Programme Specification for Franchise for a BSc (Hons) Degree in Cyber Security

STAFFORDSHIRE UNIVERSITY

A·P·I·I·T
ASIA PACIFIC INSTITUTE OF INFORMATION TECHNOLOGY

This document specifies the BSc (Hons) degree in Cyber Security as a 3+0 franchised degree programme from Staffordshire University (SU), UK to be delivered by Asia Pacific Institute of Information Technology (APIIT) which is part of the APIIT Education Group.

March 2013 (updated 27th July 2018)

Contents

1. Vision, Mission and Goals of Asia Pacific Institute of Information Technology (APIIT)

The Vision, Mission and Goals (VMG) of APIIT are as follows:

For internal use only		**Our promise: We enhance Lifelong Career Opportunities**
Term	**Definition [1]**	**APIIT is committed:**
Vision	The aspirations of the organisation.	**“To be a “best-in-class” Institution providing 3+0 Staffordshire University Degree Programmes and home grown Foundation and Diploma programmes to meet the needs of an international market for affordable, high-quality programmes designed to achieve strong employability[2]”**
Mission	Overriding purpose in line with the value and expectations of the stakeholders. Answers the question: what business are we in?	• Provide internationally recognised academic qualifications backed by strong internal and external quality assurance and compliance with MQA • To develop employable professional graduates. • A strong emphasis on staff development at all levels • A learning environment designed to support individual and collective learning through effective teaching and independent learning. • Integrity, honesty, respect for others and the environment in all activities
Goals	General statement of aims or purpose	• To be a leading regional centre of excellence with strong recognition within local and international markets based on the existing reputation of APIIT and SU in these markets. • Embed creativity[3], innovation and technology[4] into the curriculum and delivery of our programmes • Support and complement the policies of the Government of Malaysia by providing opportunities to acquire an academic qualification through higher learning; regardless of nationality, race, sex, religion or ethnic origin. • Contribute to the goal of making Malaysia a developed nation and centre for education.
Strategic Objectives	Long term direction incorporating more precise statement of the goal	To: • Deliver programmes that improve graduate employability by providing them with the necessary knowledge and skills for now and into the future. • Be continuously well informed by being involved in research, development and scholarship. • Encourage debate and innovation through research and scholarship; combining the power of people and technology to improve the way we learn and work. • Offer high quality facilities and educational experience. • Provide an enjoyable environment to learn and study.

APIIT has collaborated with Staffordshire University (SU) since 1994. In 2004 APIIT became a University college and so began to phase out the franchised degrees offered in conjunction with SU. However, using a separate license owned by APIIT it is now proposed to offer a range of new franchise 3+0 programmes with SU which builds on the long standing partnerships. This is in line with the VMG above

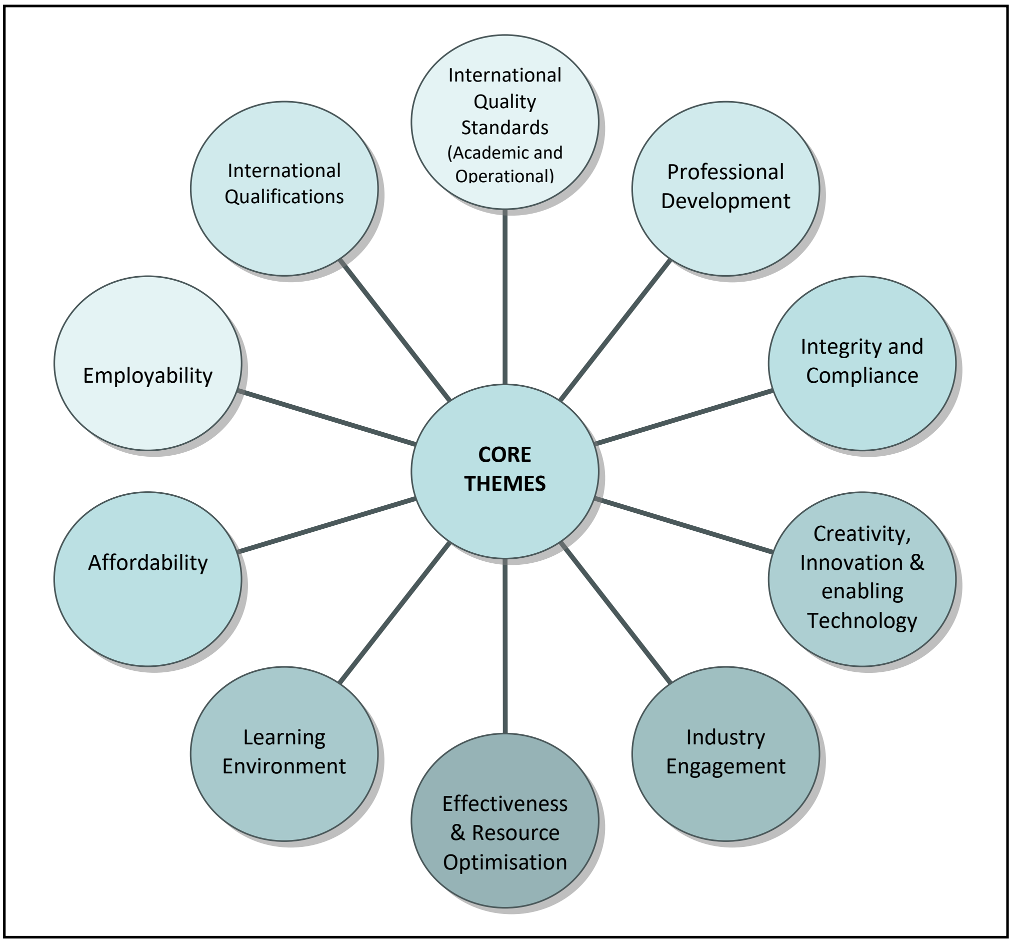
[1] Source: Johnson G E & Scholes K, *Exploring Corporate Strategy* Prentice Hall, 2004

[2] Defined as: Preparing people for work today and in the future. We will prepare students for employment by developing their team working abilities, communication and English language skills, professional approach and life long learning capability. Our programmes and student learning will balance the academic & practical aspects of work and study and will develop innovative and multi disciplinary approaches. We will also create a professional, ethical, and environmentally friendly environment in which research, development, commercialisation and practical scholarship are valued to further support the career opportunities for our students and all staff

[3] Defined as “The application of ideas that are new, regardless of whether the new ideas are embodied in (goods), processes or services, or in work organisation, management or marketing systems” Department of Further Education, Employment, Science and Technology, Australia http://www.innovation.sa.gov.au/sti/pages/gloss

[4] The use of a new technology, item, or process to change what goods and services are provided, the way they are produced, or the way they are distributed.” Canadian Foundation for Economic Education http://mvp.cfee.org/en/glossary.html

The core themes running through all of the development of APIIT are:


International Quality Standards (Academic and Operational)
Professional Development
Integrity and Compliance
Creativity, Innovation & enabling Technology
Industry Engagement
Effectiveness & Resource Optimisation
Learning Environment
Affordability
Employability
International Qualifications
CORE THEMES

2. Aims, Objectives and Learning Outcomes of the Programmes

2.1 Programme Aims

The aims of the Programme are:

1. To equip the student with the knowledge and understanding of security principles within a computing environment, relevant current biometric and security technologies, and their evolution;
2. To apply security concepts, principles and theories to 'real-world' case studies for the student to be able to identify and implement specific security practices, features and techniques to enhance the security of computer and computer based systems;
3. To equip the student with the skills to evaluate, apply and implement security technologies/systems, being capable of assessing risk, providing input into security policy and strategy and providing advice or guidance to organisations on the ways of mitigating the latest threats and trends.
4. To raise student awareness of multi-dimensional challenges of security issues and leading edge knowledge within the cyber security field.
5. To comprehend the contested nature of the cyber security agenda and to develop incisive enquiry skills that allow students to research and debate these contested issues for themselves.
6. To develop competences in a range of appropriate methods and techniques to collect, analyse and present data that will enable students to generate new and warranted knowledge.
7. To provide an intellectually demanding, enjoyable and stimulating programme of study that will enable students to become confident in their ability to receive information critically, to process it logically and to communicate it effectively.
8. To equip students with appropriate employability, enterprise and life-long learning skills so that they can successfully develop their careers after graduation.

