Programme specification

1. Overview/ factual information

Programme/award title(s)	1. BSc (Hons) Cyber Security (360 points) 2. DipHE IT & Computing (Cyber Security) (240 points) 3. Cert HE IT & Computing (Cyber Security) (120 points)
Teaching Institution	Arab Open University (AOU)
Awarding Institution	The Open University (OU) The Arab Open University (AOU)
Date of first OU validation	10 June 2021
Date of latest OU (re)validation	----------
Next revalidation	2026
Credit points for the award	360 points
UCAS Code	NA
HECoS Code	100376 - computer and information security (Major/50%) 100365 - computer networks (Major/50%)
LDCS Code (FE Colleges)	NA
Programme start date and cycle of starts if appropriate.	September 2021
Underpinning QAA subject benchmark(s)	Subject Benchmark Statement 2019 by Quality Assurance Agency for Higher Education's (QAA's), refer to https://www.qaa.ac.uk/
Other external and internal reference points used to inform programme outcomes. For apprenticeships, the standard or framework against which it will be delivered.	**External:** • Cyber Security Curricula 2017, ACM-IEEE Computer Society - https://www.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf • OU, UK Website : www.open.ac.uk • The Future of Jobs Report 2020-World Economic Forum https://www.weforum.org/reports/the-future-of-jobs-report-2020 **Internal:** • AOU Mission, Vision and Values - https://www.arabou.edu.kw/university/Pages/vision-and-mission.aspx • Learning and Teaching Strategy, Arab Open University https://www.arabou.edu.kw/blended-learning/Pages/about.aspx • The Bachelor Degree Award Requirements Bylaws, Arab Open University https://www.arabou.edu.kw/university/Documents/Regulations/student/en/The%20Bachelor%20Degree%20Award%20Requirements%20Bylaws.pdf

	• The Bachelor Award Examinations and Assessment Bylaws, Arab Open University https://www.arabou.edu.kw/university/Documents/Regulations/student/en/The%20Bachelor%20Award%20Examinations%20and%20Assessment%20Bylaws.pdf
Professional/statutory recognition	Recognised by Ministries of Higher Education in KSA, Kuwait, Lebanon, Egypt, Oman, Jordan, Bahrain, Sudan, Palestine and validated by Open University Validation Partnership (OUVP), UK.
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	Full time [3.5 - 12] Years.
Dual accreditation (if applicable)	• The Open University (OU), United Kingdom • The Arab Open University (AOU), accredited from the Ministry of Higher Educations (MoHEs)
Date of production/revision of this specification	March 29, 2021

2. Programme Aims and Objectives

2.1 Educational aims and objectives

Cyber Security is concerned of all the technologies and practices that keep computer systems and electronic data safe. And, as more and more of our business and social lives are online, it's an enormous and growing field. Accordingly, offering Cyber Security programme is considered attractive to many educational explorers and industries.

The Cyber Security programme directly addresses the key challenges in Cyber Security and cover the skills gap in the market. This programme is directly contributing to positioning the University as the premier employment- focused and research informed institution, thus allowing the University to make a positive impact on the economy, society and culture of the MENA region and beyond through innovation and engagement.
The Cyber Security programme aims to provide graduates with an ability to:

1- Acquire the necessary theoretical foundation and practical skills in the Cyber Security domain, which will enable them to work effectively in industry and prepare them for postgraduate study.
2- Evaluate and analyse a broad range of tools and techniques, which are at the forefront of defined aspects of Cyber Security and an ability to exercise critical judgement.
3- Critically analyse and apply essential concepts, principles, practices, and research showing effective judgement to frame questions and to solve problems.
4- Investigate and critically evaluate arguments, assumptions, and data to identify the root cause of computer-based malicious activity.
5- Critically review and recognize the legal, social, ethical and professional issues involved in Cyber Security and be guided by the adoption of their best practices.
6- Undertake projects to a professional industry recognized standard, within Computer Security, by the consistent application of development, management and evaluation methods and techniques.
7- Develop transferable skills necessary for employment including initiation, commitment, time-management, decision making, documentation, presentation, and the ability to communicate findings with both specialist and non-specialist audiences.

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)

To obtain the BSc. Honours degree in Cyber Security, students must achieve 360 credit points in core modules. Cyber Security will also be offered as a pathway in the BSc of the ITC programme

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.
NA

2.4 List of all exit awards
• Cert HE IT & Computing (Cyber Security) (120 points) • DipHE IT & Computing (Cyber Security) (240 points)

3. Programme structure and learning outcomes

Programme Structure

Compulsory modules		Credit points	Optional modules	Credit Hours	Is module compensatable?	Semester runs in
Level 0: Foundation Year including University and Faculty requirements						A.Y. 2021-2023
Level 1 (AOU) = Level 4 (OU)	TM129 Technologies in Practice	30	Nil	8	NA	
	MT131 Discrete Mathematics	15	Nil	4	NA	
	MT132 Linear Algebra	15	Nil	4	NA	
	M110 Python Programming	30	Nil	8	NA	
	TM112 Introduction to Computing & Information Technology	30	Nil	8	NA	
Level 2 (AOU) = Level 5 (OU)	TT284 Web Technologies	30	Nil	8	NA	A.Y. 2023-2024
	T216A Cisco Networking (CCNA) Part 1	30	Nil	8	NA	
	T216B Cisco Networking (CCNA) Part 2	30	Nil	8	NA	
	TM256 Cyber Securitys	30	Nil	8	NA	
Level 3 (AOU) = Level 6 (OU)	TM311 Information Security	30	Nil	8	NA	A.Y. 2024-2025
	TM359 System Pentration Testing	30	Nil	8	NA	
	T318 Applied Netowrk Security	30	Nil	8	NA	
	TM471 Graduation Project	30	Nil	8	NA	

Intended learning outcomes are listed below:

