QUALITY ASSURANCE DOCUMENT QA3 – PROGRAMME SPECIFICATION

1. Programme Code	TBC					
2. Programme Title	MSc Cyber Security					
3. Target Award Title	MSc Cyber Security					
4. Exit Award Title(s)	Postgraduate Diploma Cyber Security Postgraduate Certificate Cyber Security					
5. Subject area	Cyber Security					
6. School	School of Computing					
7. Programme Team Leader(s)	TBC					
8. Programme Type	BL and DL					
9. Delivery Model	DL F/T	X	BL F/T	X	Apprenticeship	
	DL P/T	X	BL P/T	X	Other	
Where delivery model identified as 'Other' please provide details						
10. Location of delivery	DL BL – Leeds, Manchester, Birmingham, London Ealing Holborn Tower Hill, Berlin					
11. Proposed Start date	February 2024					
12. Reference points	• QAA Subject Benchmark, Computing available here • The UKPSF for teaching and supporting learning in higher education available here. • Arden Excellence Framework for Inclusive Curriculum here • IET (AHEP4) Accreditation here • NCSC Accreditation here					
13. Professional, Statutory & Regulatory Bodies (PSRB)	***The following accreditations are to be sought:*** • ***NCSC***					

14. Programme aims
The aim of MSc Cyber Security programme is to provide a distinctive, inter-disciplinary and integrated programme aimed primarily at individuals who are either employed in or who are looking to work in Cyber Security roles within the computing sector. The programme is designed to expose programme participants to a range of topics relating to cyber security and IT security management. The modules are designed to develop critical thinking and analytical skills with an emphasis on practical hands-on problem solving and reflection to further develop interpersonal skills and support life-long learning. Topics covered within the modules are aligned to current cyber vendor professional offerings and are supported with access to vendor labs and materials. There will also be opportunities to take professional certifications throughout the programme. The programme is also fully aligned to

the syllabus required to achieve NCSC accreditation and will also allow students to register for professional membership with the IET.

Programme participants will build on their existing understanding of cyber security through evaluating and investigating a range of contemporary management and security issues within a global context. As well as developing their technical expertise, participants will also develop their critical thinking, creativity, interpersonal and multidisciplinary skills ensuring they have the tools to succeed in the modern workplace.

The purpose of the programme is to enable students to demonstrate the following:

- A critical awareness of contemporary cyber issues including legal, ethical and regulatory requirements.
- Critical skills in risk assessment and management from both an offensive and defensive position
- An ability to analyse, interpret and recommend creative solutions to real world problems at a national and global level
- A critical approach to the application of information assurance methodologies and security testing
- Evaluate use of digital technologies, tools and strategies within the cyber security domain
- Highly developed skills around incident management and forensics
- A critical evaluation of the roles of Incident Management and Business Continuity planning
- Ability to work and think both independently, as well as part of a team

15. Programme Entry Requirements

Please adapt standard/typical entry requirements as necessary.

Standard entry requirements:

- A 2.2 Honours degree in a computing related subject, or a 2.2 Honours degree with 18 months relevant computing work experience.

Typical non-standard entry requirements:

- A minimum of 3 years of relevant computing work experience, or equivalent.

Standard English language requirements:

- English Language proficiency equivalent to IELTS 6.5, with no less than 6.0 in each component, if English is not the applicant's first language (or appropriate previous study in English).

16. Learning, teaching and assessment methods and strategies

The programme will use an active learning blended learning approach that combines access to industry-leading resources, technical and academic knowledge, online support and engagement with module lecturers and peers. This will enable learners to rapidly develop new skills and knowledge and apply them to solve problems. A variety of learning spaces will be created that are inclusive, supportive and accessible to all to encourage critical thinking and creativity.

