PROGRAMME SPECIFICATION

1. Key Information

Programme Title:	MSc in Cyber Resilience
Awarding Institution:	Buckinghamshire New University
Teaching Institution(s):	Buckinghamshire New University
Subject Cluster:	Computing
Award Title (including separate Pathway Award Titles where offered):	MSc in Cyber Resilience
Pathways (if applicable)	n/a
FHEQ level of final award:	7
Other award titles available (exit qualifications):	Postgraduate Diploma in Cyber Resilience Postgraduate Certificate in Cyber Resilience
Accreditation details:	n/a
Length of programme:	1 year
Mode(s) of Study:	Full Time (12 months) (Block Mode)
Mode of Delivery:	In person (on-site) delivery
Language of study:	English
QAA Subject Benchmark(s):	Computing (March 2022) Business (March 2023)
Other external reference points (e.g. Apprenticeship Standard):	Chartered Institute of Information Security (CIISec) Skills Framework
Course Code(s):	MSCYBRBF
UCAS Code(s):	n/a
Approval date:	04/07/23
Date of last update:	04/07/23

2. Programme Summary

Cyber resilience is the ability to protect data and recover from cyber threats. It requires a holistic approach that combines physical, procedural, and electronic security systems, as well as strategic planning and risk analysis. Cyber resilience is not only a technical issue, but also a “people problem” that involves human and organisational factors. Because Cybersecurity cannot provide a 100% guarantee of safety, this BNU course aims to reflect the multi-disciplinary nature of cyber resilience, based on the revised ISO27002:2022 standard. It offers a rigorous academic design, comprehensive cyber security training, and professional standards and guidelines. It draws on knowledge and skills from various fields, such as Computer Science, Law, Mathematics, Business Studies, Management Sciences, Criminology, Ethics, and Philosophy.

The course allows learners to choose their modules, the pace, and the mode of learning, to apply their learning in authentic and work-related contexts. The course is relevant to various cultures and regions and incorporates ethical and professional dimensions. It uses effective tools, but does not depend on a single system, to enable cyber resilience. It prepares learners to cope with the evolving challenges and demands of a technologically smart world.

3. Programme Aims and Learning Outcomes

Programme Aims

This programme aims to:

1. **Holistic Understanding:** Equip learners with a comprehensive grasp of cyber resilience beyond technical aspects.

2. **ISO27002 Application:** Familiarize students with the revised ISO27002:2022 standard and its practical use.

3. **Multi-Disciplinary Approach:** Prepare graduates to tackle complex cyber challenges using insights from diverse fields.

4. **Flexible Learning and Application:** Empower students to choose modules, pace, and apply learning authentically.

5. **Adaptability in a Smart World:** Equip graduates to navigate evolving cyber threats effectively.

Programme Learning Outcomes

Knowledge and Understanding (K)

On successful completion of the programme a learner will be able to:

ID	Learning Outcome
K1	Analyse how different cyber-attacks can harm organisations and use risk management to protect them better.
K2	Propose cyber-security solutions that consider all aspects of the problem and reduce cyber threats in different business situations.
K3	Evaluate how computer networks are designed and what weaknesses they have for modern business and user needs and spot network security threats.
K4	Propose cyber-security solutions that use technical and logical methods to reduce network security threats and make different technology users more resilient.
K5	Design effective research studies, employing both quantitative and qualitative research methods and evaluating different epistemological positions.

Analysis and Criticality (C)

On successful completion of the programme a learner will be able to:

ID	Learning Outcome
C1	Apply problem solving skills through both inductive and deductive reasoning processes in the production of cyber-resilience strategies in a smart world.
C2	Evaluate contingency planning as an aspect in developing and delivery resilience programmes within a range of business and user environment.
C3	Demonstrate technical skills in identifying dysfunction within computer networks and be able to respond with quick fixes and develop longer-term (planned) system analysis and resilience.
C4	Analyse individual user problems within a typical IT infrastructure and propose solutions.
C5	Design and produce a research proposal, to create a piece of critical research that has the potential to add to the overall academic discipline.

