MSc Information Security Management

Programme Specification

1. Programme title	MSc Information Security Management
2. Awarding institution	Middlesex University
3. Teaching institution	Middlesex University Hendon (HE)
4. Details of accreditation by professional/statutory/regulatory body	
5. Final qualification(s) available	MSc Information Security Management PG Information Security Management PG Cert Information Security Management
6. Year effective from	**September 2021**
7. Language of study	English
8. Mode of study	FT/PT

9. Criteria for admission to the programme

The principal criteria for admission are that entrants are capable of working at postgraduate level and are able to succeed at, and benefit from, the programme. The following would normally be considered appropriate entry qualifications:

- An Honours Degree in a discipline related to the programme, such as relevant numerate subjects or those providing a significant exposure to Information Technology, or
- An Honours Degree together with employment or professional experience in a field relevant to the programme and at an appropriate level in the field. Applicants with degrees in other disciplines need to be computer literate.

We normally require graduates with a 2:2 honours degree, or equivalent qualification, in an appropriate subject. We also consider candidates with other relevant qualifications. Those without formal qualifications need to demonstrate a minimum of three years' relevant work experience and the ability to study at postgraduate level.

Individual applicants may wish to claim certain number of credits against their learning that may have taken place outside education or through training that is not assessed as part of an education system. Typically, these applicants would possess knowledge and skills that may have been acquired at the workplace through practice but may not be supported by formal qualifications. Applicants may also hold academic, vocational or professional qualifications that may be aligned to certain modules of the programme at an appropriate level. Typically, such qualifications are supported by evidence in the form of certification. Each of these cases is considered individually with the scope to assess whether applicants should be allowed in the programme with specific credit that would count towards the end qualification, to an appropriate point of the programme. As each case is treated individually, applications with Recognition of Prior Experiential Learning or Recognition of Prior Certificated Learning are eligible to be considered.

- International students whose first language is not English or who have not been taught in the English medium throughout must achieve minimum score of an IELTS of 6.5 or above, with a minimum of 6.0 in all components.

University policies supporting students with disabilities apply, as described in the Guide and Regulations, ‘Information for Students with Disabilities’.

10. Aims of the programme

The programme aims to:

1. Give students a sound theoretical and practical understanding of principles and concepts in information security management across a number of specialist areas (technical, regulatory and financial risk from technology).
2. Equip students with relevant theoretical and practical understanding of tools, techniques, procedures and skills necessary to effectively carry out and manage effective digital forensic investigations especially relating to computer incidents and computer misuse.
3. Give students a broad understanding of regulatory compliance, audit and security, and the detection, investigation and prevention of financial crime in corporate environments from emerging technologies.

4. Equip students with the technical skills necessary to develop and implement strategies for the introduction and management of information systems and knowledge management programmes.
5. Equips students with blockchain strategy knowledge to assess an organisations viability in adopting this technology.
6. Develop critical, analytical and intellectual abilities of students by nurturing creative and independent thinking, and the ability to communicate clearly and coherently.
7. Provides students with knowledge about information security management, cyber and information security in managing data, systems and people.
8. Develops management knowledge to lead wide range of technical teams (including investigators, financial specialists, fintech specialists, security teams).

11. Programme outcomes

A. Knowledge and understanding

On completion of this programme the successful student will have knowledge and understanding of:

On completion of this programme the successful student will have knowledge and understanding of:

1. Tools and techniques necessary for carry out and manage digital forensic investigations.
2. The nature, collection, handling and analysis of digital evidence in a forensic investigation.
3. Regulatory compliance and the detection, investigation, and prevention of financial crime in corporate environments from emerging technologies
4. Be able to manage audit and security processes within an organisation
5. Assisting organisations in developing effective knowledge/data management programmes to maintain competitive advantage in knowledge/data driven economies.
6. Be able to provide advisory services relating to blockchain strategy to organisations.

Teaching/learning methods

Students gain knowledge and understanding and develop cognitive skills and abilities through self-directed, resource-based learning, small group discussions, small group and individual exercises, lab sessions, demonstration software, on-line examples and the research project. Weekly seminar sessions supported by the Local Study Centre Tutor(s) provide the opportunity to address questions, queries and problems.

Throughout their studies students are encouraged to undertake independent study both to supplement and consolidate what is being learnt and to broaden their individual knowledge and understanding of the subject. Critical evaluation and selection of methods, tools and solutions engage the students in relating theory to practice.