An approach of practical workshops and discussions will be supported by on-line learning materials and activities. On-line learning materials will be used to introduce key topics which then will be further developed in workshops through practical problem-solving activities. This will allow learners to apply the theories, models and frameworks, adding depth and breadth to theoretical concepts to become effective learners. Student will be required to reflect on their own experience within the subject area and recommend personal and professional improvements to support life-learning.

A virtual learning environment will be used to encourage individual and group contributions and discussions on key topics and issues. Materials and discussion groups will be available on the virtual learning portal to support and engage learners in topic specific queries posed by tutors and peer groups ensuring diverse formative feedback and learning opportunities are available to all. Practical workshops supplement the online materials and allow learners the opportunity to practise and acquire new technical and personal skills. Workshops will employ a range of approaches, including case studies, labs, group discussion and other forms of collaborative learning such as role-plays, one-to-one interactions including peer feedback and review, question and answer sessions.

In order to develop the student's capacity and confidence as an effective learner, they will also engage in independent learning. Self-guided labs and online materials will be available to promote deep learning. Embedded within the text are also links to further reading and appropriate websites. Feedback within the learning materials is provided to allow programme participants to check understanding and progress whilst discussion forums will allow peer engagement and opportunities for formative feedback.

Teaching/learning methods adopted are transferrable across all modules and include online class discussions, exercises/case studies and group discussions. Assessments encourage students to critically reflect, embrace new challenges and adapt their approaches to ensure they are constantly learning new skills in preparation for employability and life-long learning

For each subject being taught a programme of structured online learning activities using both formative and summative assessment is available, emphasis being on active learning ensuring activities revolve around high student engagement and lecturer facilitation.

Learning and Teaching activities are:

Asynchronous

- Independent and directed student study, supported throughout by comprehensive online blended learning teaching materials and resources accessed through Virtual Learning Environment
- Guided group / project based work
- Practical, hands-on labs
- Online-self assessment, checkpoints and reflective activities

- Use of key module reading lists
- Assessment preparation
- Arden University learning resources (e.g., Library and Careers Portal)
- Discussion forums to allow students to discuss and critically engage with themes emerging from the online materials they engage with, following the posing of questions or propositions, case studies or similar by either tutor or students themselves

Synchronous

- Online and face to face workshop facilitated by lecturers where theory and practice are integrated
- Access to industry software and labs
- Live chats
- Office Hours
- Assessment preparation and support

These strategies will enable students to engage with a variety of learning tools that best meet their learning styles, overall objectives and personal circumstances. Independent study is the cornerstone of the learner experience, supported by subject specialist engagement with tutor and peer engagement.

Assessment Methods and Strategies

Assessment is carried out according to context and purpose and recognises that learners may exhibit different aptitudes in different forms of assessment. All assessments are portfolio based where learners will submit artifacts of their choice. This will include a report which contains elements of reflection and recommendations for personal and professional improvement. Assessments are based round real-life problems and learners will be encouraged to contextualise around their own experiences.

Opportunities for both summative and formative feedback will be clearly visible within the programme and assessment briefs and in line with Arden policy. Formative Feedback will be provided throughout the modules and is built into asynchronous and synchronous delivery through peer assessment in discussion forums/in sessions, group activities, draft submissions with feedforward feedback and tutorials with lecturers.