Application and Practice (P)

On successful completion of the programme a learner will be able to:

ID	Learning Outcome
P1	Identify the needs of a range of stakeholders in developing strategical, tactical and operational programmes to enhance cyber resilience in a smart world.
P2	Analyse the financial, social and legal impact(s) of a range of cyber security business risks and the potential solutions possible to enhance cyber resilience within different business and user environments.
P3	Design technical programmes flexibly to enhance cyber resilience, considering the needs of a range of stakeholders.
P4	Identify the impact of cyber security vulnerabilities and propose network security solutions to enhance cyber resilience in diverse business and user contexts.
P5	Justify ethical issues in relation to scientific research within the field of computing, information security and cyber-resilience.

Transferable skills and other attributes (T)

On successful completion of the programme a learner will be able to:

ID	Learning Outcome

T1	Define their own potential role and responsibilities with an organisation in developing cyber resilience.
T2	Review their own knowledge deficiencies and personal development needs to develop, work and practise cyber resilience initiatives and as part of their own personal development plan (PDP).
T3	Manage an IT Security Infrastructure and their own potential role in ensuring the functionality of computer networks.
T4	Construct computer networks based upon critically reasoned concepts in cyber resilience.
T5	Research quantitative and qualitative methods to evaluate and assess understanding to critically reflect upon learning as part of a personal development plan (PDP).

Graduate Attributes

The BNU Graduate Attributes of: Knowledge and its application (K1); Creativity; Social and ethical awareness and responsibility; and Leadership and self-development focus on the development of innovative leaders in professional and creative capacities, who are equipped to operate in the 21st Century labour market and make a positive impact as global citizens.

Opportunities for learners on successful completion of the programme

The course has been designed to produce ‘hands on’ professionals with a broad range of career possibilities in the fields of Cyber Security and Resilience, working as developers or managers of a development team. Graduates may find employment in software houses, corporate environments (marketing, communications, information technology, training departments), in educational institutions, the banking sector, and companies with an on-line presence or technology need.

Employment possibilities for learners successfully completing the MSc. in Cyber Resilience include Cyber Risk Analyst, Application developer, Technical Advisor, Systems Security Architect, Access Control Administrator, Access Control Developer, Business Continuity Planner, Cyber Forensic Investigator, Penetration Tester, Cyber Resilience Consultant. Successful graduates may also apply for a research degree in a related area.

4. Entry Requirements

The University’s general entry requirements will apply to admission to this programme.

Typical applicant profile and any programme-specific entry requirements

The course is open to graduates holding a suitable honours degree awarded by a British University, a former British polytechnic, the Council for National Academic Awards (CNAA) or an equivalent qualification. It is not intended that this qualification will necessarily be in computer science or an IT related discipline, or a subject area with a substantial computing component. Graduates with appropriate industrial background will also be acceptable.

Candidates are required to show competence in both written and spoken English to the University standard. International learners will be required to have obtained one of the following (other equivalent English language qualifications may be accepted):

- GCSE or GCE O Level in English Language at grade C/4 or above.
- British Council/Cambridge International English Testing Service (IELTS) minimum score of 6.5 in each component.
- American Test of English as a Foreign Language (TOEFL) score of 600 with a test of Written English (TWE) score of 600. The minimum overall score for the computer based TOEFL test is 250.
- Cambridge Proficiency Test in English Language at grade C or above.

If an applicant does not meet the entry requirements they may, if they have relevant professional experience, still be invited for interview, where they will be required to demonstrate the necessary knowledge and understanding for entry onto the course.

Previous study, professional and / or vocational experiences may be recognised as the equivalent learning experience and permit exemption from studying certain modules in accordance with our accreditation of prior learning (APL) process.