Learning Outcomes	
3A. Knowledge and understanding	
Learning outcomes:	**Learning and teaching strategy/ assessment methods**
When you complete your studies for this qualification, you will have knowledge and understanding of: **A1.** Indicate a broad critical range of the fundamental principles, concepts and techniques in relation to design and development of secure digital systems and their secure use. **A2.** Identify theories, practices, and major trends of Cyber Security within networked systems including an appreciation of a range of methods, models and tools to support secure management and analysis of information systems, along with awareness of the various operating systems and platforms. **A3.** Describe the development and implementation of secure systems as well as methods and tools used in the design, implementation and testing including offensive methodologies. **A4.** Recognize the professional, psychological, ethical, social and legal issues that can be associated with the development and deployment of digital systems.	**Learning and teaching strategy:** Knowledge and understanding is acquired from specially prepared teaching texts for majority of modules, supported by self-assessment and in-text questions, reference texts, multi-media packages, directed reading, computer mediated conferencing, web-based resources, and video and audio recordings. Student learning is supported by a tutor, who is the student's first and main point of contact, answering their queries, grading and commenting on their work. AOU's learning/teaching strategy provides contact hours that are equal to 25% of the course credit hours. Thus, AOU students experience the benefits of both the open and traditional university systems. The Cyber Security programme will be delivered through two complementary modes: 1. Face-to-face interactive tutorials, constituting 25% of course credit hours.

Learning Outcomes	
3A. Knowledge and understanding	
A5. Demonstrate the ability to critically analyse, develop and apply digital solutions appropriate to security examination and testing.	2. Interactive self-learning delivered through specially designed teaching and support materials that are conducive for self-learning, constituting 75% of course credit hours. Students work independently with the teaching materials but are encouraged to form self-help groups with other students, communicating face-to-face, email and computer conferencing. **Assessment Strategy:** Assessment of the knowledge and understanding components of the Cyber Security programme is achieved through a combination of continuous assessment and exams. These assessments are central to the teaching of each module, enabling tutors to identify and comment on student knowledge and understanding. Every major module comprises of: ▪ Tutor marked assignments (TMAs) ▪ Midterm Assessment (MTA) ▪ Final Exam However, other assessment mechanisms are used for specific modules and graduation project.

3B. Cognitive skills	
Learning outcomes:	**Learning and teaching strategy/ assessment methods**
On completion of this qualification you will have developed the following cognitive skills: **B1.** Apply and critically evaluate key digital and Cyber Security concepts in a range of contexts. **B2.** Select and apply appropriate techniques and tools for abstracting, modelling, problem solving, designing and testing Cyber Security systems and be aware of the limitations involved **B3.** Compare, contrast and critically analyse and refine specifications and implementations of digital systems from a Cyber Security perspective. **B4.** Device and carry out Cyber Security project that applies and extends your knowledge and understanding and critically reflect on the processes involved and the outcomes of your work. **B5.** Appreciate of the risks, safety issues, legislation and regulatory requirements when designing/managing/deploying/securing a Cyber Security-based system.	**Learning and teaching strategy:** Cognitive skills and processes are introduced at a very simple level at Level 1, primarily via material specifically designed to develop mathematical, programming and technological skills in a progressive way. Although modules at Levels 2 and 3 continue this work, there is significant variation between modules in the degree to which skills are taught explicitly in the module materials. Cognitive skills are promoted in the teaching materials via a range of activities including self-assessment exercises, multi-media tasks and computer-based investigations. They are supported by tutor led face to face discussions and activities. Computer conferencing facilities provide an environment for interaction bringing students, tutors and module team's members together for critical discussions and guidance. Tutor feedback aids the development of these skills. **Assessment Methodology**: Assessment of the cognitive skills of the programme are achieved through a combination of continuous assessment: Every major module comprises of: ▪ Tutor marked assignments (TMAs) ▪ Midterm Assessment (MTA)

3B. Cognitive skills	
	▪ Final Exam The cognitive skills are assessed by questions asking for the application of concepts in new situations for analysis, for synthesis, etc., In some modules, this skill will be assessed using more open-ended design, investigative and project activities. However, other assessment mechanisms are used for specific modules and graduation project

3C. Practical and professional skills	
Learning outcomes:	**Learning and teaching strategy/ assessment methods**
When you complete this qualification you will be able to: **C1.** Analyse, design, evaluate and/or test digital and Cyber Security systems, using appropriate simulation and modelling tools where appropriate. **C2.** Plan and organize yourself and your work appropriately, including keeping systematic records of work in progress and outcomes.	**Learning and teaching strategy:** Practical and professional skills are taught cumulatively throughout the programme. Students are exposed to a variety of introductory courses, which would lead to more advanced courses in Cyber Security. These skills are developed and enhanced through the teaching and communication with the tutor. Modules will include supplementary material that will enrich the learning experience and increase the knowledge learnt. Some modules will adopt the practical hands-on approach that aim to develop the student's skills in the contexts of computation, testing and analysis. Some modules will include

3C. Practical and professional skills	
C3. Address the professional, ethical, social and legal issues that may arise during the development and use of digital and Cyber Security systems. **C4.** Use appropriate professional tools to support your work.	specialised software and tools that will improve the teaching strategy. Modules also provide study guides, assignment and project guides and specimen examination papers. Feedback on assignments provides individual tuition and guidance. Students are taught this material through interactive classroom activities and presentations. In writing their TMA, students make use of different electronic resources such as the internet and the e-library. AOU has developed its e-library through the addition of relevant databases which include academic refereed journals, publications, and conference proceedings to support the students in research based assignments. **Assessment Methodology**: Assessment of the practical skills of the programme is achieved through a combination of continuous assessment: ▪ Tutor marked assignments (TMAs) ▪ Midterm Assessment (MTA) ▪ Final Exam However, other assessment mechanisms are used for specific modules and graduation project