17. Intended programme learning outcomes and the means by which they are achieved and demonstrated		
Learning outcomes	**The means by which these outcomes are achieved**	**The means by which these outcomes are assessed**
At the end of this course you, the student, will be able to:		
1. Critically evaluate a range of security process and technologies and effectively manage their deployment in required situations.	Acquisition of knowledge and understanding through an integrated learning and teaching pedagogy that includes both asynchronous and synchronous activity drawing upon a range of academic and professional body source materials; students thus have multiple opportunity to gather knowledge and gain understandings of core concepts. Throughout the programme, the learner is encouraged to develop intellectual skills further by undertaking further independent study and research, i.e., in addition to "directed study" and learning. Discussion of real-world cases and problems to explore ethical and regulatory issues together with strategic challenges.	Coursework consisting of portfolio assessment contains artifacts, justification, and reflections Formative Feedback is an integral part of the programme and provided in all modules. Such opportunities are built into the asynchronous and synchronous module delivery. These may take the form of peer assessment in discussion forums/in sessions, group activities, draft submissions with feedforward feedback and tutorials with lecturers. The virtual learning environment (VLE) enables students to engage in targeted online discussions relating to specific aspects of the programme modules and critiquing established areas of theory and practice. Students are encouraged to not just post discussion items in the relevant forum but also to ensure they comment on posts
2. Evaluate internal and external security threat and work to develop innovative strategic approaches to mitigate them		
3. Undertake self-led research into cyber security issues in the workplace demonstrating an ethical approach to the application of principles.	Independent and directed student study, supported throughout by comprehensive classroom based and online blending learning teaching materials and resources. Discussion in class and online forums where students discuss and critically engage with themes emerging from the materials they learn from; this might include: cyber security issues in relation to business concerns, case studies, financial statements, datasets and industry reports, simulations using	
4. Shows technical expertise, making effective and efficient use of cyber security skills and adapting to new situations		

5. Synthesise and apply innovative methodologies, techniques, tools and technologies from a range of fields within cyber security to provide a complete solution to novel or complex problems.	platforms like Bloomberg, IbisWorld, etc. Synchronous seminars facilitated where theory and practice are integrated. This strategy enables students to engage with a variety of learning tools, case materials, datasets, financial information and analytical software that best meet learning styles, overall objectives and personal circumstances Problem solving and diagnostic skills are developed throughout the programme by formative assessment tasks including problem analyses, analysing case studies, ethical dilemma exercises and self-assessments. Practical skills are further developed and integrated through a series of in-class and online activities intended to build practical skills, these can include: labs, group forums and activities and informal peer assessment	uploaded by their peers. Students will have access to academic and support staff in all the modules studied. These staff include subject matter experts (lecturers), study support tutors, Inclusion Team, EAP tutors, Careers and Library support. Students are invited to attend synchronous learning activities relating to both areas, academic content and study support. They will also have opportunities to arrange one to one meetings, either face-to-face or online, where they can discuss specific areas of concern with the tutor(s)
6. Demonstrate systematic creative approaches to problem solving in the cyber security domain, showing initiative and originality.		
7. Systematically collect and use data from a wide range of sources to synthesise and evaluate effective decision alternatives in relation to design, construction or management of cyber security domains		
8. Demonstrate a reflective approach to work and the capacity to take responsibility for engaging in self-directed life-long learning for personal and professional development.	Engaging in reflection on study activities such as: feedback (peer and tutor), cases, accounting and finance conventions and datasets. Advisory and consulting skills are developed via the demonstration of creative thinking and problem solving, analysis, judgement and self-reflection in the development of contextually relevant solutions to a range of cyber security challenges and situations including the construction of real world projects Group discussions in class and on the online forum promoting debating argumentation, listening and team working skills. Considering employability and career development options, strategies and challenges that draws upon their personal	

	reflections of their study experience on the entire programme, peer and tutor feedback, a skills audit and personal analysis. Use of vendor resources on module and opportunity to take professional certifications.	

18. Graduate Attributes and the means by which they are achieved and demonstrated *Attributes must be covered and assessed in every level of study on a programme.*		
Graduate Attribute	**The means by which these attributes are achieved**	**The means by which these attributes are assessed**
1. Digitally literate	Digital technologies are used throughout the entire programme. Learners will interact with an online VLE environment to access online blended materials and engage with discussion forums and SAQs. Critical technologies for productivity such as Zoom and O365 will be used to participate in online meetings and create artefacts for assessment portfolios. Cyber specific digital technologies and tools will be used in each module for activities, lab exercises and assessments. Extracurricular activities such as vendor labs and certifications will also be available for self-directed study For academic contexts, all Arden University supporting resources such as Library and Careers Portal are also accessed via digital technologies This learning outcome will be specifically achieved in the following	Use of subject specific and general digital tools within Portfolio create for assessment where multiple digital technologies and tools will be used to create a solution to resolve a security problem