5. Programme Structure

Level	Modules (Code, Title and Credits)	Exit Awards
Level 7	**Core modules:** COM7071 Risk, Resilience and Cyber Security (20 Credits) COM7072 Resilient Networks and IT Infrastructures (20 Credits) COM7098 Research Methods and Study Skills (20 Credits) COM7099 Extended Project (40 Credits) **Option modules: (80 Credits)** FOUR other modules from, COM7073 Cryptanalysis & Steganography (20 Credits) COM7074 Web Security & E-Commerce (20 Credits) COM7075 AI, Biometrics and Smart Systems (20 Credits) COM7076 Computer Forensic Investigations (20 Credits) COM7077 Malware Engineering (20 Credits) COM7078 Penetration Testing (20 Credits) COM7079 Cloud Security Solutions (20 Credits) COM7080 Audit, Compliance and Legislation (20 Credits)	MSc in Cyber Resilience [180 CREDITS]
Level 7	**Core modules:** COM7071 Risk, Resilience and Cyber Security (20 Credits) COM7072 Resilient Networks and IT Infrastructures (20 Credits) **Option modules: (80 Credits)** FOUR other modules from: COM7073 Cryptanalysis & Steganography (20 Credits) COM7074 Web Security & E-Commerce (20 Credits) COM7075 AI, Biometrics and Smart Systems (20 Credits) COM7076 Computer Forensic Investigations (20 Credits) COM7077 Malware Engineering (20 Credits) COM7078 Penetration Testing (20 Credits) COM7079 Cloud Security Solutions (20 Credits) COM7080 Audit, Compliance and Legislation (20 Credits)	Postgraduate Diploma in Cyber Resilience [120 CREDITS]

	COM7098 Research Methods and Study Skills (20 Credits)	
Level 7	**Core modules:** COM7071 Risk, Resilience and Cyber Security (20 Credits) **Option modules: (40 Credits)** TWO other modules from: COM7072 Resilient Networks and IT Infrastructures (20 Credits) COM7073 Cryptanalysis & Steganography (20 Credits) COM7074 Web Security & E-Commerce (20 Credits) COM7075 AI, Biometrics and Smart Systems (20 Credits) COM7076 Computer Forensic Investigations (20 Credits) COM7077 Malware Engineering (20 Credits) COM7078 Penetration Testing (20 Credits) COM7079 Cloud Security Solutions (20 Credits) COM7080 Audit, Compliance and Legislation (20 Credits) COM7098 Research Methods and Study Skills (20 Credits)	Postgraduate Certificate in Cyber Resilience [60 CREDITS]

Please note: Not all option modules will necessarily be offered in any one year. Other option modules may also be introduced at a later stage enabling the programme to respond to changes in the subject area.

6. Learning, Teaching and Assessment

Learning and teaching

This post-graduate degree in cyber resilience is designed to suit the needs of both employers and learners. It offers:

- **Flexibility**: Learners can attend 30 hours of face-to-face sessions in week-long blocks over a two-year period (or longer). They can also switch between full-time and part-time modes depending on their circumstances.
- **Support**: Learners can access online surgeries, discussions, and guidance from tutors and peers during the four weeks after each block. They can also use all the University facilities at any time.
- **Quality**: Learners can benefit from the intensive lab-based workshops, the blended learning approach, and the rigorous assessment methods. They can also apply their skills and knowledge to real-world scenarios and challenges.

The degree is aligned with the University's Curriculum 23 (C23) Framework and consists of 10 modules, each lasting five weeks. The first week of each module is an intensive lab-based workshop at the Cyber Security Centre of Excellence Labs on the High Wycombe Campus. The subsequent four weeks are for self-directed learning and online support. Full-time learners can complete the degree in 12 months, while part-time learners have up to 48 months.

Assessment

This document explains the assessment methods and criteria for the MSc in Cyber Resilience. The assessment types are:

- **Diagnostic**: This shows a learner's readiness and challenges for a programme of study.
- **Formative**: This gives feedback to learners on their progress and development but does not count towards the final grade.
- **Summative**: This measures a learner's achievement or failure in relation to the learning outcomes of the programme of study.

Some assessments may have more than one function. For example, some coursework may be both formative and summative, and some exams may be both summative and diagnostic.