3D. Key/transferable skills	
Learning outcomes:	**Learning and teaching strategy/ assessment methods**
When you complete this qualification you will be able to: **D1.** Communicate information, findings, arguments efficiently with specialized and non-specialized audiences through professional documentation and presentation skills. **D2.** Demonstrate professional working skills including initiation, commitment, decision making as well as the ability to work individually and as part of a team. **D3.** Select, and use accurately, appropriate numerical and analytical techniques to solve problems. **D4.** Use information retrieval skills, gathering and evaluating different types of information. **D5.** Manage their own learning and development, including time management and organizational skills in order to keep up-to-date with digital and Cyber Security systems.	**Learning and teaching strategy:** Transferable skills are developed throughout the programme. The skills of research, presentation, self-reflection and communication are essential to all modules and are increasingly developed as the student progresses throughout the programme. The interactive blended learning delivered through specially designed support material helps students to enhance their own independent learning skills. AOU expect students to naturally develop the skills of learning to learn as they develop through the suite of modules, and this is drawn to their attention through a combination of skills based assessment and tutor feedback during face-to-face tutorials and feedback to assignments. Level-1 and level-2 modules supports the students in acquiring basic skills and level 3 modules expect students to show application of skills developed earlier levels. Higher level modules aim to develop students' ability to conduct independent research using a variety of databases and websites, and to develop group-working skills. As work becomes more complex at these modules, students are tested on their abilities to respond positively to feedback from a variety of audiences, as well as to manage increasingly large workloads. **Assessment Methodology**: Assessment of the key skills of the programme is achieved through a combination of continuous assessment:

3D. Key/transferable skills	
	▪ Tutor marked assignments (TMAs) ▪ Midterm Assessment (MTA) ▪ Final Exam In some cases the assessment is implicit, but where the relevant skills have been taught in the related course material the assessment is generally explicit. However, other assessment mechanisms are used for specific modules and graduation project

3.2 Learning Outcomes of Exit Awards

3.2.1. Cert HE IT & Computing (Cyber Security)

Requirements of Cert HE IT & Computing (Cyber Security) :

Level 1 (AOU) = Level 4 (OU)				
Code	**Module Title**	**Source**	**Point**	**CHs**
TM129	Technologies in practice	OU	30	8
MT131	Discrete Mathematics	AOU	15	4
MT132	Linear Algebra	AOU	15	4
M110	Python Programming	AOU	30	8
TM112	Introduction to Computing and Information Technology	OU	30	8
			120	**32**

Educational aims

The aim of this certificate is to equip you with the basic skills and knowledge that you will need to underpin a career in the computing and IT sector. It will develop your knowledge and understanding of the fundamental technologies, techniques and trends of modern digital technology and introduce you to some of the issues involved in their application. You will gain some practical experience in the use of a modern programming environment and ubiquitous computing devices.

Learning Outcomes

A. Knowledge and understanding:
Students graduating from Cert HE IT & Computing (Cyber Security) should be able to:

A1. Indicate basic principles, concepts and techniques in relation to secure digital systems.
A2. Identify basic theories, and practices of networking and security
A3. Describe basic steps for development and implementation of secure systems.
A4. Recognize main professional, psychological, ethical, social and legal issues in IT.

B. Cognitive Skills:

Students graduating from Cert HE IT & Computing (Cyber Security) should be able to:

B1. Evaluate key digital and cybersecurity concepts in a range of contexts.
B2. Select appropriate techniques and tools for abstracting cybersecurity systems.
B3. Compare specifications of digital systems from a security perspective

C. Practical and/or professional Skills:

Students graduating from Cert HE IT & Computing (Cyber Security) should be able to:

C1. Design outlines of a Cyber Security system
C2. Organize yourself and your work appropriately.
C3. Address basic professional, ethical, social and legal issues in IT
C4. Use appropriate tools to support your work

D. Transferable skills:

Students graduating from Cert HE IT & Computing (Cyber Security) should be able to:

D1. Communicate information with specialized and non-specialized audiences through documentation and presentation skills.
D2. Demonstrate working skills including initiation and commitment as well as the ability to work individually and as part of a team.
D3. Select, and use accurately, appropriate numerical techniques to solve problems.
D4. Use information retrieval skills
D5. Manage their own learning and development.

3.2.2. DipHE IT & Computing (Cyber Security)

Requirements of DipHE IT & Computing (Cyber Security)

Level 1 (AOU) = Level 4 (OU)				
Code	**Module Title**	**Source**	**Point**	**CHs**
TM129	Technologies in practice	OU	30	8
MT131	Discrete Mathematics	AOU	15	4
MT132	Linear Algebra	AOU	15	4
M110	Python Programming	AOU	30	8
TM112	Introduction to Computing and Information Technology	OU	30	8
			120	**32**
Level 2 (AOU) = Level 5 (OU)				
Code	Module Title	Source	Point	CHs
TT284	Web technologies	OU	30	8
T216A	Cisco networking (CCNA) part1	OU	30	8
T216B	Cisco networking (CCNA) part2 TM357	OU	30	8
TM256	Cyber Security	OU	30	8
			120	**32**

Educational aims

The aim of this diploma is to equip you with the knowledge and skills you will need to underpin a broad-based career in the computing and IT sector. As an independent learner you will gain many transferable skills – such as communication, numeracy and organisational – that are valued by employers. You will also acquire an understanding

of the fundamental concepts, technologies and techniques applicable to both computing and IT and a second complementary discipline.

Learning Outcomes

A. Knowledge and understanding:
Students graduating from DipHE IT & Computing (Cyber Security) should be able to:

A1. Indicate a range of the fundamental principles, concepts and techniques in relation to secure digital systems and their secure use.
A2. Identify theories, and practices of cybersecurity within networked systems including an appreciation of a range of methods, models and tools to support secure management
A3. Describe the development and implementation of secure systems as well as methods and tools used in the design and implementation.
A4. Recognize the professional, psychological, ethical, social and legal issues that can be associated with the development and deployment of digital systems
A5. Demonstrate the ability to develop and apply digital solutions appropriate to security examination.