	modules: • COM7017 Offensive Security	
2. Contextually innovative	Learners will be exposed to real life cyber issues through online materials, workshop activities and assessments where they will need to critically evaluate security issues, reflect on the different approaches and identify a solution This learning outcome will specifically be achieved in the following modules: • COM7013 Network Security • COM7018 Secure System Design	Discussions, activities, and assessments are based around problem solving scenarios in which learners need critically evaluate and contextualise the subject matter to create a solution. They will also be required to reflect on the project and their personal and professional development
3. Socially intelligent and proactively inclusive	There will be opportunities in all modules for peer collaborations and team engagements allowing learners to experience different views and gain an understanding of equality, diversity, and inclusion. This will be specifically highlighted through workshop activities and discussions forums. Students are also encouraged and required to explore their own personal development route to university and career paths through reflection and use of SMART criteria (Specific, Measurable, Attainable, Relevant and Timebound) This learning outcome will be specifically achieved in the following modules: • COM7012 Information Security Management • COM7014 Advanced Computing Project	Assessment Portfolio's are required to contain reflections consisting of personal and professional continuous development improvements to support potential career pathway of choice. This will demonstrate research within their considered career paths and outline aims and objectives to achieve desired outcome. Collaboration opportunities are available throughout all modules on the programme. COM7xx Information Security Management has part of the assessment as group work
4. Professional knowledgeable in their subject area	Learners will be exposed to real life cyber issues through online materials, workshop activities and assessments. They will need to critically evaluate and contextualise security issues, reflect on the	Discussions, workshop activities and peer collaboration will prepare students for problem solving

	different approaches and identify a solution and justifications supported by a range of evidence from academia and professional body resources. Careers portal and department support students within their career pathways and communicate opportunities that will benefit both personal and professional development. This learning outcome will be specifically achieved in the following modules: • COM7015 Cloud and Web Services Security • COM7016 Digital Forensics and Incident Management	assessments where they will need to critically evaluate and contextualise the subject matter at a local, national and global level.

19. Summary of modules and mapped programme learning outcomes

List modules in order of delivery

Level	Module Code and Module Title	Module type *Compulsory (C) or Optional (O)*	Pinned/paired Modules	LO 1	LO 2	LO 3	LO 4	LO 5	LO 6	LO 7	LO 8			GA1	GA2	GA3	GA4
7	**COM7012 Information Security Management**	**C**	✓		✓	✓		✓		✓	✓					✓	
7	**COM7013 Network Security**	**C**	✓	✓	✓		✓	✓	✓						✓		
7	**COM7018 Secure System Design**	**C**		✓	✓			✓	✓	✓					✓		
7	**COM7017 Offensive Security**	**C**		✓		✓	✓	✓	✓		✓			✓			
7	**COM7015 Cloud and Web Services Security**	**C**		✓	✓		✓		✓	✓	✓						✓
7	**COM7016 Digital Forensics and Incident Management**	**C**				✓	✓			✓	✓						✓
7	**COM7014 Advanced Computing Project**	**C**		✓		✓		✓	✓	✓	✓					✓	
Master's (MA/MSc/MBA) To be awarded the Masters, students must complete a total of 180 credits at Level 7 including 60 credits from the final project.																	
Master's Top-Up Master's top-up programmes must include 60 credits from the final project.																	
PG Cert																	

To be awarded the PG Cert in Cyber Security students must successfully complete 60 credits at Level 7.
PG Diploma To be awarded the PG Dip in Cyber Security students must successfully complete all modules except the Project module to a total minimum of 120 credits at Level 7.