The MSc in Cyber Resilience uses various forms of assessment to ensure success and link to the learning outcomes. These include:

- **Written assignments**: These are based on classroom learning and further reading and/or research.
- **Implementations**: These involve applying tools and techniques learnt to solve a real problem.
- **Oral or written in-class work**: These require demonstrating knowledge and defending points of view under time pressure.
- **Practical examinations**: These test learners' ability to apply and discuss concepts from the programme under time limits.

The MSc in Cyber Resilience is delivered in block mode, which means that learners attend 30 days of face-to-face sessions in week-long blocks over a one-year period (or longer). They also have four weeks of self-directed learning and online support after each block. Full-time learners can complete the degree in 12 months, while part-time learners have up to 48 months. They can also switch between modes as needed.

The pass mark for each module is 50%, in line with C23 academic regulations.

An oral examination (viva voce) with a presentation is required for the module COM7099 Extended Project to verify the final mark. Modules with a research-based exam will also have a short test to verify ownership of the work. Learners who fail the test or the viva will be subject to academic misconduct procedures.

Work will be marked according to the general criteria listed in Table 1. Specific subject-centred criteria are given in the individual syllabuses in the module descriptors.

Grade (%)		Indicative meaning
Distinction	90-100	The work submitted is flawless, contains clear elements of innovative thinking and is of publishable quality.
	80-89	The work submitted is complete; the learner shows s/he can work on this subject independently in company/research environment producing high quality of work
	70-79	The work submitted is complete, with major critical additions by the learner who demonstrates competence in all relevant technical matters and clear and undeniable understanding of the theory.
Merit	60-69	The work submitted is complete, with minor critical additions by the learner. Some lacking in breadth of literature review. The work lacks sufficient elements of original thinking.
Pass	50-59	The work submitted is complete, but nothing much above 'textbook' – evaluation includes few points but little critical analysis. There is evidence of quality work but insufficient in quantity to warant a merit mark. All sections are covered just competently. The learner can work in a company in this field.
Fail	31-49	The work submitted is incomplete – the learner has submitted work and listed steps but the arguments around the critical analysis and evaluation are not convincing. The learner may benefit from being reassessed on this component.
	21-30	The learner has understood the question but has made weak effort.
	1-20	The learner has misunderstood the point of what s/he had to do.

0	The learner has not submitted any work or has submitted work in breach of the assessment regulations.

Table 1 – Assessment Criteria

Learners should note that all assessment produces a grade that must be submitted to an examinations board for approval. Grades given by examiners when assessed work is returned represent a formative indicator that learners should consider in conjunction with the feedback to learn if and where the work could have been improved. Grades decided by the assessment board are final grades and can only be changed through the appeals procedure.

Contact Hours

1 unit of credit is the equivalent of 10 notional learning hours. Full time undergraduate learners study 120 credits (1200 hours) and full-time postgraduate learners study 180 credits (1800 hours) per year or 'stage' of the course.

Course Stage	Scheduled Activities (Hours)	Guided Independent Study (Hours)	Placement / Study Abroad / Work Based Learning (Hours)
Full-Time – 1 Year	726	1074	N/A
Part Time – 2 -4 Years	182 to 363 (approx. per year)	269 to 532 (approx. per year)	N/A

7. Programme Regulations

This programme will be subject to the following assessment regulations:

- *Regulations for Taught Degree Programmes (2023)*

8. Support for learners

The following systems are in place to support learners to be successful with their studies:

- The appointment of a personal tutor to support a learner through their programme.
- A programme handbook and induction at the beginning of their studies.
- Library resources, include access to books, journals and databases - many of which are available in electronic format – and support from trained library staff.
- Access to Blackboard, our Virtual Learning Environment (VLE), which is accessible via PC, laptop, tablet or mobile device.
- Access to the MyBNU portal where a learner can access all University systems, information and news, record their attendance at sessions, and access their personalised timetable.
- Academic Registry staff providing general guidance on university regulations, exams, and other aspects of learners and course administration.
- Central learner services, including teams supporting academic skills development, career success, learner finance, accommodation, chaplaincy, disability and counselling.
- Support from the Bucks Learners' Union, including the Learners' Union Advice Centre which offers free and confidential advice on university processes.
- Where a learner may identify with disabilities that require further adjustments these will be handled, and adaptations made in accordance with the reasonable adjustment policy.