B. Cognitive Skills:

Students graduating from DipHE IT & Computing (Cyber Security) should be able to:

B1. Apply and evaluate key digital and cybersecurity concepts in a range of contexts.
B2. Select and apply appropriate techniques and tools for abstracting, modelling, problem solving, designing cybersecurity systems.
B3. Compare and refine specifications and implementations of digital systems from a cybersecurity perspective
B5. Appreciate of the risks, safety issues, legislation and regulatory requirements when designing/managing a cybersecurity-based system

C. Practical and/or professional Skills:

Students graduating from DipHE IT & Computing (Cyber Security) should be able to:

C1. Design digital and cybersecurity systems, using appropriate simulation and modelling tools where appropriate
C2. Plan and organize yourself and your work appropriately, including keeping systematic records of work in progress and outcomes
C3. Address the professional, ethical, social and legal issues that may arise during the development and use of digital and cybersecurity systems
C4. Use appropriate professional tools to support your work

D. Transferable skills:

Students graduating from DipHE IT & Computing (Cyber Security) should be able to:

D1. Communicate information, findings, arguments efficiently with specialized and non-specialized audiences through professional documentation and presentation skills.
D2. Demonstrate professional working skills including initiation, commitment, decision making as well as the ability to work individually and as part of a team.
D3. Select, and use accurately, appropriate numerical and analytical techniques to solve problems.
D4. Use information retrieval skills, gathering and evaluating different types of information
D5. Manage their own learning and development, including time management and organizational skills in order to keep up-to-date with digital and Cyber Security systems

4. Distinctive features of the programme structure

- **Where applicable, this section provides details on distinctive featurs 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

The Cyber Security Programme is designed to deliver a unique set of courses that can help students to equip a set of analytical, practical and professional skills. This program is designed to meet the requirements of AOU policies and frameworks. In addition, the programme is supported through AOU strategic plan in term of offering new programmes that meet MENA market's needs.

Admitting students to Cyber Security program is consistent with AOU vision and mission. The programme is designed to allow students from different ages and experiences to join the programme and move on smoothly. However, some restrictions might be applied according to the local policies at the offering countries.

The profile of admitting students is according to the mission of AOU and also in compliance with the programme aims and available resources in the various branches. All freshmen shall sit for the Language Placement Test in English pursuant to the standards approved by the University Council. The students score low grade in the admission test shall register for the English orientation course. However, the credit hours due to such courses shall not be included in his/her cumulative averages. Students may study for the first semester of the programme, only the university general requirements. Elective modules are not part of the 360 points validated by the OU but are present to satisfy overall aims of the programme and the labour market needs. The programme comprises of two types of elective modules: faculty mandatory

electives and faculty general electives. Students are allowed to choose modules from the faculty general electives. The elective modules assess a number of learning outcomes that blend well in terms of covering some of the learning outcomes of practical and professional skills, and key/transferable skills from the Cyber Security programme.

In addition to the above mentioned, the programme has the following distinctive features:

- The program will be offered in blended learning teaching style, which provide our students with more flexibilities in term of completing time and without any geographical restrictions. All modules are delivered based on a blended learning model, which consist of 25% face-to-face and 75% is self-learning. The 25% face-to-face consist of 2 hours per week for 8 CHs module, and 2 hours biweekly for the 4 and 3 CHs modules or based on local regulations of MoHE, in addition to one office hour per 2 taught hours. On the other hand, the 75% self-learning depends on the students' self-study based on the teaching materials uploaded on the Central-LMS. Such materials are mainly PowerPoint slides, lectures note, activities, and other e-resources.
- The selected courses in the program is unique and meet the market needs locally and globally.
- Professional staff with good experience in Cyber Security are hired to deliver the core courses.
- The program will enable the students to acquire professional certificates in the domain of Cyber Security.
- 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.

Overall Programme Structure

The 96 Credit Hours core modules are placed in section-3 for validation. Students seeking a BSc Honours degree in Cyber Security (CyS) at AOU must complete at least 131 credit hours including the 96 CH core modules and 35 AOU requirements.

1. Overall CyS Programme Requirements (AOU) (Table-1)
2. General University requirements (Table-2)
3. Faculty compulsory Requirements (Table-3)
4. Faculty elective requirements (Table-4)
5. Faculty core requirements (Table-5)

6. Specialization/Core Requirements (Table-6)

Table 1: Programme Requirements

Requirement type	Credit Hours
University Requirements/ Mandatory	18
University Requirements/ Electives	3
Faculty Requirements/ Mandatory	8
Faculty Requirements/ Electives	6
Specialization Requirements/ Mandatory	96
Total Credit Hours	131

The details of the previous requirements will be described as follows:

University Requirements/ Mandatory (60 points) (18 Credit Hours)

Table 2: Details of University Requirements (Mandatory)

Module	Module Title	Credit	Pre-requisites
AR113	Arabic Communication Skills	3	--
GB102	Principles of Entrepreneurship for	3	--
GR118	Life Skills and Coexistence	3	--
GT101	Learning and Information	3	--
EL111	English Communication Skills I	3	EL099
EL112	English Communication Skills II	3	EL111
Total		18	

** The list of modules and/or the modules contents may be updated/replaced as per AOU university council decision or local accreditation requirements.*

University Requirements/ Electives (10 points) (3 Credit Hours)

Table 3: Details of University Requirements (Electives)

Module Code	Module Title	Credit Hours	Pre-requisites
GR111	Arabic Islamic Civilization	3	--
GR112	Issues and Problems of Development in the	3	--
GR115	Current International Issues and Problems	3	--
GR116	Youth Empowerment	3	--
GR117	Women Empowerment	3	--
GR121	Environment and Health	3	--
GR131	General Branch Requirement	3	--
CH101	Chinese for Beginners (I)	3	--
CH102	Chinese for Beginners (II)	3	CH101
SL101	Spanish for Beginners (I)	3	--
SL102	Spanish for Beginners (II)	3	SL101