Students will have the opportunities to learn from industry experts, who deliver experience, insight, and current thinking to address domain specific learning. These experts come from a diverse range of industries (law enforcement, compliance, audit and risk management, investigations)

7. Manage information security management, cyber security and audit and security in learning scenarios. 8. Legal and professional issues related to computer-related crime, digital evidence and digital forensic investigations. 9. Principles and concepts of relating to new investigation methods for emerging technologies. 10. Be able to manage audit and security processes within an organisation. 11. Digital crime investigation frameworks, guidelines and procedures.	offering students an opportunity to engage and develop their networks. **In the event that teaching cannot be delivered face-to-face, online delivery for lectures, seminars and workshops will be made available using video conferencing tools. Remote access technology will also enable students to access software in specialist labs.** **Assessment methods** Students' knowledge and understanding is assessed by any method below: • Individual coursework • Group coursework • Presentations • PG Individual Project • Investigative Reports • Technical Reports • Business Reports • Solving Case Scenarios • Blogs • Quizzes • Digital Polls • Creation of Visualization Documents (Timelines, Mind Maps)
B. Skills On completion of this programme the successful student will be able to: 1. Apply relevant tools and techniques to carry out a digital forensic investigation. 2. Investigate, collect and analyse and present relevant digital evidence from digital devices including online data stores (open blockchains). 3. Advise on managing compliance in corporate environments and implementing tools and techniques for detecting, investigating and	**Teaching/learning methods** Students develop practical abilities through the teaching and learning programme outlined above. These abilities are also nurtured through small group discussions, small group and individual exercises, laboratory sessions using commercial and open-source software, on-line problem-solving examples and the research project. Students learn transferable skills through the teaching and learning programme outlined above. Although not all the skills are explicitly taught, they are nurtured and

preventing financial crime from emerging technologies. 4. Advise on blockchain strategy for organisations 5. Apply relevant information security management, cyber security and audit and security principles by implementing effective solutions as an individual or in cooperation with others. 6. Select and use a variety of modes of discourse for effective communication according to the needs of the intended audience. 7. Perform effectively as a member of student teams in complex and diverse scenarios. 8. Demonstrate a critical understanding of, and the ability to deploy effectively, a wide range of learning methods resources and technologies, including, but not limited to, Information and Communication Technologies. 9. Manage their own learning and development autonomously, demonstrating time management and organisational skills at a professional level. 10. Demonstrate self-direction and originality in learning and problem-solving in familiar and unfamiliar situations. 11. Appreciate the need for continuing professional development in recognition of the need for lifelong learning. 12. Advise on relevant legal and professional issues related to computer-related crime, digital evidence and digital forensic investigations. 13. Apply and validate new methods of investigation.	developed throughout the programme, which is structured and delivered in such a way as to promote this process. **In the event that teaching cannot be delivered face-to-face, online delivery for lectures, seminars and workshops will be made available using video conferencing tools. Remote access technology will also enable students to access software in specialist labs.** **Assessment methods** Students' knowledge and understanding is assessed by any method below: • Individual coursework • Group coursework • Presentations • PG Individual Project • Investigative Reports • Technical Reports • Business Reports • Solving Case Scenarios • Blogs • Quizzes • Digital Polls • Creation of Visualization Documents (Timelines, Mind Maps)

12. Programme structure (levels, modules, credits and progression requirements)

12.1 Overall structure of the programme

Full time structure for modules (taught 15 credit modules are 12 weeks).

Semester 1 and 2			
CST4340 (30) Data Management for Decision Support			
Semester 1		**Semester 2**	
CST4240 (15) FinCrime Risks from Emerging Technologies	**CST4230 (15)** Digital investigations and Incident Management	**CST4280 (15)** Blockchain Strategy	**CST4290 (15)** Cyber and Information Security
CST4210 (15) Audit and Security		**CST4300 (15)** Information Security Management	
CST4340 (30) Data Management for Decision Support			
Semester 3			
CST4390 (60) PG Individual Project			

Part Time structure for taught modules (taught 15 credit modules are 12 weeks).