The procedures used for assessment cover the subject knowledge, abilities and skills developed through the degree course.

Programme specific support

Whilst studying in a blended learning/block mode, learners are expected to take ownership of their learning, actively guiding it through their selection of modules and complementary studies towards their own educational, academic and career development. While the University records and maintains a document of each learner's academic performance, Personal Development Planning (PDP) is the process of the learners' recording of their own reflection on their learning.

Reflection allows learners to monitor their own performance and to take a conscious approach to what they need to learn, when they need to learn, and what is the best method for themselves to assist their own learning. PDP allows learners to realise their development needs by increasing their self-awareness, reflecting on their personal development and their functioning among colleagues, responding to feedback and being self-critical, and by increasing their confidence and skill of self-promotion.

During the course, learners will be expected to keep a continuously updated record of their performance as is recorded by the University centrally and by module leaders on returned work; in addition, learners are expected to maintain in parallel their own personal development records listing reflective reviews of learning achieved per module taken (including zero-credit activities), aims and objectives that are to be met by – or with the help of – the course, and reviews of progress made towards the set aims. In addition to providing a reminder to learners of their long-term aims and helping to motivate them during their study, the PDP records will also help to produce personal statements (such as CVs) for future employers.

The continuously updated records that should be maintained in each learner's PDP file are listed in Table 2 below:

Record	Produced by	Updated per	Owner
written feedback received on assessed work	Course team	Assessment	School
transcript of marks	University	Semester	University
learning outcomes aimed for	learner	Learning event	learner
statement of progress for each aimed outcome	learner	Learning event	learner
evidence supporting progress statements	learner	Learning event	learner
reflective review of progress made	learner	Learning event	learner
additional support required – if any	learner	Learning event	learner

Table 2 – Contents of Personal Development Planning (PDP) file

Learners are expected to bring their PDP records for discussion with their personal tutor at least once per semester, and to use them when making an argument for the selection of electives and for the suitability of their final project topic. The discussions with staff regarding the development and improvement of a learner's PDP will remain confidential.

9. Programme monitoring and review

BNU has several ways for monitoring and reviewing the quality of learning and teaching on this programme. Learners will be able to comment on the content of their programme via the following feedback mechanisms:

- Formal feedback questionnaires and anonymous module 'check-ins'
- Participation in external surveys
- Programme Committees, via appointed learner representatives
- Informal feedback to your programme leader

Quality and standards on each programme are assured via the following mechanisms:

- An initial event to approve the programme for delivery
- An annual report submitted by the External Examiner following a process of external moderation of work submitted for assessment
- The Annual Monitoring process, which is overseen by the University's Education Committee
- Periodic Subject Review events held every five years
- Other sector compliance and review mechanisms

10. Internal and external reference points

Design and development of this programme has been informed by the following internal and external reference points:

- The Framework for Higher Education Qualifications (FHEQ)
- The BNU Qualifications and Credit Framework
- The BNU Grading Descriptors
- The University Strategy, Impact 2022
- The QAA Subject Benchmark Statement – see below:

Cyber Resilience is multi-disciplined and hence uses multiple QAA Benchmarks.

1. Computing is concerned with the understanding, design and exploitation of computation and computer technologies. It is a discipline that:

   - blends elegant theories (including those derived from a range of other disciplines such as mathematics, engineering, psychology, graphic design, or well-founded experimental insight) with the solution of immediate practical problems
   - underpins the development of both small and large-scale systems that are secure, reliable, usable and support organisational goals
   - helps individuals in their everyday lives and realise their career aspirations
   - is pervasive, ubiquitous and diversely applied to a range of applications, and important components are often invisible to the naked eye.