FR101	French for Beginners (I)	3	--
FR102	French for Beginners (II)	3	FR101

** The list of modules and/or the modules contents may be updated/replaced as per AOU university council decision or local accreditation requirements.*

Faculty Requirements / Mandatory (30 points) (8 Credit Hours)

Table 4: Details of Faculty Requirements (Mandatory)

Module code	Module title	Credit Hours	Points	Source	Pre-requisites
MST129	Applied Calculus	4	15	AOU	EL099
TM260	Ethics, Law and the Governance in IT	4	15	AOU	TM256[+]

+ TM260 and TM256 can be taken concurrently.
**The TM260 may be replaced by an applied module as per the local accreditation requirement.*

Faculty Requirements / Elective (20 points) (6 Credit Hours)

Table 5: Details of Faculty Requirements (Electives)

Module code	Module title	Credit Hours	Points	Source	Pre-requisites
MS102	Physics	3	10	AOU	EL111
M109	.NET Programming	3	10	AOU	EL111
MT101	General Mathematics	3	10	AOU	--
TM290	Cryptography and Internet Security	3	10	AOU	TM112
MT395	Applied Cyber Security	3	10	AOU	TM260

Note:
1) The student will not be allowed to take more than one elective module per level from the above Table-5.
2) The Cyber Security Students are highly recommended to study MT395 as an elective module

Specialisation/ Core Requirements (96 Credit Hours)

The students will be encouraged to finish each level before moving on to the next level. The details of core modules are given as follows:

Table 6: Details of Specialization/Core Requirements

Level	Code	Module Title	Source	Points	Credit Hours	Pre-requisites
Level 1 (AOU) = Level 4 (OU)	MT131	Discrete Mathematics	AOU	15	4 CHs	EL111
	MT132	Linear Algebra	AOU	15	4 CHs	EL111
	M110	Python Programming	AOU	30	8 CHs	EL111
	TM112	Introduction to computing and information technology	OU	30	8 CHs	M110
	TM129	Technologies in practice	OU	30	8 CHs	M110
Level 2 (AOU) = Level 5 (OU)	TT284	Web technologies	OU	30	8 CHs	TM112
	T216A	Cisco networking (CCNA) part1	OU	30	8 CHs	TM112
	T216B	Cisco networking (CCNA) part2	OU	30	8 CHs	T216A
	TM256	Cyber Security	OU	30	8 CHs	TM129
Level 3 (AOU) = Level 6 (OU)	TM311	Information security	OU	30	8 CHs	T216A
	TM359	System penetration testing	OU	30	8 CHs	TM256
	T318	Applied Network Security	AOU	30	8 CHs	T216B
	TM471	Graduation Project	AOU	30	8 CHs	TM311 or TM359 or T318

Cyber Security Programme – Recommended Study Plan

The academic year at AOU consists of two main academic semesters (Fall and Spring), each consists of 16 weeks, and additional (optional) summer semester of 10 weeks. The following structure plan is a suggested plan based on Fall and Spring semesters.

First Year				
Semester	**Modules**	**Title**	**Credit Hours**	**Prerequisite**
1st (13 CHs)	EL111	English Communication Skills I	3	EL099
	GR118	Life Skills and Coexistence	3	-
	GT101	Computing Essentials	3	-
	MST129	Applied Calculus	4	EL099
2nd (14 CHs)	AR113	Arabic Communication Skills	3	-
	EL112	English Communication Skills II	3	EL111
	MT131	Discrete Mathematics	4	EL111
	MT132	Linear Algebra	4	EL111
Second Year				
Semester	**Modules**	**Title**	**Credit Hours**	**Prerequisite**
1st (14 CHs)	GB102	Principles of Entrepreneurship for Non-Specialists	3	-
	M110	Python Programming	8	EL111
		A module from University Requirement/Elective	3	-

2nd (19 CHs)	TM112	Introduction to Computing and Information Technology	8	M110
	TM129	Technologies in practice	8	M110
		Faculty Elective	3	
Third Year				
Semester	**Modules**	**Title**	**Credit Hours**	**Prerequisite**
1st (16 CHs)	TT284	Web technologies	8	TM112
	T216A	Cisco networking (CCNA) part1	8	TM112
2nd (20 CHs)	T216B	Cisco networking (CCNA) part2	8	T216A
	TM256	Cyber Security	8	TM129
	TM260	Ethics, Law and the Governance in IT	4	TM256
Fourth Year				
Semester	**Modules**	**Title**	**Credit Hours**	**Prerequisite**
1st (20 CHs)	TM311	Information security	8	T216B
	TM359	System penetration testing	8	TM256
	TM471A	Graduation Project-A	4	TM311 or TM359 or T318
2nd (15 CHs)	T318	Applied Network Security	8	T216B
	TM471B	Graduation Project-B	4	TM471A
		Faculty Elective	3	

Cyber Security Programme Structure

Level	**Cyber Security Programme Structure**				
Level 0	**University Requirements (Student may select from variety of modules)**				
Level 1 (AOU) = Level 4 (OU)	**Faculty Requirements**				
	MST129 Applied Calculus (4 CHs)				
	Specialization/Core Requirements				
	TM129 Technologies in Practice (8 CHs)	MT131 Discrete Mathematics (4 CHs)	MT132 Linear Algebra (4 CHs)	M110 Python Programming (8 CHs)	TM112 Introduction to computing and information technologies (8 CHs)
	Faculty Elective				
	MS102 Physics (3 CHs)	M109 .NET Programming (3 CHs)			MT101 General Mathematics (3 CHs)
Level 2 (AOU)	**Faculty Requirements**				
	TM260				