Year 1 (60 credits)			
Semester 1		**Semester 2**	
CST4240 (15) FinCrime Risks from Emerging Technologies	**CST4230 (15)** Digital investigations and Incident Management	**CST4280 (15)** Blockchain Strategy	**CST4290 (15)** Cyber and Information Security
Year 2 (Semester 1 and 2) (60 credits)			
CST4340 (30) Data Management for Decision Support			
Year 2 Semester 1		**Year 2 Semester 2**	
CST4210 (15) Audit and Security		**CST4300 (15)** Information Security Management	
Semester 3 (60 credits)			
CST4390 (60) PG Individual Project			

12.2 Levels and modules

Level 7

COMPULSORY	OPTIONAL	PROGRESSION REQUIREMENTS
Students must take all of the following: CST4210 Audit and Security CST4230 Digital investigations & Incident Management CST4240 FinCrime Risks from Emerging Technologies CST4280 Blockchain Strategy CST4290 Cyber and Information Security CST4300 Information Security Management CST4340 Data Management for Decision Support CST4390 PG Individual Project		Students must pass all taught modules and achieve 120 credits before they can progress on to CST4390 – PG Individual Project module.

12.3 Non-compensatable modules

Module level	Module code
7	CST4390

13. Information about assessment regulations

Information on how the University formal assessment regulations work, including details of how award classifications are determined, can be found in the University Regulations at

https://www.mdx.ac.uk/__data/assets/pdf_file/0040/577687/Regulations-2020-21.pdf

- Practical aspects of the programme are often assessed via coursework that may be carried out using specialist software and may include lab tests.
- Theoretical material is assessed by coursework.
- Grades are awarded on the standard University scale of 1–20, with Grade 1being the highest. To pass a module all assessment, must be passed individually with a minimum grade of 16. Failure in one of the components will result in the failure of the module.

14. Placement opportunities, requirements and support

No placement option is available for this programme

15. Future careers / progression

All programmes in the faculty – their curricula and learning outcomes – have been designed with an emphasis on currency and the relevance to future employment.

- The majority of graduates are employed in IT posts relevant to the subject.
- Over 20% of students pursue further postgraduate study or research.
- The programme enables students to pursue careers in varied specialisms, these include but are not limited to: Financial Services, Auditing, Management, Financial Compliance, Consultancy, Emerging Technology Strategists, Digital Investigations, Civil Service and Law Enforcement.

Campus Careers Offices can be found on each campus for advice, support and guidance – or go to http://www.mdx.ac.uk/campus/support/careers/index.asp

16. Particular support for learning (if applicable)

The Department's Teaching and Learning Strategy is compliant with those of the University, in seeking to develop learner autonomy and resource-based learning.

In support of the students learning experience:

- All new students go through an induction programme and some have early diagnostic numeric and literacy testing before starting their programme. Learning Resources (LR) provide workshops for those students needing additional support in these areas.
- Students are allocated a personal email account, secure networked computer storage and dial-up facilities.
- New students are provided with a hard copy of the Faculty Subject Handbook at enrolment (electronic copies for all students can also be found at UniHub.
- Soft copies of all module handbooks can be found online. Web-based learning materials are provided to further support learning.
- Extensive library facilities are available on all campuses. This is available as learning resources through the My Learning Portlet system.
- High-quality specialist network, software, digital and wireless laboratories equipped with industry standard software, hardware and tools as appropriate, for formal teaching as well as self-study. Middlesex University is a Cisco Local Academy.
- Access to campus-based teaching and learning support drop-in sessions, arranged by the school to provide assistance and guidance.
- Tutorial sessions for each module organised for groups of up to 20 students are provided for additional teaching support.
- Formative feedback is given throughout the assessment period, using various methods. Students are given opportunities to show their assessment for feedback prior to submitting summative assessments. This process supports students in successfully completing their assessments.
- Research activities of academic staff feed into the teaching programme, which can provide individual students with ad-hoc opportunities to work with academics on some aspect of research.

Middlesex University encourages and supports students with disabilities. Some practical aspects of Science and Technology programmes may present challenges to students with particular disabilities. You are encouraged to visit our campuses at any time to evaluate facilities and talk in confidence about your needs. If we know your individual needs, we'll be able to provide for them more easily. For further information contact the Disability Support Service (email: disability@mdx.ac.uk).