- Computing provides an intellectually rich, innovative and creative subject discipline in one of the most pervasive aspects of modern life. It requires a disciplined approach to problem-solving, and blends theory from multiple disciplines like mathematics, engineering, and graphical design with the solution of practical problems. **(QAA: March 2022)**

2. Business and management provide a critical understanding of organisations, cultures and structures, their management, and wider economic, environmental and social contexts. It instils an understanding of responsible leadership and develops skills and attributes which equip graduates to become impactful global and inclusive citizens, as well as reflective, independent and collegial lifelong learners. Graduates will be able to demonstrate knowledge, understanding and critical evaluation in many areas such as ethics; responsibility and sustainability; risk management; marketing and sales; finance and accounting; people and organisational behaviour; operations and business innovation; data analytics; information systems; business policy, strategy and intelligence; public and non-profit management; and entrepreneurship and enterprise development. **(QAA: March 2023)**

Mapping of QAA Subject Benchmark Statement to Programme Learning Outcomes

Subject Benchmark Statement	Knowledge and understanding (K)					Analysis and Criticality (C)					Application and Practice (P)					Transferable skills and other attributes (T)				
Benchmark / Standard requirement	**K1**	**K2**	**K3**	**K4**	**K5**	**C1**	**C2**	**C3**	**C4**	**C5**	**P1**	**P2**	**P3**	**P4**	**P5**	**T1**	**T2**	**T3**	**T4**	**T5**
QAA COMPUTING																				
Demonstrate a systematic understanding of knowledge, as appropriate to the area of study, much of which is at, or informed by, the forefront of their academic discipline, field of study or area of professional practice. Alongside this, demonstrate a critical awareness of current problems and/or recent development within the discipline.	X				X	X					X	X	X			X	X	X		
Demonstrate a degree of originality in the application of knowledge, together with a practical understanding of how established investigative techniques of research and enquiry are used to create and interpret knowledge in the discipline.		X		X						X	X		X	X	X	X			X	
Be able to analyse, apply and critically evaluate concepts, principles and practices at the forefront of the area of study.		X					X		X											
Be able to demonstrate judgement, critical thinking, research design, and well-	X		X	X				X	X					X						X

Subject Benchmark Statement	**Knowledge and understanding (K)**					**Analysis and Criticality (C)**					**Application and Practice (P)**					**Transferable skills and other attributes (T)**				
Benchmark / Standard requirement	**K1**	**K2**	**K3**	**K4**	**K5**	**C1**	**C2**	**C3**	**C4**	**C5**	**P1**	**P2**	**P3**	**P4**	**P5**	**T1**	**T2**	**T3**	**T4**	**T5**
developed problem-solving skills with a high degree of autonomy, and to create effective computational artefacts given complex or open constraints.																				
Demonstrate the ability to apply computing techniques, as appropriate to the area of study, within complex or unpredictable scenarios, in a systematic manner, making appropriate decisions given incomplete or missing data					X		X													
Demonstrate elements of self-direction in tackling and solving problems, alongside approaching Demonstrate self-direction in tackling and solving complex problems, alongside approaching Typical Excellent and implementing tasks and activities in a proactive and effective manner.							X	X					X	X		X	X	X		
Ability to communicate their work to specialist and a diverse range of non-specialist audiences. Identify appropriate practices in complex and unpredictable professional environments, and perform work within a professional, legal and ethical framework – including data management and use, security, equality, diversity and inclusion (EDI) and sustainability		X		X							X	X			X				X	

Subject Benchmark Statement	Knowledge and understanding (K)					Analysis and Criticality (C)					Application and Practice (P)					Transferable skills and other attributes (T)				
Benchmark / Standard requirement	**K1**	**K2**	**K3**	**K4**	**K5**	**C1**	**C2**	**C3**	**C4**	**C5**	**P1**	**P2**	**P3**	**P4**	**P5**	**T1**	**T2**	**T3**	**T4**	**T5**
– in the work that they undertake.																				