The specific Aims for Information Technology also map against the relevant aims of the programme proposed here as follows:

Possess fundamental knowledge, principles and skills in Information Technology	To equip the student with the knowledge and understanding of security principles within a computing environment, relevant current biometric and security technologies, and their evolution;
Have strong analytical and critical thinking skills to solve problems by applying knowledge, principles and skills in Information Technology	To apply security concepts, principles and theories to 'real-world' case studies for the student to be able to identify and implement specific security practices, features and techniques to enhance the security of computer and computer based systems To comprehend the contested nature of the cyber security agenda and to develop incisive enquiry skills that allow students to research and debate these contested issues for themselves
Posses the ability to design, implement, and manage Information Technology solutions and resources, and recognise the impact of technology on	To equip the student with the skills to evaluate, apply and implement security technologies/systems, being capable of assessing risk, providing input into security policy and strategy and providing advice or guidance to organisations on the ways of mitigating the latest threats and trends.

individuals, organisations and society	To raise student awareness of multi-dimensional challenges of security issues and leading edge knowledge within the cyber security field.
Possess skills to integrate various technology solutions	To apply security concepts, principles and theories to ‘real-world’ case studies for the student to be able to identify and implement specific security practices, features and techniques to enhance the security of computer and computer based systems

2.2 Programme Learning Outcomes

At the end of your studies you should be able to:

Knowledge & Understanding

Demonstrate a systematic understanding of computing concepts and principles showing the acquisition of coherent and detailed knowledge, at least some of which is at, or informed by, the forefront of computing research and development.

Demonstrate a critical understanding of the process of evidence gathering, preparation and delivery of testimony as an expert witness concerning computer based crimes.

Demonstrate a critical understanding of, and ability to apply, the concepts, principles, theories and techniques used in Cyber Security for the development and maintaining of secure IT systems

Learning

Develop lines of argument and evaluate possible approaches, tools, techniques and solutions based on knowledge of underlying Cyber Security concepts and principles, while understanding the uncertainty, ambiguity and limitations of this knowledge.

Enquiry

Initiate and carry out projects within Cyber Security

Ethically gather information pertaining to computing problems, possible solutions, and the success of these solutions, from existing or potential users and/or organisations using recognised techniques.

Find, critically evaluate, manage, apply, and understand information from a range of sources, acknowledging the cultural, ethical, economic, legal, and social issues surrounding the use of information.

Analysis

Critique current research in Cyber Security and critically evaluate arguments, assumptions, abstract concepts and data (that may be incomplete) to draw conclusions

Problem Solving

Develop appropriate questions and strategies to achieve a solution (or identify a range of solutions) to a Cyber Security-based problem.

Plan and carry out a large and complex Cyber Security project

Communication

Communicate ideas, problems and solutions to both specialist and non-specialist audiences in a variety of forms

Write a structured formal report using appropriate referencing, and techniques for documentation.

Application

Apply the concepts, principles, theories and techniques, including those at the forefront of computing knowledge, of Cyber Security to the process of solving complex Cyber Security-based problems

Reflection

Work in a professional manner, recognising the legal, social, ethical and professional issues involved in the exploitation of computer technology, and being guided by the adoption of appropriate professional, ethical and legal practices.

3. Mapping of Vision, Mission and Goals (VMG) and the Programme Aims

The following maps the aims of the Programme against the VMG.

Programme Aims	**Key elements of APIIT's VMG**
1. To equip the student with the skills to evaluate, apply and implement security technologies/systems, being capable of assessing risk, providing input into security policy and strategy and providing advice or guidance to organisations on the ways of mitigating the latest threats and trends.	High-quality programmes designed to achieve strong employability
2. To equip the student with the knowledge and understanding of security principles within a computing environment, relevant current biometric and security technologies, and their evolution.	Integrity, honesty, respect for others and the environment in all activities
3. To apply security concepts, principles and theories to 'real-world' case studies for the student to be able to identify and implement specific security practices, features and techniques to enhance the security of computer and computer based systems.	
4. To raise student awareness of multi-dimensional challenges of security issues and leading edge knowledge within the cyber security field.	
5. To comprehend the contested nature of the cyber security agenda and to develop incisive enquiry skills that allow students to research and debate these contested issues for themselves.	Embed creativity, innovation and technology into the curriculum and delivery of our programmes
6. To develop competences in a range of appropriate methods and techniques to collect, analyse and present data that will enable students to generate new and warranted knowledge.	Deliver programmes that improve graduate employability by providing them with the necessary knowledge and skills for now and into the future.
7. To provide an intellectually demanding and stimulating course that will enable students to become confident in their ability to receive information critically, to process it logically and to communicate it effectively	Encourage debate and innovation through research and scholarship; combining the power of people and technology to improve the way we learn and work.
8. To equip students with appropriate employability, enterprise and life-long learning skills so that they can successfully develop their careers after graduation.	Develop employable professional graduates

4. Mapping of Programme Learning Outcomes and MQF Learning Outcomes Domains

All APIIT Programmes identify learning outcomes according to the categories below and also each module, as well as identifying the Learning Outcomes in the MQF which are addressed, also lists the learning and employability skills to be introduced, and/or developed and assessed. The table below identifies the SU learning outcomes, learning skills and employability skills and maps these against the MQF learning outcomes domains. It also identifies the SU Graduate attributes and maps these against the APIIT employability skills.

Generic Learning Outcomes Domains		Learning Skills	Employability Skills	SU Generic Graduate attributes
Malaysian Qualifications Framework	SU			
Knowledge	Knowledge and understanding	Critical thinking & analysis	Knowledge Subject defined skills Critical thinking	**Discipline Expertise:** Have an understanding of the forefront of knowledge in their chosen field
Practical skills	Application		Techniques Research Academic Writing skills Taking tests	
Social skills and responsibilities		Self & cultural awareness	Enthusiasm Self and cultural awareness Global awareness	**Global Citizenship:** Have an understanding of global issues and of their place in a globalised economy
Values, attitudes and professionalism			Reflection Ethical Personal manner and appearance Timeliness and punctuality Integrity Trustworthiness	**Professionalism:** Be prepared to be work-ready and employable and understand the importance of being enterprising and entrepreneurial (and see below)
Communications, leadership and team skills	Communication	Communication Team working	Verbal Writing English language Presentational Team working Motivating others Empathy Assertiveness Leadership	**Communication and Teamwork:** Be a effective communicator and presenter and able to interact appropriately with a range of colleagues Have developed the skills of independence of thought and (when appropriate) social interaction through teamwork
Problem solving skills	Enquiry Analysis Problem solving	Effective problem solving Creativity & innovation	Enquiry Analytical Problem solving Creativity Innovation Ingenuity Imagination	**Reflective and Critical Learner:** Have the ability to carry out inquiry-based learning and critical analysis Be a problem solver and creator of opportunities **Lifelong Learning:** Be technologically, digitally and information literate Be able to apply to a range of life experiences to facilitate life-long learning and life-long success.
Information management and lifelong learning skills	Learning	ICT skills Learning Numeracy & quantitative skills	ICT Numeracy Learning Independent work and autonomy Personal development	
Managerial and entrepreneurial skills	Reflection	Self management	Adaptability Managerial and supervisory Audience focus Self management Drive to achieve	**Professionalism:** Be prepared to be work-ready and employable and understand the importance of being enterprising and entrepreneurial

The following maps the Programme Learning Outcomes and *Generic SU graduate attributes* applicable to all SU Programmes with the MQF domains.

