access the student services and other learning resources and to print the exam slip, this guarantees that input from the majority of the students is collected and hence a wider representation of the students' views. Data is compiled in an Excel Form and exported to SPSS whereby statistical analysis such as the mean, median, mode, maximum, and minimum are generated. As for further comments and other string entries, these are provided in separate files that are examined in full detail by the branch director. Related remarks and requests are forwarded to the MSc programme coordinator and tutors. Necessary actions can be taken at the branch level, and where actions need faculty or Head Quarters approval, the branch raises the issue and follows up through the branch director and its representatives with the relevant faculty or committee for implementation.

- In addition, for each semester, we plan a structured group interview with students, in which we ask them to give us their opinions on the programme and courses. In addition, we carefully plan and design this meeting to reach to constructive debate and to make students feel free to express their views without any personal risk.

To sum up, upon examining the student views on the overall performance of all part-time and full-time tutors teaching on the MSC programme are evaluated against performance including specific teaching aspects.

The performance appraisal of faculty members is vital to objectively evaluate the performance, contributions, and personal development of each academic staff members. The faculty appraisal process requires faculty members to fill in the "Personal Development Planning" section and project their objectives for the upcoming year. This requires a reflection on fulfilment and achievements. Staff appraisal of full-time faculty members is usually performed once per year according to a defined procedure and criteria, which addresses several components including teaching, research, and community service towards the institution to promote its image. The process is working perfectly well whereby, the outcome of the process is a detailed action plan for the academic staff which is usually followed-up by the programme coordinator and branch director. The QA department at the branch monitors the PDP and appraisal process.

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

The following two changes are proposed to the programme in addition to some changes related to the module delivery:

- New elective module will be offered to provide the students modern topics in this domain that are complementary to the existing compulsory modules. We propose a new elective course "M818: Machine learning in cyber security".
- Changing the pathway name to "Cyber Security and Forensics".

Proposed updates for the module delivery:

- Add more practical lab sessions in the different modules to enhance the practical skills of the students (Labs are conducted using a set of modern software tools, which are carefully selected by the module chair).
- Additionally, zero-credit crash courses are also offered for the students to fill some practical gaps in the domain (e.g., Networking, Python, Kali Linux, penetration testing, etc.).
- The TMA (partially or totally) will be more oriented to conduct a short research work in order to allow the students to practice the research methodology in the modules before starting the research project module.

Annexe 1: Curriculum map of the MSc in Computing (Cyber Security and Forensics) – (F66).

Annexe 2: Exit award: Postgraduate Diploma in Computing (Cyber Security and Forensics) – (E81), with curriculum map.

Annexe 3: Notes on completing the OU programme specification template.

Annexe 1 - Curriculum map: MSc in Computing (Cyber Security and Forensics) – (F66)

This table indicates which study units assume responsibility for delivering (shaded) and assessing (✓) particular programme learning outcomes of the Cyber Security and Forensics pathway.

		Learning outcomes of the "Cyber Security and Forensics" pathway																														
Level	**Study module/unit**	**PWA1**	**PWA2**	**PWA3**	**PWA4**	**PWA5**	**PWA6**	**PWA7**	**PWA8**	**PWA9**	**PWA10**	**PWB1**	**PWB2**	**PWB3**	**PWB4**	**PWB5**	**PWB6**	**PWB7**	**PWC1**	**PWC2**	**PWC3**	**PWC4**	**PWC5**	**PWC6**	**PWC7**	**PWC8**	**PWD1**	**PWD2**	**PWD3**	**PWD4**	**PWD5**	**PWD6**	**PWD7**
7	M811 (A&B)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓			✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	M812 (A&B)	✓		✓	✓	✓		✓			✓	✓	✓			✓	✓			✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	T828 (A&B)		✓	✓	✓			✓	✓	✓	✓			✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	M816 (A&B)			✓													✓								✓	✓	✓	✓	✓	✓	✓	✓	✓
	M818 (A&B)		✓	✓	✓			✓								✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	T802 (A&B)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Annexe 2 - Exit Awards: Postgraduate Diploma in Computing (Cyber Security & Forensics) – (E81)

AOU awards a Postgraduate Diploma (E81) only as an exit award in case students fail to complete the research and dissertation module T802. In this case, students should complete 90 points of compulsory modules and 30 points of elective module. Totally, the 120 points are required as described in the following.

- 90 points from the following compulsory courses:
    - Information Security (M811 A&B)
    - Digital Forensics (M812 A&B)
    - Network Security (T828 A&B)

- 30 points from the following elective modules:
    - Data management (M816 A&B)
    - Machine learning in Cyber Security (M818 A&B)

Curriculum map exit award: Postgraduate Diploma in Computing (Cyber Security and Forensics) – (E81)

This table indicates which study units assume responsibility for delivering (shaded) and assessing (✓) particular programme learning outcomes of the exit award: Postgraduate Diploma in Computing (Cyber Security and Forensics) – (E81).

		Learning outcomes of the Cyber Security and Forensics Pathway																														
Level	**Study module/unit**	**PWA1**	**PWA2**	**PWA3**	**PWA4**	**PWA5**	**PWA6**	**PWA7**	**PWA8**	**PWA9**	**PWA10**	**PWB1**	**PWB2**	**PWB3**	**PWB4**	**PWB5**	**PWB6**	**PWB7**	**PWC1**	**PWC2**	**PWC3**	**PWC4**	**PWC5**	**PWC6**	**PWC7**	**PWC8**	**PWD1**	**PWD2**	**PWD3**	**PWD4**	**PWD5**	**PWD6**	**PWD7**
7	M811 (A&B)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓			✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	M812 (A&B)	✓		✓	✓	✓		✓			✓	✓	✓			✓	✓			✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	T828 (A&B)		✓	✓	✓			✓	✓	✓	✓			✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	M816 (A&B)			✓													✓								✓	✓	✓	✓	✓	✓	✓	✓	✓
	M818 (A&B)		✓	✓	✓			✓								✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

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.