Subject Benchmark Statement	Knowledge and understanding (K)					Analysis and Criticality (C)					Application and Practice (P)					Transferable skills and other attributes (T)				
Benchmark / Standard requirement	**K1**	**K2**	**K3**	**K4**	**K5**	**C1**	**C2**	**C3**	**C4**	**C5**	**P1**	**P2**	**P3**	**P4**	**P5**	**T1**	**T2**	**T3**	**T4**	**T5**
QAA BUSINESS																				
A systematic and deep understanding of relevant knowledge about organisations, their external context, how they are managed and the detailed relationship between these and their application to practice.	X					X			X										X	
Comprehensive understanding of appropriate techniques sufficient to allow detailed investigation, research or advanced scholarship into relevant business and management issues or specialism within business and management.					X		X									X	X			
An excellent command of subject-specific academic and professional skills relevant to the appropriate field of business					X			X					X					X		X

and management as well as consistent proficiency in generic skills and attributes.																				
A critical awareness of current issues in business and management which is informed by leading edge research and practice in the field as well as by a proactive and independent approach to learning.	X								X		X	X		X						
Conceptual understanding that enables students to evaluate critically current research and advanced scholarship in the field of business and management or a specialism within it.			X			X	X													
Application of relevant knowledge to a range of complex situations, taking account of its relationship and interaction with other areas of the business or organisation.		X						X							X					
Originality and creativity in the application of knowledge, together with a practical understanding of how established techniques of research and enquiry are used to create and interpret knowledge in business and management, or in a specialist field within it.				X	X								X							X

Ability to evaluate and integrate theory and practice in a wide range of situations.		X					X													
An understanding of how the boundaries of knowledge are advanced through research.					X										X					X
A commitment to championing the values of global social responsibility, ethical values and behaving with integrity.			X												X					
An ability to take an international perspective, including understanding the impact of globalisation on businesses, societies and the environment and the ethical implications.		X										X								
An ability to manage and lead with a strong sense of global social responsibility, appreciating the contradictory challenges this presents in complex business and management environments.	X												X	X				X		

Mapping of Programme Learning Outcomes to Core Modules

Programme Learning Outcome	**Knowledge and understanding (K)**					**Analysis and Criticality (C)**					**Application and Practice (P)**					**Transferable skills and other attributes (T)**				
Module Code (Core)	**K1**	**K2**	**K3**	**K4**	**K5**	**C1**	**C2**	**C3**	**C4**	**C5**	**P1**	**P2**	**P3**	**P4**	**P5**	**T1**	**T2**	**T3**	**T4**	**T5**
Level 7																				

Programme Learning Outcome	**Knowledge and understanding (K)**					**Analysis and Criticality (C)**					**Application and Practice (P)**					**Transferable skills and other attributes (T)**				
Module Code (Core)	**K1**	**K2**	**K3**	**K4**	**K5**	**C1**	**C2**	**C3**	**C4**	**C5**	**P1**	**P2**	**P3**	**P4**	**P5**	**T1**	**T2**	**T3**	**T4**	**T5**
COM7071	x	x				x	x				x	x				x	x			
COM7072			x	x				x	x				x	x				x	x	
COM7098					x					x					x					x
COM7099	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x

Mapping of QAA Subject and External Benchmarks to Core and Option Modules

CIISec Skills Framework Standard												
Cognitive abilities: Knowledge and understanding of												
A1 The relationship between an organisation's business needs and their requirements for information security.	X								X	X		X
A2 Requirements for balancing of cost against security risk for the business.	X			X								X