MQF Domain	SU Programme Learning Outcomes
Knowledge	*Generic SU graduate attribute:* **Discipline Expertise:** Have an understanding of the forefront of knowledge in their chosen field **Knowledge & Understanding** Demonstrate a systematic understanding of computing concepts and principles showing the acquisition of coherent and detailed knowledge, at least some of which is at, or informed by, the forefront of computing research and development. Demonstrate a critical understanding of the process of evidence gathering, preparation and delivery of testimony as an expert witness concerning computer based crimes. Demonstrate a critical understanding of, and ability to apply, the concepts, principles, theories and techniques used in Cyber Security for the development and maintaining of secure IT systems.
Practical skills	**Application** Apply the concepts, principles, theories and techniques, including those at the forefront of computing knowledge, of Cyber Security to the process of solving complex Cyber Security-based problems
Social skills and responsibilities	*Generic SU graduate attribute:* **Global Citizenship:** Have an understanding of global issues and of their place in a globalised economy
Values, attitudes and professionalism	*Generic SU graduate attribute:* **Professionalism:** Be prepared to be work-ready and employable and understand the importance of being enterprising and entrepreneurial
Communications, leadership and team skills	*Generic SU graduate attribute:* **Communication and Teamwork:** Be a effective communicator and presenter and able to interact appropriately with a range of colleagues Have developed the skills of independence of thought and (when appropriate) social interaction through teamwork **Communication** Communicate ideas, problems and solutions to both specialist and non-specialist audiences in a variety of forms. Write a structured formal report using appropriate referencing, and techniques for documentation.

Problem solving skills	*Generic SU graduate attribute:* **Reflective and Critical Learner:** Have the ability to carry out inquiry-based learning and critical analysis Be a problem solver and creator of opportunities **Enquiry** Initiate and carry out projects within Cyber Security. Ethically gather information pertaining to computing problems, possible solutions, and the success of these solutions, from existing or potential users and/or organisations using recognised techniques. Find, critically evaluate, manage, apply, and understand information from a range of sources, acknowledging the cultural, ethical, economic, legal, and social issues surrounding the use of information. **Analysis** Critique current research in Cyber Security and critically evaluate arguments, assumptions, abstract concepts and data (that may be incomplete) to draw conclusions. **Problem Solving** Develop appropriate questions and strategies to achieve a solution (or identify a range of solutions) to a Cyber Security-based problem. Plan and carry out a large and complex Cyber Security project.
Information management and lifelong learning skills	*Generic SU graduate attribute:* **Lifelong Learning:** Be technologically, digitally and information literate. Be able to apply to a range of life experiences to facilitate life-long learning and life-long success. **Learning** Develop lines of argument and evaluate possible approaches, tools, techniques and solutions based on knowledge of underlying Cyber Security concepts and principles, while understanding the uncertainty, ambiguity and limitations of this knowledge.
Managerial and entrepreneurial skills	*Generic SU graduate attribute:* **Professionalism:** Be prepared to be work-ready and employable and understand the importance of being enterprising and entrepreneurial **Reflection** Work in a professional manner, recognising the legal, social, ethical and professional issues involved in the exploitation of computer technology, and being guided by the adoption of appropriate professional, ethical and legal practices.

The above LOs have been mapped against the generic learning outcomes for a degree in the Information Technology Programme standards as below:

Generic LOs	APIIT LOs

Apply skills and principles of lifelong learning in academic and career development	**Lifelong Learning:** Be technologically, digitally and information literate. Be able to apply to a range of life experiences to facilitate life-long learning and life-long success. **Learning** Develop lines of argument and evaluate possible approaches, tools, techniques and solutions based on knowledge of underlying Cyber Security concepts and principles, while understanding the uncertainty, ambiguity and limitations of this knowledge.
Communicate effectively with peers, clients, superiors and society at large	**Communication:** Be an effective communicator and presenter and able to interact appropriately with a range of colleagues Communicate ideas, problems and solutions to both specialist and non-specialist audiences in a variety of forms. Write a structured formal report using appropriate referencing, and techniques for documentation.
Demonstrate teamwork, leadership. Interpersonal and social skills	**Teamwork** Have developed the skills of independence of thought and (when appropriate) social interaction through teamwork
Utilise relevant techniques and demonstrate analytical and critical thinking skills in problem solving	**Enquiry** Initiate and carry out projects within Cyber Security. Ethically gather information pertaining to computing problems, possible solutions, and the success of these solutions, from existing or potential users and/or organisations using recognised techniques. Find, critically evaluate, manage, apply, and understand information from a range of sources, acknowledging the cultural, ethical, economic, legal, and social issues surrounding the use of information. **Analysis** Critique current research in Cyber Security and critically evaluate arguments, assumptions, abstract concepts and data (that may be incomplete) to draw conclusions. **Problem Solving** Develop appropriate questions and strategies to achieve a solution (or identify a range of solutions) to a Cyber Security-based problem. Plan and carry out a large and complex Cyber Security project.
Demonstrate professionalism and social and ethical considerations in accordance with ethical and legal principles	**Professionalism:** Be prepared to be work-ready and employable and understand the importance of being enterprising and entrepreneurial **Reflection** Work in a professional manner, recognising the legal, social, ethical and professional issues involved in the exploitation of computer technology, and being guided by the adoption of appropriate professional, ethical and legal practices.
Apply broad business and real world perspectives daily and demonstrate entrepreneurial skills	**Global Citizenship:** Have an understanding of global issues and of their place in a globalised economy **Professionalism:** Be prepared to be work-ready and employable and understand the importance of being enterprising and entrepreneurial

Demonstrate knowledge and understanding of essential facts, concepts, principles, and theories related to Information Technology	Demonstrate a systematic understanding of computing concepts and principles showing the acquisition of coherent and detailed knowledge, at least some of which is at, or informed by, the forefront of computing research and development. Develop lines of argument and evaluate possible approaches, tools, techniques and solutions based on knowledge of underlying Cyber Security concepts and principles, while understanding the uncertainty, ambiguity and limitations of this knowledge
Apply theoretical principles of Information Technology in relevant areas	Apply the concepts, principles, theories and techniques, including those at the forefront of computing knowledge, of Cyber Security to the process of solving complex Cyber Security-based problems
Design implement and manage Information Technology solutions and resources, and recognise the impact of technology on individuals, organisation and society	Demonstrate a critical understanding of, and ability to apply, the concepts, principles, theories and techniques used in Cyber Security for the development and maintaining of secure IT systems. Work in a professional manner, recognising the legal, social, ethical and professional issues involved in the exploitation of computer technology, and being guided by the adoption of appropriate professional, ethical and legal practices
Integrate various technology solutions	Develop appropriate questions and strategies to achieve a solution (or identify a range of solutions) to a Cyber Security-based problem. Plan and carry out a large and complex Cyber Security project. Apply the concepts, principles, theories and techniques, including those at the forefront of computing knowledge, of Cyber Security to the process of solving complex Cyber Security-based problems

5. Measurement of the Programme Learning Outcomes

The Learning Outcomes specified for the Programme are each measured in the modules which combine to make up the curriculum for the Programme. Each Module Descriptor identifies the Learning Outcomes for the module and maps these against the MQF Learning Outcome domains. Each Module Descriptor also identifies the employability (transferable) skills which are either introduced or developed and whether or not they are assessed in the module.

The following table maps the module Learning Outcomes against the MQF Learning Outcomes domains. The Domains and skills have already been mapped to the APIIT learning Outcomes in Section 4 herein.

Thus as the modules collectively address the Learning Outcomes and skills for the programme it is the task of the assessments in each module to measure the attainment of each LO. This is done by identifying which assessment tests the attainment of each LO which is verified by the external examiner(s) for each module assessment.