= Level 5 (OU)	Ethics, Law and the Governance in IT (4 CHs)			
	Specialization/Core Requirements			
	TT284 Web technologies (8 CHs)	T216A Cisco networking (CCNA) part1 (8 CHs)	T216B Cisco networking (CCNA) part2 (8 CHs)	TM256 Cyber Security (8 CHs)
	Faculty Elective			
	TM290 Cryptography and Internet Security (3 CHs)			
Level 3 (AOU) = Level 6 (OU)	**Specialization/Core Requirements**			
	TM311 Information security (8 CHs)	TM359 System penetration testing (8 CHs)	T318 Applied Network Security (8 CHs)	TM471 Graduation Project (8 CHs)
	Faculty Elective			
	MT395 Applied Cyber Security (3 CHs)			

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

AOU provides various services to ensure that all students enjoy peaceful and calm stay, and assists them in dealing with any psychological, behavioural, social, educational, financial, health and safety. Students at AOU, including FCS students, are offered various methods of student support. These include:

Learning Management System (LMS)
LMS is a software application / Web-based technology that is used as the major media of communication between students and tutors. LMS main page gives up-to-date information about AOU branches to students from concerned programmes.

LMS features help students to post queries, search for information over a certain topic, read daily posts and comments. Some of the LMS features are as follows:

- Assignment submission through the TMAs submission links
- Discussion forum between all users
- Downloading and uploading processes
- Getting marks
- Using Moodle Instant Messages
- Doing online quizzes
- Accessing mock up exams
- Having access to the E-Library
- adding course page for student/tutors (introduction, communication tools, announcement section, TMA & MTA grades section, contact your teacher section)
- Providing a free plagiarism online checker website on the LMS to help students in checking their TMA similarity.
- Check all university announcements through the LMS Home Page
- Joining LMS online training link

- Having access to all official social media accounts and YouTube channel through the LMS
- Availability of exams schedule and semester calendar etc.
- Availability of E-Books materials are available for all courses as a PDF files

SIS (Student Information System)
AOU established a centralized SIS that integrates data obtained from the branches' student databases. The SIS comprises security, student information, financial services, academic advising and online registration.
The system allows the student to benefit from various electronic services, which include:

- **Online Registration**: to register, update and delete course to be studied at AOU.
- **Online Payment**: to view and pay the fee online.
- **View/Print Semester Timetable**: to view a detailed timetable whenever needed
- **View/Print Student Schedule**: to view a detailed schedule whenever needed
- **View/Print Academic Plan**: to view or print academic plan which is reflective of the studied courses and the remaining courses.
- **View/Print Examination Results**: to view or print unofficial slip of the academic performance (transcript).
- **Create a Student Personal Development Plan (PDP)**: to facilitate the achievements of academic and career goals.
- **Edit Students' Contact profile**: to update the contact details at any time assuring appropriate channel of communication with AOU.
- **View student Exam Slip**: to view the location of the exams.
- **View Advising details**: to view the advising details logged by the advisor.

Student Support Services:

- **Exam Postponing System**: To submit a request to postpone a midterm or final exam with attaching the excuse.
- **Appeal System**: To submit a request for formal review of an academic decision regarding course final examination grade or course continuous assessment marks.
- **Complaint System**: To submit any claim unrelated to academic grades.
- **Inquiries System**: To submit an inquiry related to subject other than appeal and complaint.
- **Disability and Dyslexia Support System**: To submit a description of any disabilities or learning difficulties, so the university can take it in consideration and to provide the necessary services to enable the student to fulfil the intended learning outcomes of their study in a friendly educational and social environment.
- **Induction Programme/Orientation Day**: Students Affairs Department organizes an induction program/orientation day for the new students, in coordination with all administrative and academic departments at the beginning of each semester.
- **Practical laboratory sessions for programming courses**.
- **The university website** www.arabou.edu.kw embodies a lot of guidance and support materials such as: Course Guides, Study Calendars etc.
- **Tutor Contact**: Tutors hold weekly office hours. Tutors are committed to helping students with their problems. All tutors have regular office hours to meet students. The tutors can also be contacted through email. All part-time and full-time tutors are requested to hold two weekly office hours for each taught section. There are also chat sessions online with tutors, and face-to-face feedback sessions. Additionally, emails are constant means by which tutors and students can discuss important ideas related to course material. Furthermore, tutors are available via phones, as well, to answer any urgent queries and offer support.
- **Academic Advising**: Proper academic advising is regarded as a very critical factor affecting student's success and retention and is given exceptional attention in all

branches. Each student is assigned to an advisor. Each advisor should show his advisee the ultimate way to achieve his/her goal while taking into account his strengths, weaknesses, and past performance.

Given that, AOU adopts a blended learning approach that fosters flexibility for the students; two types of advising are offered at the AOU: Face to face advising and E-Advising. Both are offered within certain context and in accordance to specific criteria and guidelines. Advising usually starts at the beginning of the semester, before registration, but continues throughout the semester, where students can meet their advisors in their office during the semester. Face to face advising is mandatory for new comers, and for old students who are not eligible for e-advising. The advisor takes into consideration several factors, among these factors, the financial situation of the student, his workload (part time/full time job), and the student's results in the placement test. The e-advising is offered for continuing students with good GPA and according to the academic advising policy.

Student Counselling Unit: The unit, available at some branches and being adopted for future implementation in many, provides a range of services and activities that help the student to achieve social and psychological adaptation. Individual sessions in which the student meets with the Psychological Counsellor. These sessions help the students to identify the problems facing them or the difficulties that prevent them from achieving their objectives. The Psychological Counsellor helps them to develop skills and capabilities which can help them to handle all kinds of problems.