A3 External requirements and standards in terms relevant to an organisation.			X							X		X
A4 The potential strategic application of information security and initiate investigation and development of innovative methods of protecting information assets to the benefit of the organisation and the interface between business and information security.			X	X	X	X		X	X			X
A5 Legal and regulatory requirements that could affect organisation security policies, and the processes and techniques used in verifying compliance against security policies, standards, legal and regulatory requirements.	X									X		X
A6 The different forms of threat to, and vulnerabilities of, information systems and assets and associated risk management needs.	X	X					X					X
A7 Common technical security controls available to prevent, detect and recover from security incidents and to mitigate risk. Including security architectures relating to business needs and commercial product development that can be realised using available tools, products, standards and protocols; and delivering systems assured to have met their security profile using accepted methods		X	X	X	X	X	X	X		X		X

A8 Development and application of standards and strategies for verifying that measures taken mitigate identified risks.	X									X		X
A9 Management requirements for all aspects of a security programme, including reacting to new threats and vulnerabilities, secure operational and service delivery consistent with security polices, standards and procedures, and handling security incidents of all types according to common principles and practices, consistent with legal constraints and obligations.	X					X				X		X
A10 Business Continuity and Resilience requirements	X	X	X	X	X	X	X	X	X	X		X
Intellectual Skills: Able to												
B1 Undertake a gap analysis against relevant external policies, standards and guidelines, and initiate remedial action where appropriate.	X										X	X
B2 Balance technical, physical, personnel and procedural controls to address information risks in the most effective way.	X										X	X
B3 Identify and advise on the technical, physical, personnel and procedural risks associated with third party relationships.		X		X	X	X		X	X			X
B4 Identify assets that require protection, the relevant threats to the assets, exploitable vulnerabilities and assess the level of threat posed by potential threat agents.	X	X		X				X		X	X	X
B5 Interpret relevant security policies and risk profiles into secure architectural solutions that mitigate the risks and conform to legislation.		X	X		X		X		X	X		X
B6 Assess whether a process is “fit for purpose” and meets the security requirements.								X		X	X	X
B7 Manage or investigate an information security incident at all levels.						X						X

B8 Verify that information processes meet the security criteria (requirements or policy, standards and procedures).	X	X								X		X
B9 Define the need for, and implement processes for establishing business continuity.	X											X
Practical skills: able to												
C1 Incorporate physical, personnel and procedural issues into the overall security governance process.	X											X
C2 Ensure security policies support compliance with corporate governance practices.										X		
C3 Produce an information security risk assessment.	X										X	X
C4 Determine the business impact of a risk being realised.	X											X
C5 Develop information risk management strategies to reduce the risk.	X											X
C6 Select the most appropriate tools and techniques for auditing effectiveness of mitigation measures in place.										X		X
C7 Devise standard solutions that address requirements delivering specific security functionality whether for a business solution or for a product.				X	X							X
C8 Select and test the appropriate security products, components and technologies to meet a security requirement.		X		X	X				X			X
C9 Establish and maintain Security Operating Procedures in accordance with security policies, standards and procedures.		X	X							X		X
C10 Coordinate penetration testing on information processes against relevant policies.								X				X

C11 Maintain security records and documentation in accordance with Security Operating Procedures										X		X
C12 Administer logical and physical user access rights.		X		X					X			
C13 Monitor processes and response to a breach of security policy.		X				X						X
C14 Analyse system information (e.g. system logs, network traffic, hard disks, virtual memory, etc.) for evidence of breaches of security policy or law.		X	X									X
C15 Analyse software for malicious intent (malware).			X				X					X
C16 Carry out security compliance audits in accordance with an appropriate methodology.										X	X	X
C17 Implement procedures for responding to and stabilising the situation following an incident or event.	X					X				X		X
Transferable skills: able to												
D1 Encourage an information risk awareness culture within an organisation.	X										X	X
D2 Exploit opportunities for introducing more effective secure business and operational processes.		X	X	X	X		X	X	X	X		X
D3 Manage the development or delivery of information security awareness and training programmes.											X	X

D4 Manage implementation of information security programmes, and co-ordinating security activities across the organisation.	X									X		X
D5 Engage with the Change Management process to ensure that vulnerabilities are mediated.	X	X							X	X		X
D6 Develop, co-ordinate and evaluating plans to communicate with internal stakeholders, external stakeholders and the media.	X			X							X	X