Table 1: Mapping of Modules Learning Outcomes to MQF Learning Outcome Domains

		Learning Outcomes							
Module Code	**Module**	**MQF1**	**MQF2**	**MQF3**	**MQF4**	**MQF5**	**MQF6**	**MQF7**	**MQF8**
CE00869-4	Algorithms & Data Structures in C	✓	✓				✓		
CE00842-4	Hardware & Software Systems & Graphics	✓	✓			✓	✓		
CE00398-4	Introduction to Forensic Tools & Techniques	✓	✓						
CE00126-4	Introduction to Networking with LANs & WANs	✓		✓			✓		
CE00398-4	Introduction to Security Technologies	✓	✓				✓		
CE00371-4	Introduction to Software Development	✓					✓		
CE61014-4	Maths & Statistics for Computing		✓				✓		
CE00853-4	Systems and Database Analysis	✓	✓				✓		
CE00373-5	Computer Systems Low Level Techniques	✓					✓		
CE01099-5	Ethical Hacking	✓	✓		✓		✓		
CE00804-5	Hardware & Software Systems & Networks	✓	✓					✓	✓
CE00881-5	LAN Switching and WAN Networks	✓	✓					✓	
CE00399-5	Biometrics 1	✓	✓				✓		
CE00917-5	Router Security Technologies	✓	✓				✓		
CE00315-5	Professional & Enterprise Development	✓	✓		✓		✓	✓	✓
CE00352-5	System Programming and Computer Control	✓	✓				✓		
COCS60717	Advanced Cyber Security	✓			✓	✓			
CE00336-6	Image Processing	✓	✓				✓		
CE55015-6	Concepts in Information Systems Security	✓	✓		✓		✓		
CE04046-6	Malicious Software and Security Programming	✓	✓		✓		✓		
CE53004-6	Group Case Study	✓	✓	✓	✓	✓	✓	✓	✓
CE00837-6	Project: Artefact Realisation, Testing & Evaluation	✓	✓	✓	✓	✓	✓	✓	✓
CE00835-6	Project: Planning, Management, Communication & Appraisal	✓	✓	✓	✓	✓	✓	✓	✓
CE00836-6	Project: Research, Analysis & Artefact Design	✓	✓	✓	✓	✓	✓	✓	✓

6. Employability

The BSc (Hons) in Cyber Security aims to produce graduates who are reflective and critical learners, with a global perspective, and who are prepared for the world of work. This is achieved through a number of measures:

- Across all levels of the degrees and across all Cyber Security modules, we aim to provide our graduates with ***discipline expertise***. We instill a critical knowledge of the discipline that is underpinned by the experience, research and scholarship of the academic staff and which strives to reflect the key security issues that affect the world in which we live.
- As part of our commitment to ensuring that Cyber Security graduates demonstrate ***professionalism***, we aim to produce graduates who are equipped to enter the world of work and are ***enterprising*** or ***entrepreneurial*** by nature. We use tutorial modules, practical work, field work, dissertations (or work-place projects) and professional practice, to develop and refine the transferable skills (and the confidence and proficiencies that such skills endow) that create graduates with the abilities that employers seek. In addition, Professional and Enterprise Development module in Level 4 introduces employability skills and professionalism that relate directly to working environment.
- In order to capitalize on the knowledge and understanding that the degree aims to develop, ***effective communication*** and an ability to work in teams and with diverse stakeholders, are seen as essential attributes of our graduates. The development of communication, ***presentation*** and ***team working*** skills lie at the heart of the Cyber Security degree and are nurtured from first principles to a high level of proficiency in many of the thematic modules and, especially, through tutorial programmes, field work and the work placement or professional practice modules.
- Employers also value ***independence of thought*** and a ***creative*** ability to find solutions. The degree in Cyber Security enables students to take ownership of their learning – whether individually or in groups – and encourages independence of thought and ***problem-solving*** across a spectrum of activities: in the conduct of a research dissertation or a work-place project; in student-led investigative field projects; in critical reading and writing in thematic modules; or in tutorial discussions and presentations.

These are essential attributes of the ***critical***, ***reflective*** and ***life-long learners*** that Staffordshire graduates are expected to become. Throughout the three years of the degree, students are encouraged to develop their understanding through critical reflection; to question different views and perspectives and to use both their generic and specialist skills (including risk assessment, together with security policy and strategies) to recognize and resolve problems.

Increasingly those problems are set in a global context and globalisation and ***global citizenship*** are central to the way that security specialists look at the world. The majority of the thematic modules that structure these awards explore understandings of how global systems work; how those systems impact upon individuals; and how cyber security graduates can work professionally to manage global security issues.

Graduates will find employment across a wide range of careers destinations including government agencies, local authorities, banking industries, anti-virus companies, consultancies, specialist sectors of the cyber security industry such as virus analysis, anti-malware analysis, risk analysis, security IT auditing, malicious program detection development, vulnerability research, network security engineering and penetration testing or will enter the industrial or commercial sectors. Others will undertake further postgraduate training across a range of academic and vocational courses.

7. Teaching, Learning and Assessment

7.1 Teaching and Learning

Different people learn in different ways and therefore the programme utilises a range of different teaching methods and situations – lectures, problem-based tutorials, practical laboratory sessions, group-based activities, project work, virtual learning environments, seminars, workshops (skills-based) etc. – that best deliver the specific learning outcomes of the modules. In all classes emphasis is placed on active, experiential learning usually based around a case study, or specific crime/event based scenarios. Students will be actively challenged during tutorials to explain or defend a particular viewpoint/finding/analysis, as the students may in the future be expected to defend their expert witness testimony within a legal environment. The use of industry standard packages, such as Encase and Forensic Tool Kit (FTK), .XRY and Biometric hardware and software will be used with real life case studies to provide good exposure to students. With a dedicated and self-contained laboratory, with its own private internal network and contains some of the latest equipment and software, students will be able to practice and develop their practical and troubleshooting skills as required.

Learning approaches are chosen to be compatible to the method of delivery and can include: case studies, investigations, seminars, resource based learning and independent reading. A wide range of teaching, learning and assessment approaches are used and are seen as beneficial in exposing the student to diverse approaches.

The emphasis is on developing students as confident, independent learners. Students are encouraged to access a variety of materials, journals, text books, e-journals etc., as part of their independent learning. This independent learning is directed, with lecturers providing general reading lists to prepare for or follow-up classes, specific assignment reading as well as a range of formative tasks and activities. All this directed study supports and builds upon the knowledge and skills learnt in class to provide a fuller understanding of the subject.

7.2 Assessment

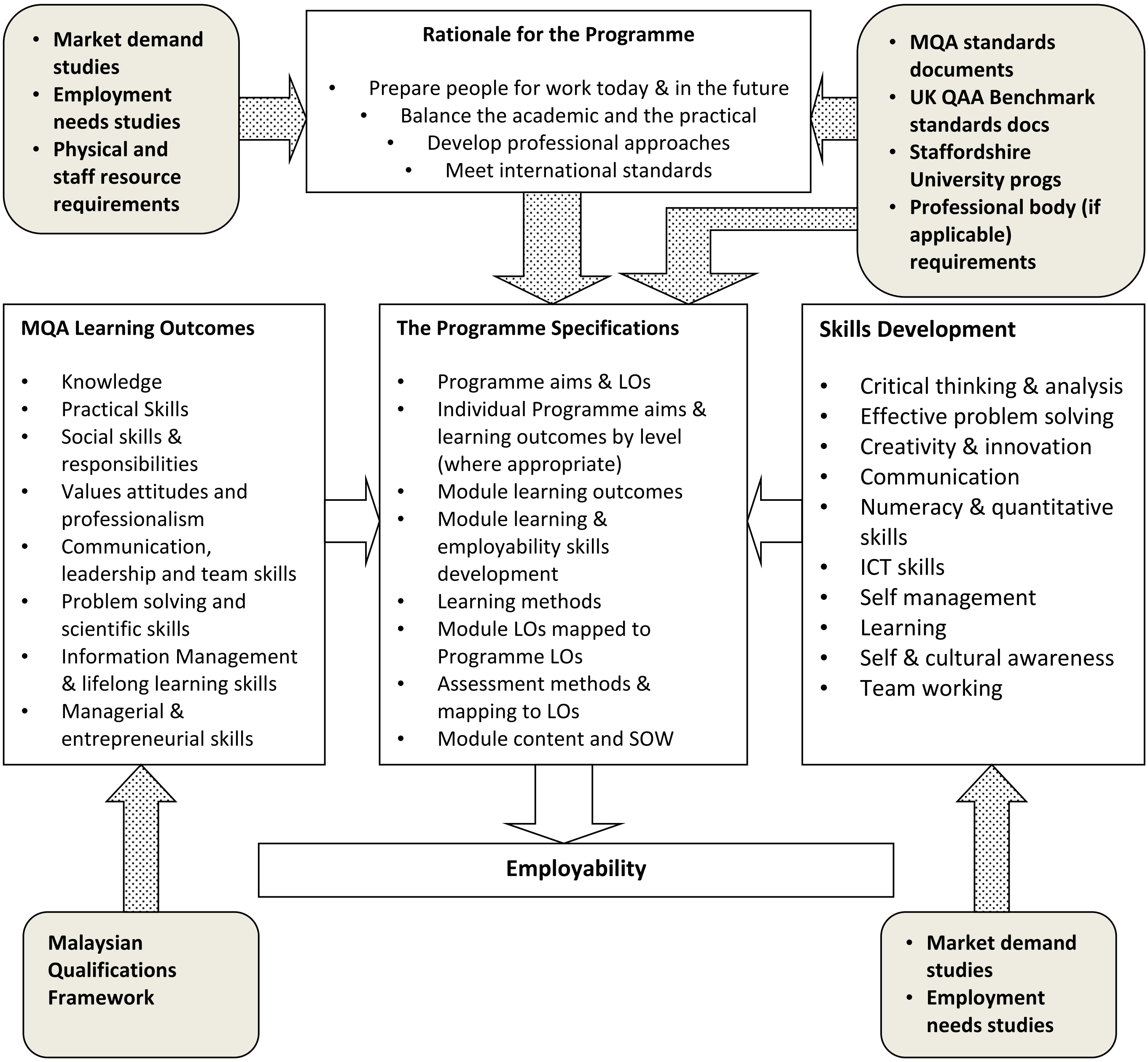
The Cyber Security award employs an innovative range of formative and summative assessments. Typically formative assessment is used as an aide to check students' understanding of a specific subject or topic. The method of assessment is chosen to meet the academic content and outcomes the module is to assess. These will include individual coursework assignments, group-work assignments, presentations, demonstrations, written reports, end-of-module examinations, and oral viva.