Written guidance including:

- Student Handbook
- Teaching and Learning policy https://www.arabou.edu.kw/blended-learning/Pages/about.aspx
- The Bachelor Degree Award Requirements Bylaws
- https://www.arabou.edu.kw/university/Documents/Regulations/student/en/The%20Bachelor%20Degree%20Award%20Requirements%20Bylaws.pdf
- The Bachelor Award Examinations and Assessment Bylaws, https://www.arabou.edu.kw/university/Documents/Regulations/student/en/The%20Bachelor%20Award%20Examinations%20and%20Assessment%20Bylaws.pdf
- Equal opportunity policy
- https://www.arabou.edu.kw/university/Documents/Regulations/aou/en/Equal%20Opportunity%20and%20Respect%20for%20Diversity.pdf
- Student Guide on Plagiarism https://www.arabou.edu.kw/students/guide/Pages/cheating.aspx
- Plagiarism Policy https://www.arabou.edu.kw/university/Documents/Regulations/academic/en/Scheme%20of%20penalties%20-%20%20AUG%202020.pdf
- Appeals and complaints http://www.arabou.edu.sa/students/examinations/Pages/student-appeal-system.aspx https://mdl.arabou.edu.kw/oman/pluginfile.php/38519/mod_folder/content/0/7.%20Academic_Appeal_Complaints%20June-2018.pdf?forcedownload=1

ICT facilities:

- IT Help Desk
- Student email
- Wireless Internet access most of the AOU country campuses.
- Student representatives in the Student Council and Branch Council allowing students to share in the decision making process.

- Career planning guidance and services.

6. Criteria for admission *(For apprenticeships this should include details of how the criteria will be used with employers who will be recruiting apprentices.)*
AOU, based on its belief in equal-opportunity education and the two interconnected principles of lifelong learning and education for all, tries to reach out to as many learners as possible. This is why it tries – in those branch countries where there are interested learners – to open, in addition to the main branches themselves, centres in remote areas, making education available to those who may not have an opportunity otherwise. The standard criterion for admission to FCS programme is a high school certificate or its equivalent in the scientific pathway. The FCS follows the AOU's policies and Rules and Regulations, considering the students' entry into the undergraduate CyS programme. The main Entry Requirement into the CyS Programme is a valid High School certificate. Nevertheless, it is worth noting that the admission criteria should fulfil any other conditions determined by the university or competent authorities of the offering branch countries. In all AOU branches students will find the same process of admission through the following link: https://www.arabou.edu.kw/students/pages/apply-to-aou.aspx [Note: This link contains all the details on the admission policies and procedures at the nine branches, as well as the application process.]

7. Language of study
Language of study is English Language.

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)
- 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 examination's 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) à 20%
- Mid-Term Assessment (MTA) à 30%
- Final Exam à 50%

Weightages of Assessment Components for TM471 Graduation Project module:

For the graduation module TM471 the assessment components and the associated weightages are as follows:

- Preliminary presentation: 5 %
- Project Report Part-1: 25%
- Project Presentation (Final): 10%
- Project Report (Final): 35%
- Project deliverable: 25%

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. The Grade Point Average and Equivalent Letter Grades:

AOU follows the Grade Point Average (GPA) on a scale of 0 to 4 in its grading processes, i.e., the different categories of achievement are distinguished by awarding students grades on a scale from 0 to 4.

5. Quality of Assessment:

QAA defined Benchmark standards and the excellence level are taken into consideration in the preparation of the assessment materials. The assessment materials contain questions of appropriate difficulty level standard in order to differentiate students according to their knowledge level and skills. The assessment materials are subject to External Examiners' scrutiny to ensure that standards are compatible to institutions of similar standings in the UK.

6. Marking, Double-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.

There is appropriate arrangement for Group Marking and Double Marking. During Group marking under the supervision of the BCC, internal review is undertaken. Double-marking is undertaken as part of the tutor monitoring process in which the BCC evaluates the performance of the tutors.

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.

7. 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.

As a partner of the OU, UK, AOU is required to meet all academic standards required for validation and accreditation set for UK universities and institutes of higher education. This includes engagement with the QAAD Academic Infrastructure and guidelines provided by the OU, UK. AOU offers its programme in 9 Arab countries, it is crucial to meet the local quality assurance requirements in the offering countries as well.
FCS continuously evaluates the quality and standards of teaching and learning of the programmes and its delivery using different well-designed appraisal and evaluation systems that include key indicators for assessing the performance of the offered programmes. Following are the methods for evaluating and improving the quality and standards of teaching and learning adopted in AOU

10.1 Programme

- Periodic review and revalidation of programme by an external panel (Revalidation every 5 years)
- Programme review by the Quality Assurance agency in the offering countries.

- Annual Monitoring Report (AMR): AMR is a comprehensive document produced at the end of every academic year. The AMR focuses on the developments and challenges related to all matters of teaching and learning environment. The evidence it contains is both qualitative and quantitative in nature. Academic programmes give a detailed account of student enrolment, withdrawal, progression, achievement trends. It also includes an analytical commentary related to the course material, assessment designs, students' learning outcomes, tutor performance, appeals and complaints, grievance systems, student and tutor feedback. This takes account of the views of tutors, students and any issues raised by the external examiners. A detailed action plan is produced accordingly and communicated to all programme coordinators at the eight branches to leverage the strengths and address the weaknesses of the faculty.
- Annual Programme Evaluation (APE): The programme management team at the branches completes an annual programme evaluation report which is submitted as part of the AMR at the end of every academic year. The report consists of analytical commentary of the course material, assessment design, student and tutor feedback, external examiners' comments and responses to external examiners' reports in addition to programme achievements and good practices.
- External Verifier/Examiner
- Quarterly Periodic Reports (QR)
- Subject areas committees at FCS
- Internal Moderation
- Academic reviewer's involvement in the programme review
- Reviews made by local ministries of Higher Education and Quality Assurance agencies.
- Feedback from students: AOU recognizes the importance of student views and feedback. For this purpose, student's views survey is circulated during each semester where students are expected to give a formal feedback on the tutorial, content, delivery style, clarity of learning outcomes, and helpfulness of the tutor towards the student. Student feedback will duly be communicated to the respective module tutor and appropriate measures will be taken, if necessary.
- Feedback from employers: A feedback is gathered through the survey that is conducted at various interval to collect the expectation and feedback of the employers.
- Feedback from Alumni: A feedback is collected about the graduates of AOU by Students Affairs departments in the respective branches at the end of every academic semester. The survey inquires about various aspects such as: employment status, field of employment, relation of employment to the student programme, etc.
- Academic standards committee involvement in programme updates
- Industrial Advisory Board: Keeping abreast of industry developments is an essential aspect of preparing students for their future careers. IAB has been functioning in all the branches at FCS. IAB creates a strong link between industry and the FCS and is contributing in achieving the FCS's goals and objectives. Members of this board are professionals in industry and government who collaborate and build cooperative efforts with the FCS, advice on academic programs, and help in building future faculty direction. FCS alumni are members of this board in all the branches.