17. JACS code (or other relevant coding system)	G500
18. Relevant QAA subject benchmark group(s)	(QAA) Computing Masters 2019 https://www.qaa.ac.uk/docs/qaa/subject-benchmark-statements/subject-benchmark-statement-computing-(masters).pdf?sfvrsn=15f2c881_10

19. Reference points

The following reference points were used in designing the programme:

- QAA Framework for Higher Education Qualifications in England, Wales and Northern Ireland
- QAA Computing subject benchmark statement towards Benchmarking Standards for Taught master's degrees - Publication Date: 30th October 2019
- CAPE guidelines for programme specifications
- QAA Code of Practice for the assurance of academic quality and standards in HE
- University Policy, Regulations and Guidelines
  Middlesex University and Faculty of Science and Technology Teaching
- Learning and Assessment policies and strategies.

20. Other information

N/A

Please note programme specifications provide a concise summary of the main features of the programme and the learning outcomes that a typical student might reasonably be expected to achieve if s/he takes full advantage of the learning opportunities that are provided. More detailed information about the programme can be found in the rest of your programme handbook and the university regulations.

Curriculum map for *[MSc Information Security Management]*

This section shows the highest level at which programme outcomes are to be achieved by all graduates, and maps programme learning outcomes against the modules in which they are assessed.

Programme learning outcomes

Knowledge and understanding	
A1	Tools and techniques necessary for carry out and manage digital forensic investigations.
A2	The nature, collection, handling and analysis of digital evidence in a forensic investigation.
A3	Regulatory compliance and the detection, investigation, and prevention of financial crime in corporate environments from emerging technologies
A4	Be able to manage audit and security processes within an organisation
A5	Assisting organisations in developing effective knowledge/data management programmes to maintain competitive advantage in knowledge/data driven economies.
A6	Be able to provide advisory services relating to blockchain strategy to organisations
A7	Manage information security management, cyber security and audit and security in learning scenarios.
A8	Legal and professional issues related to computer-related crime, digital evidence and digital forensic investigations.
A9	Principles and concepts of relating to new investigation methods for emerging technologies.
A10	Be able to manage audit and security processes within an organisation.
A11	Digital crime investigation frameworks, guidelines and procedures.
Skills	
B1	Apply relevant tools and techniques to carry out a digital forensic investigation.
B2	Investigate, collect and analyse and present relevant digital evidence from digital devices including online data stores (open blockchains).
B3	Advise on managing compliance in corporate environments and implementing tools and techniques for detecting, investigating and preventing financial crime from emerging technologies.
B4	Advise on blockchain strategy for organisations

B5	Apply relevant information security management, cyber security and audit and security principles by implementing effective solutions as an individual or in cooperation with others.
B6	Select and use a variety of modes of discourse for effective communication according to the needs of the intended audience.
B7	Perform effectively as a member of student teams in complex and diverse scenarios
B8	Demonstrate a critical understanding of, and the ability to deploy effectively, a wide range of learning methods resources and technologies, including, but not limited to, Information and Communication Technologies.
B9	Manage their own learning and development autonomously, demonstrating time management and organisational skills at a professional level.
B10	Demonstrate self-direction and originality in learning and problem-solving in familiar and unfamiliar situations.
B11	Appreciate the need for continuing professional development in recognition of the need for lifelong learning.
B12	Advise on relevant legal and professional issues related to computer-related crime, digital evidence and digital forensic investigations.
B13	Apply and validate new methods of investigation.

		Programme outcomes																					
A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	B12	B13
1	2	3	4	5	6	7	8	9	10	11	1	2	3	4	5	6	7	8	9	10	11	12	13
Highest level achieved by all graduates																							
7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7

Module Title	Module Code by Level	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	B12	B13
Audit and Security	**CST4210**		✓		✓			✓	✓	✓	✓						✓	✓		✓	✓			✓	✓
Digital investigations & Incident Management	**CST4230**	✓	✓							✓		✓	✓	✓							✓		✓		✓
FinCrime Risks from Emerging Technologies	**CST4240**		✓	✓						✓	✓				✓			✓	✓				✓		
Blockchain Strategy	**CST4280**			✓			✓								✓	✓		✓	✓	✓					
Cyber and Information Security	**CST4290**				✓			✓									✓	✓			✓	✓			
Information Security Management	**CST4300**				✓			✓									✓	✓		✓			✓		
Data Management & Decision Support	**CST4340**					✓											✓	✓	✓			✓			
PG Individual Project	**CST4390**																			✓	✓	✓	✓		