This is to: ensure that learning outcomes are tested in the most appropriate way; reflect the sorts of materials graduates will be asked to prepare in future careers; and recognise that students have different abilities. Although the practical and skills based are the nature of the Cyber Security award, coursework, formal examinations and class-tests are also used to assess knowledge-based modules across all three levels.

8. The Process for Development of the Curriculum

The process of development is based on a clear rationale which applies to all programmes and is designed to ensure that all Programmes comply with the APIIT VMG, especially in relation to international standards and the development of employable graduates.

The process begins with consideration of market demand and employment needs. The degrees available from Staffordshire University (SU) for franchise have been studied against these demands and the physical and staffing resources required to deliver them. The SU programmes have been mapped against the QAA subject benchmark statements by SU and subsequently against the MQA standards by APIIT. The following diagram illustrates the process adopted to develop new programmes.



Market demand studies
Employment needs studies
Physical and staff resource requirements
Rationale for the Programme
Prepare people for work today & in the future
Balance the academic and the practical
Develop professional approaches
Meet international standards
MQA standards documents
UK QAA Benchmark standards docs
Staffordshire University progs
Professional body (if applicable) requirements
MQA Learning Outcomes
Knowledge
Practical Skills
Social skills & responsibilities
Values attitudes and professionalism
Communication, leadership and team skills
Problem solving and scientific skills
Information Management & lifelong learning skills
Managerial & entrepreneurial skills
The Programme Specifications
Programme aims & LOs
Individual Programme aims & learning outcomes by level (where appropriate)
Module learning outcomes
Module learning & employability skills development
Learning methods
Module LOs mapped to Programme LOs
Assessment methods & mapping to LOs
Module content and SOW
Skills Development
Critical thinking & analysis
Effective problem solving
Creativity & innovation
Communication
Numeracy & quantitative skills
ICT skills
Self management
Learning
Self & cultural awareness
Team working
Employability
Malaysian Qualifications Framework
Market demand studies
Employment needs studies

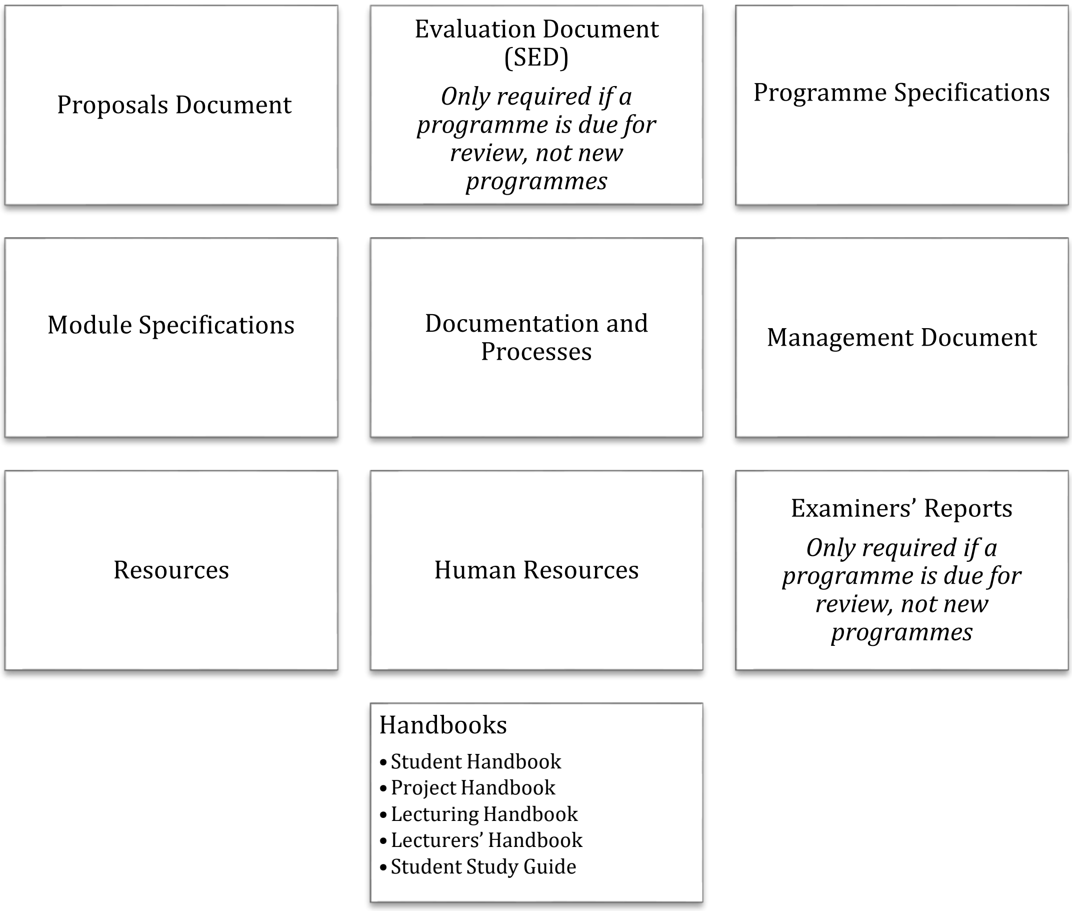
Once the programme has been developed and the Programme specifications, as described above, have been completed then the following are submitted to the Quality Partner Staffordshire University (SU) for their consideration through the conduct of a Validation. Validation is the process adopted by most UK universities to ensure that a proposed programme is appropriate for the academic level and discipline and can be delivered to an appropriate standard. It involves consideration of the Programme by an academic panel comprising SU senior staff and academic staff from the discipline under consideration as well as external panel members who are from the same discipline in other Universities. The conduct of Quality Assurance including validations at all British Universities is subject to periodic audit by the UK Quality Assurance Agency QAA).

The Validation Panel meet with representatives from APIIT to consider the proposals following which a report identifying any further requirements is produced. A second stage then takes place at the APIIT campus and the Validation Panel meet staff and students as well as inspecting resources and considers the APIIT response to the first stage Panel report.

Following the visit a report is submitted by the Validation Panel identifying commendations, conditions and requirements. Conditions must be satisfied before the programme can be delivered, requirements must be satisfied by the date specified by the Validation Panel.