10.2 Teaching and Learning

- Feedback from students (through Questionnaires, meetings with PCs, Deans, and VRAA)
- Tutorial/peer monitoring: Peer monitoring is a collegiate approach to identifying tutor's strengths and weaknesses in delivering the course content during tutorials
- General Module Chair (GCC) and Branch Module Coordinators (BCCs) monitor the delivery of their respective modules.
- Exit surveys
- Feedback from AOU Alumni
- Annual staff appraisal
- Tutor development activities such as faculty development forum, workshops and research seminars
- Best tutor awards encourage excellence in tutoring
- Academic Appraisal: is an appraisal system used to evaluate the soundness of academic staff knowledge and skills in delivery. This appraisal system is crucial to deciding the efficacy of their services rendered to the University in terms of the continued need for your services or otherwise. This appraisal process also helps you and the university identify you training needs. The academic appraisal is conducted once a year.

10.3 Assessment

- Quality assurance and oversight by the deanship
- External examiners involvement in module assessment committees (CACs)
- External examiners reports
- Feedback from tutors
- Prompt feedback on student's formative assessment (TMAs, MTA)

10.4 General feedback

- Cross-programme discussions with all branches through the members of the academic committee
- Faculty Council meetings.
- Implementation of best practices in 9 different branches with 4 different Faculties.

10.5 Committees for monitoring and evaluating quality and standards:

- Module Assessment Committee (CAC)
- Faculty Board (FB)
- Academic Committee (AC)
- Academic Standards Committee (ASC)
- AOU's Quality Assurance Committee (QAC)
- Revalidation Panel
- Student-Staff Liaison Committee (SSLC)

10.6 Local recognition by the local Authorities of Higher Education and Validation Agencies

It is worth mentioning that the programme offered at FCS is subject to the conditions and criteria of accreditation in the branch countries where the programmes are offered. Local

accreditation and re-accreditation of the programmes always goes smoothly, as they always meet the standards applied by the accrediting bodies in the branch countries. Nevertheless, the critical recommendations received from these authorities are always taken care with highest importance and FCS use them as an opportunity for further improvement

10.7 Key performance and quality Indicators

- Continuous recognition by local ministries of higher education in 9 countries
- Acceptable student retention, progression and graduation rates.
- High proportion of our Alumni find jobs immediately after graduation
- Examination results are comparable with HESA data provided by CICP
- Research informed tutoring
- Fund raising for research projects by our tutor's team

All parties of the FCS and each in its own capacity, contribute significantly to the improvement of the FCS programme in the following areas:

- Encouraging examples of good practice among the different branches to enhance the FCS programme and disseminating them across AOU branches.
- Conducting Faculty Development Workshops

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

Annexe 1: Curriculum map

Annexe 2: 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	Programme outcomes																		
		A1	A2	A3	A4	A5	B1	B2	B3	B4	B5	C1	C2	C3	C4	D1	D2	D3	D4	D5
Level 1 (AOU) = Level 4 (OU)	TM112	✓			✓		✓						✓	✓	✓		✓	✓	✓	✓
	MT131	✓	✓	✓				✓	✓			✓			✓	✓		✓	✓	
	MT132	✓	✓	✓			✓	✓	✓			✓			✓	✓		✓	✓	
	TM129	✓			✓		✓								✓	✓		✓	✓	✓
	M110			✓					✓				✓		✓	✓	✓	✓	✓	

Level	Study module/unit	Programme outcomes																		
		A1	A2	A3	A4	A5	B1	B2	B3	B4	B5	C1	C2	C3	C4	D1	D2	D3	D4	D5
Level 2 (AOU) = Level 5 (OU)	TT284	✓		✓	✓	✓	✓	✓	✓		✓	✓	✓		✓	✓	✓		✓	✓
	T216A	✓						✓				✓			✓			✓	✓	✓
	T216B		✓				✓					✓						✓	✓	✓
	TM256		✓	✓	✓	✓	✓	✓	✓		✓	✓		✓	✓			✓	✓	✓

Level	Study module/unit	Programme outcomes																		
		A1	A2	A3	A4	A5	B1	B2	B3	B4	B5	C1	C2	C3	C4	D1	D2	D3	D4	D5
Level 3 (AOU) = Level 6 (OU)	TM311		✓	✓		✓	✓		✓		✓	✓	✓	✓		✓		✓	✓	
	TM359		✓	✓		✓	✓	✓	✓			✓	✓	✓		✓	✓	✓		
	T318	✓	✓	✓			✓		✓	✓		✓	✓		✓	✓		✓		
	TM471	✓	✓				✓	✓	✓	✓		✓	✓	✓	✓	✓	✓		✓	

Annexe 2: 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**: https://www.qaa.ac.uk/docs/qaa/quality-code/qualifications-frameworks.pdf

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: subject-benchmark-statement.pdf.

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 then English** must have programme specifications both in English and the language of delivery.