Once the feedback from the Validation has been received any necessary improvements are made to the proposals before they are submitted to MQA.

The documentation submitted for validation is as follows:



Proposals Document

Evaluation Document (SED)

Only required if a programme is due for review, not new programmes

Programme Specifications

Module Specifications

Documentation and Processes

Management Document

Resources

Human Resources

Examiners' Reports

Only required if a programme is due for review, not new programmes

Handbooks

- Student Handbook
- Project Handbook
- Lecturing Handbook
- Lecturers' Handbook
- Student Study Guide

9. Curriculum Content and Structure

The overall structure of the degrees to be franchised is determined by the SU Programme Specifications, as is the credit requirement to achieve a degree and the regulations governing the delivery and award of the degree. However to enable accreditation by the Malaysian Qualifications Agency (MQA) the degrees also comply with the Malaysian Qualifications Framework (MQF). This requires that students complete a minimum of 120 credits for the award of a degree over a minimum of 3 years. Each credit requires 40 learning hours, giving a total learning time of 4,800 hours. All students must study compulsory General Studies modules which are shown in the following curriculum structure.

Thus the delivery of degrees in APIIT will be within the following structure to meet the above. Each module is 4 credits, or 160 learning hours.

The levels of the programme map the UK Qualifications Framework because the students will be awarded a UK degree on completion. In this Framework Level 4 is equivalent to the standard expected of the first year of a normal full time degree programme, level 5 is equivalent to the second year and level 6 is the final, normally, third year. In Malaysia the degree corresponds to MQF Level 6.

Each full semester is 16 weeks of contact and independent learning time followed by 2 weeks assessment, and thus the overall learning time is 108 weeks. The average learning time per week of time in the University is therefore 46 hours.

The Programme Standard for Curriculum Design and Delivery (MQA 2011) states that best practice is for teaching learning weeks per year of 36 to 40, here is proposed 36. The MOHE requires no more than 20 credits per semesters, the maximum here is 19. The proposal here is for from 16 to 19 depending on the semester as shown in the structure overleaf.

Summary of MQA Programme Computing standards requirements

120 credits, 9-30 credits of compulsory general modules, 22 to 35 credits of core modules, 20 to 66 of specialisation modules, 11 to 29 credits of electives and 6 to 12 credits of industrial training.

Semester structure						Total credits
Year 1: Level 4 Semester 1	Introduction to Software Development CE00371-4 **4 Credits**	Hardware & Software Systems & Graphics CE00842-4 **4 Credits**	Maths & Statistic for Computing CE61014-4 **4 Credits**	Introduction to Security Technologies CE00398-4 **4 Credits**	MQA U 2 Professional Development Skills CE5201 **3 Credits**	19
Semester 2	Systems and Database Analysis CE00853-4 **4 Credits**	Algorithms & Data Structures in C CE00869-4 **4 Credits**	Introduction to Networking with LANs & WANs CE00126-4 **4 Credits**	Introduction to Forensic Tools & Techniques CE00398-4 **4 Credits**	MQA U 1A Ethnic Relations: Local students Malaysian Studies: Foreign students **3 credits**	19
Year 2: Level 5 Semester 1	Professional & Enterprise Development CE00315-5 **4 Credits**	LAN Switching & WAN Networks CE00881-5 **4 Credits**	System Programming and Computer Control CE00352-5 **4 Credits**	Hardware & Software Systems & Networks CE00804-5-HSSN **4 Credits**	MQA U 1B Islamic & Asian Civilisation: Local students BM: Foreign students **3 credits**	19
MQA U4 Co Curriculum module (2 Credits)						2
Semester 2	Computer Systems Low Level Techniques CE00373-5 **4 Credits**	Biometrics 1 CE00399-5 **4 Credits**	Router Security Technologies CE00917-5 **4 Credits**	Ethical Hacking CE01099-5-EHAC **4 Credits**	MQA U 3 Malaysian Development **3 MQA credits**	19
	Internship (10 credits) A required period of attachment of 10 weeks OR Industrial Training Portfolio 10 credits					10
Year 3: Level 6 Semester 1	Project: Planning, Management, Communication & Appraisal CE00835-6 **4 Credits**	Computer Systems Security CE00360-6 **4 Credits**	Group Case Study CE53004-6 **4 Credits**	Advanced Cyber Security COCS60717 **4 Credits**		16
Semester 2	Project: Research, Analysis & Artefact Design CE00836-6 **4 Credits**	Project: Artefact Realisation, Testing & Evaluation CE00837-6 **4 Credits**	Malicious Software and Security Programming CE04046-6 **4 Credits**	Image Processing CE00336-6 **4 Credits**		16
					TOTAL Credit	120
					Total Learning	4,960 hrs

27/2/13

Components	**Programme Standard Proposed Credits**	**SU/APIIT credits in the above curriculum map**
Compulsory Modules:	9 – 30	16
Common Core Modules:	18 - 29	28
Discipline core modules:	17 – 55	52
Elective Modules:	9 - 24	16
Industry Training: 10 Credits	6 - 12	10

10. Assessment

10.1 Module Assessment

You will be assessed in every module for which you enrol. You may be required to undertake more than one element of assessment for a module, and you will be given information on what is expected of you at the start of the module. The assessment will be linked to the teaching and learning methods of the module and will be designed to test your achievement of the module's learning outcomes. A range of assessment methods may be used including formal examinations, class tests, essays, projects and case studies. All assessment must be treated with equal gravity and you must attempt all elements.

10.1.1 Module Results

You will be given a result for your performance in each module. Your result will be determined by considering your performance in relation to the relevant assessment criteria. The assessment criteria will be closely linked to the learning outcomes of the module and will be included within the handbook for each module.

Where there are two or more elements of assessment within a module, the overall result for the module will be determined according to the weighting of each assessment. However, you will be required to achieve a specified minimum mark in each element of assessment in order to achieve an overall pass in the module. If you fail to achieve the specified minimum in an element of assessment you will be required to undertake further assessment.

The University uses a Grade Point scale to record your overall module results, as detailed below:

Overall Grade Points for modules and percentage equivalents	Associated honours classification
13-15 (70-100%)	First class
10-12 (60-69%)	Second class (upper division)
7-9 (50-59%)	Second class (lower division)
4-6 (40-49%)	Third Class
3 (30-39%)	Fail grade which may be compensated
2 (20-29%)	Fail grade which cannot be compensated and, in modules with multiple assessments, the minimum grade that has to be achieved for each assessment.
0-1 (0-19%)	Fail grades which cannot be compensated and in modules with multiple assessment, any assessment with a 0 or 1 grade would have to be reattempted to pass the module overall
N	**Fail due to non-submission which cannot be compensated. No further attempt allowed**

Some awards within the modular frameworks may have more rigorous requirements in relation to compensation due to Professional Body accreditation Information on this will be provided in the award handbook for such awards.

For some awards, modules will be graded Pass or Fail only. Where this is the case, details will be provided in your award handbook.

If you are judged to have satisfied the module assessment criteria at threshold level, you will be awarded at least a Grade Point 4 (pass) for the module. You will not be permitted a further attempt at any element of assessment for which you have been awarded a pass grade in order to improve your grade, unless a claim for extenuating circumstances is upheld.

10.1.2 Compensation

Compensation is the awarding of credits for a failed module if you have demonstrated elsewhere in your modules your ability to satisfy the learning outcomes of your award level.
In certain circumstances, the Assessment Board may recommend to the Award Board that you should not be required to undertake further assessment of a failed element of assessment, but that the failure should be compensated.

The Award Board has discretion to award the credits for a module in which a compensatable fail (ie GP 3 has been reported. The result will be recorded as 4C, but the original grade point will be used in calculating classification.

An overall grade point of 0, 1 or 2 or N (a non-submission) for an undergraduate module may not be compensated.

It should be noted that some awards within the University are accredited by a professional body. These professional bodies may have regulations which supersede those of the University in terms of compensation. The Award Board will take account of any such regulations in considering whether to compensate a failed module.

A maximum of 30 credits may be awarded a compensated pass at each of Award Levels 4, 5 and 6. Partial compensation of a module (ie awarding some, but not all, of the credits associated with a module) is not allowed. Where more than 30 credits have been failed, no compensation may be applied.

In operating this compensation, you must have passed a minimum of 90 Level 6 credits.

The Award Board has the discretion to determine whether or not to award a Compensated Pass using the criteria outlined in this section. No more than 30 credits at any one award Level can be awarded a Compensated Pass. The Level 6 Award Board may award a Compensated Pass to module failures remaining at lower levels, provided that the total number of credits compensated in the award overall does not exceed 90 and the original Grade Point was 3 or above.

10.1.3 Module Failure

If you have failed to satisfy the assessment criteria of the module, you will be awarded a **fail grade** (Grade Points 3, 2, 1 or 0. If you have failed to submit any assessment for the module, you will be given a **Grade Point N** (Fail due to non-submission) for the element(s) of that module and you will only be allowed a further attempt at that element(s) of the module at the discretion of the appropriate Board.

The credits for all modules, including failed modules, must be obtained in order for you to qualify for your chosen award and this can be done in one of the ways described below, which will be decided by the Award Board, acting on recommendations from the Assessment Boards.

10.1.4 Referral, Replacement and Retake

If the Assessment Board has reported a Non-Compensatable Fail, or if the Award Board decides not to award you credits by compensation then you will be required to undergo further assessment on the subject matter covered by the module. This is in order to satisfy the Boards that you are capable of meeting the appropriate learning outcomes and is known as “referral”. The form of assessment will be determined by the Award Board, on the recommendation of the Assessment Board, as will the deadline for submission/period of the examination.

The Award Board may decide that along with a form of assessment you need to attend the classes for the module again. This may be because the module is laboratory based, or requires specialist equipment or because your performance indicates that you would benefit from attendance. In such cases, where your timetable does not prevent you from attending, attendance is compulsory. If you are not required to attend, you will normally be required to attempt the re-assessment before the beginning of the next academic year. You must make yourself available to undertake such assessment as the Award Board requires at this time. If you do not meet the referral requirements determined by the Award Board at the time prescribed by the Award Board you will be deemed to have failed the module at that attempt.

The maximum mark awarded for a successfully completed referred element of assessment is a Grade Point 4. If your module comprises more than one element of assessment and the Award Board refers you in one or more elements, the referred element(s) will be recorded at a maximum of Grade Point 4; those elements not subject to referral will retain their original mark. The overall module grade will be suffixed R.

If you have failed an Option module, you may choose not to undertake the further assessment required by the Award Board, but to replace the failed module with another of the same or greater credits.

If you made an attempt at your assessments at the first attempt:
You will only be guaranteed an opportunity to attempt a referral(s) once IF, and only if, you have made an attempt at the assessment(s) on the first occasion unless a claim for Extenuating Circumstances has been successful. If you fail to achieve a satisfactory performance in your referral attempt and are not awarded a compensated pass then the module result will be deemed a Fail. You may, however, at the discretion of the Examination Board, be able to retake the module (ie have a third attempt), except in circumstances where a GP N has been recorded for both the original attempt and the referral. In such cases, you will not be allowed to retake the module. Retaking a module means that you will have to undertake any failed elements of assessment attached to the module. The maximum mark for a retaken module is Grade Point 4. The suffix K will be used to indicate that it is a retaken module. Retaken modules carry no reassessment entitlement. A module may be retaken on one occasion only. Award Boards will not normally grant retakes for more than 30 credits (or one module greater than 30 credits) in a level.

If you did not make an attempt at your assessments at the first attempt:

If you do not submit work or attend assessments at the first attempt, that guarantee of a referral is lost and the appropriate Board will decide whether or not to allow you a referral. In making its decision, the Board may take account of your engagement with that module.

If the Board does allow you a referral(s) and you do not take the referral(s) at the time notified to you by your Faculty/School, no further referral opportunity will be given to you and you may fail the award.

Option modules which have been awarded a Fail (i.e. where no reassessment entitlement remains) may be replaced or retaken as previously described where this is possible. However, if you have exhausted all referral/retake opportunities for all modules in a specific option group, then you will not be able to meet the requirements of your chosen award and will not be permitted to continue on that award.

Core modules cannot be replaced. If you are awarded a Fail for a Core module then you will not be able to meet the requirements of your chosen award and will not be permitted to continue on that award. You will not be allowed to reapply to study the same award in the future as you will already have failed the core modules. If you pass the core modules but fail the overall award, these modules may be used towards a different award for which they are core or option modules.

In all cases, if you are allowed a referral(s), the referral(s) must be taken at the next referral opportunity, as determined by the Award Board. It is your responsibility to make sure that you know when you are required to resit.

10.2 Extenuating Circumstances

If you feel that any unforeseen and unavoidable circumstances (e.g. illness) have affected your ability to gain or demonstrate your knowledge or capabilities in one or more modules you should submit an Extenuating Circumstances form giving full details of the circumstances and supporting evidence for your claim.

If, having submitted a claim for extenuating circumstances, your claim is upheld, the Assessment Board will note where Extenuating Circumstances have been upheld and, where appropriate, recommend to the Award Board a date for (re)submission of the assessment.

If you are given a pass mark for the assessment component(s) for which extenuating circumstances have been upheld, you will be given the opportunity either to accept the grade achieved or submit for further assessment in that module (or components of that module) which you had claimed had been affected by extenuating circumstances.

If you decide to submit for further assessment in the module (or components of that module) which were upheld to have been affected by extenuating circumstances, and you obtain a higher grade than the original grade, the higher grade will be recorded. If you obtain a lower grade than the original grade, the original grade will be recorded.

If you have had your claim for extenuating circumstances upheld against a number of modules (or components of modules) you must decide which modules (or components on modules), if any, you wish to submit for further assessment.

You must make that decision by informing your home Faculty/School, within ten working days of the decision of the relevant examination board being notified to you, in writing, which module(s) (or components of module(s)) you have decided to submit for further assessment. A proforma for such purposes is available from your Faculty/School Office.

If you do not return the proforma within the ten working days specified, your home Faculty/School will assume that you do not wish to submit for further assessment. It is therefore your responsibility to abide by this deadline.

10.3 The Conferment of Awards

10.3.1 Eligibility for your Award

Once you reach the end of your award the Award Board for your award will consider whether you have met all the learning outcomes and the credit requirements for successful completion of the award (see also sections on module enrolment and student workload). If you have met the requirements the Award Board will grant you that award.

If you have enrolled for an Honours Degree programme and met the requirements for completion of your award then the Award Board will consider awarding your degree with Honours. Honours are classified as follows:

- First Class Honours
- Second Class Honours (Upper Division)
- Second Class Honours (Lower Division)
- Third Class Honours

If you have not met the conditions for Honours you may be referred in some of your modules. At this point the Award Board may decide to set a ceiling on the maximum Honours classification available to you, once you have completed successfully those referrals and any retakes or replacements. The maximum degree classification you receive will not be lower than the base class as calculated once referrals have been completed successfully. The Award Board may also wish to consider you for the award of an Ordinary Degree.

If you have no referral, retake or replacement module opportunities remaining, the Award Board will consider your eligibility for the award of an Ordinary Degree.

10.3.2 The Determination of Honours Classification

Stage 1 - Your Overall Score

In determining your degree classification the Award Board will consider your performance in all modules at both Levels 5 and 6 (excluding any Additional modules) studied at any stage of your award. Please note that this refers to the level of the modules and not the year/level of the award you are studying.

Having checked that you have passed all the modules and satisfied all the requirements of your award the Award Board will consider your overall score in Level 5 and 6 modules.

This overall score will be determined by taking into account all your Level 5 module results and giving them a 30% weighting, and all your Level 6 module results and giving them a 70% weighting. The size of multiple modules will also be taken into account by counting the grade point achieved in a 15 credit module once, in a 30 credit module twice, in a 45 credit module three times and so on.

Where compensation is awarded by a Level 6 Award Board (to either Level 5 or Level 6 modules) the original Grade Point achieved will contribute to the overall score.

In summary then:

Overall Score = 30% of average grade points per 15 credits at Level 5 + 70% of average grade points per 15 credits at Level 6.

For students who have been admitted to the University at Award Level 6 (and have not studied any credits at Level 5 at this University) the overall score will normally be 100% of the average grade point per 15 credits at Level 6. Any available academic history may, at the discretion of the Award Board, be considered where appropriate.

If you have been awarded credit through the Accreditation of Prior (Experiential) Learning (AP(E)L) scheme, these modules will be recorded on your profile as Grade Point 4E and this grade will not be taken into account when calculating your average grade point for classification purposes.

Your overall score will determine your "base" classification as follows:

Overall Score	**Base Classification**
13.0 or higher	First Class Honours
10.0 to 12.99	Upper Second Class Honours
7.0 to 9.9	Lower Second Class Honours
4.0 to 6.99	Third Class Honours
3.99 or below	See regulations on Ordinary Degrees

If you have met the requirements for your award you will be awarded at least your "base" classification.

If you have achieved at least 90 Level 6 credits in a class higher than the base, the Award Board will award you one class higher than the base.

Stage 2 - Consideration of your Level 6 Results

Finally the Award Board will consider whether your performance in modules at Level 6 (your profile) suggests that you should be awarded a higher classification than the "base" indicated by your overall score.

If you have:

Achieved at least a Grade Point 4 in all Level 6 modules;

And Achieved at least 60 Level 6 Credits in a class higher than the base

the Award Board has discretion to consider you for the award of one classification higher than base if you have at least 60 credits in a class higher than your base classification.

In operating this discretion the Award Board will also consider:

- The number of Level 6 credits you have studied
- Your Overall Grade Point Average
- Your Grade Point Average in your best 60 Level 6 credits
- Where your overall score lies within the classification band
- Any claims for Extenuating Circumstances that have been upheld

The Award Board will not consider such factors as:

- Your personality and personal relationships
- Any judgment about your potential ability (i.e. not realised in your assessment results)
- Any intentions you may have to progress to post-graduate study or employment requiring a certain Honours classification
- Attendance

If any Level 6 credits have been compensated then you will be awarded your base classification only.

10.4 General Regulations

10.4.1 Attendance

Attendance is required at all teaching sessions for the modules for which you have enrolled. Sessions include all tutor-led activities such as lectures, seminars, tutorials and presentations. “Sessions” should not be interpreted as “weeks”. For small group sessions (sessions which involve a sub-set of the whole module cohort) you must attend the sessions to which you have been assigned.

If you are absent from a module(s) or programme of study on four consecutive occasions in a semester, including lectures, tutorials, seminars and laboratory based classes for reason other than personal illness without written approval you may be deemed to have withdrawn from the module(s) or programme of study and your registration on that module(s) or programme of studies cancelled. You may be excluded from further teaching, denied access to examinations and refused the opportunity to submit assessment for the module or award. You will therefore need to seek permission to start again on the same module (or a replacement where applicable).

All students are also required to maintain an attendance of 80% in each module and will be sent a letter advising of poor attendance after 3 and 6 absences from a module. APIIT will also monitor attendance of foreign students to ensure their attendance meets the minimum requirements of the Malaysian immigration other such authorities.

10.4.2 Breaches of Assessment Regulations - Academic Dishonesty

Cheating and/or plagiarism of any kind will not be tolerated and will be dealt with very seriously. Cheating is defined as any attempt to complete an examination or assessment by unfair means. Plagiarism is defined as submitting the work of others as your own without appropriate referencing and citation for the purposes of satisfying assessment requirements. Plagiarism also includes allowing your work to be copied by another student.

10.4.3 Submission and Late Submission of Coursework

You must submit all pieces of assessment required for each module on or before the submission date for each piece of assessment. Failure to do so may result in failure of the module overall. The submission date will be specified for each piece of assessment for each module. It is your responsibility to make sure you know when your submission dates are and to comply with them.

Failure to meet this deadline will be treated as a non-submission and a Grade Point 0 will be awarded for that component. The only exceptions to these rules apply where a valid claim for extenuating circumstances can be made.

10.4.4 Appeals Against an Examination Board Decision

You may request that any assessment be rescrutinised after the final results are confirmed by the Award Board. You may not appeal against academic judgment but if you believe a material error has been made you may ask for a review of the Examination board decision.

You may also request a review if there is evidence supporting extenuating circumstances which was not available at the time of the Examination Board decision.

10.5 Mapping of Assessments

Module Code	Module	Test	Exam	Portfolio	Essay	Assignment
CE00869-4	Algorithms & Data Structures in C		✓			✓
CE00842-4	Hardware & Software Systems & Graphics	✓				✓
CE00398-4	Introduction to Forensic Tools & Techniques	✓				✓
CE00126-4	Introduction to Networking with LANs & WANs					✓
CE00398-4	Introduction to Security Technologies	✓				✓
CE00371-4	Introduction to Software Development					✓
CE61014-4	Mathematics & Statistics for Computing					✓
CE00853-4	Systems and Database Analysis					✓
CE00373-5	Computer Systems Low Level Techniques	✓		✓		
CE01099-5	Ethical Hacking	✓				✓
CE00804-5	Hardware & Software Systems & Networks		✓			
CE00881-5	LAN Switching and WAN Networks		✓		✓	✓
CE00399-5	Biometrics 1				✓	✓
CE00917-5	Router Security Technologies		✓			
CE00315-5	Professional & Enterprise Development	✓				✓
CE00352-5	System Programming and Computer Control		✓			✓
COCS60717	Advanced Cyber Security					✓
CE00336-6	Image Processing					✓
CE00360-6	Computer Systems Security					✓
CE04046-6	Malicious Software and Security Programming					✓
CE53004-6	Group Case Study				✓	✓
CE00837-6	Project: Artefact Realisation, Testing & Evaluation					✓
CE00835-6	Project: Planning, Management, Communication & Appraisal					✓
CE00836-6	Project: Research, Analysis & Artefact Design					✓

11 Entry Requirements

Entry into the Programmes will be via one of the following routes:

Route 1: Entry to level 4 Degree

- 2 Principal passes at STPM Level and 4 credit passes at SPM,
- 2 Passes at “A” Levels and 4 Grade C Passes at O Levels/GCSE, or
- The APIIT Foundation or equivalent
- A Qualification accepted by SU as equivalent to the above

All students must demonstrate that they have met the equivalent of IELTS 6 either through formal English language assessment or through success in prior study at “A” level or equivalent in English.

Additionally students entering the Journalism degrees will be required to have an IELTS of 7.5 or equivalent

Route 2: Direct Entry to Level 5 Degree

- Successful completion of the relevant APIIT Diploma, or
- Successful completion of study in another recognised institution with academic credits equivalent to level 4 of an honours degree in relevant subjects

12. Module Descriptors

12.1 List of modules

Level 4

CE00869-4	Algorithms & Data Structures in C
CE00842-4	Hardware & Software Systems & Graphics
CE00398-4	Introduction to Forensic Tools & Techniques
CE00126-4	Introduction to Networking with LANs & WANs
CE00398-4	Introduction to Security Technologies
CE00371-4	Introduction to Software Development
CE61014-4	Mathematics & Statistics for Computing
CE00853-4	Systems and Database Analysis

Level 5

CE00373-5	Computer Systems Low Level Techniques
CE00804-5	Hardware & Software Systems & Networks
CE01099-5	Ethical Hacking
CE00399-5	Biometrics 1
CE00881-5	LAN Switching and WAN Networks
CE00315-5	Professional & Enterprise Development
CE00917-5	Router Security Technologies
CE00352-5	System Programming and Computer Control

Level 6

CE00360-6	Computer Systems Security
CE04046-6	Malicious Software and Security Programming
CE00336-6	Image Processing
CE53004-6	Group Case Study
COCS60717	Advanced Cyber Security
CE00837-6	Project: Artefact Realisation, Testing & Evaluation
CE00835-6	Project: Planning, Management, Communication & Appraisal
CE00836-7	Project: Research, Analysis & Artefact Design

12.2 Module Descriptors by Level

Please refer to the module file for this group of programmes.