CURRICULUM DOCUMENT

QUALIFICATION:

MASTER OF COMPUTER SCIENCE (Level 7, 90 ECTS)

EXIT QUALIFICATION:

POSTGRADUATE CERTIFICATE IN COMPUTER SCIENCE (Level 7, 30 ECTS)

POSTGRADUATE DIPLOMA IN COMPUTER SCIENCE (Level 7, 60 ECTS)

EAI/2026/260501

Approved by the Senate on 06 May, 2026

Euro American Institute

AGORA BUSINESS CENTRE LEVEL 2
TRIQ IL- WIED TA' L-IMSIDA
MSIDA, MSD 9020, Malta
info@euroamerican..edu.eu

PROGRAMME SPECIFICS

Title Of The Qualification/ Award

Master of Computer Science (MCS)

MQF Level

MQF Level 7

Programme Duration

Full - Time: 1.5 Years, Part - time: 3 Years

Total Learning Hours

2250 Hours

Language/ Of Instruction Of Programmes

English

Exit Awards/Qualifications

These exit points offer flexibility and formal recognition at various stages of the Master of Computer Science (MCS) programme, supporting students in reaching their career and educational objectives, even if they do not complete the full Master of Computer Science (MCS) degree.

- **Postgraduate Certificate in Computer Science (30 ECTS):** This award is conferred upon students who successfully complete a series of core modules totalling 30 ECTS credits. The Postgraduate Certificate in Computer Science provides a comprehensive overview of critical areas in computer science, including programming, data analysis, software engineering, and system design. This certificate is particularly advantageous for individuals seeking to advance their careers in the tech industry or enhance their technical expertise without the commitment of a full master's programme.
- **Postgraduate Diploma in Computer Science (AI & Data Science or Cybersecurity) (60 ECTS):** This award is granted to students who successfully complete a comprehensive set of 30 ECTS credits in core modules and 30 ECTS credits in a chosen specialisation (AI & Data Science or Cybersecurity). The core modules provide a strong foundation in Computer Science, covering essential concepts This diploma is particularly advantageous for professionals seeking to enhance their expertise in a specific

area of computer science, strengthening their career prospects in the tech industry.

PROGRAMME STRUCTURE

Module Title	Compulsory (C) or Elective (E)	MQF Level of each Module	Mode of Teaching (Lectures, workshops, placement, asynchronous, forums, VLE, etc.)	Mode of Assessment (Examination, assignment, project, blog, etc.)
Software programming principles and practices in Java	Compulsory (C)	**7**	Lectures, Workshop / Case Analysis, Asynchronous forums and VLE	Written assignments 40%) Programming /Mini Project (30%) Final Examination (30%)
Database & SQL Programming	Compulsory (C)	**7**	Lectures, Workshop / Problem Based Assignment / Case Analysis, Asynchronous forums and VLE	Written assignments (40%) Simulation Assessment (30%) Final Examination (30%)
Computer Architecture	Compulsory (C)	**7**	Lectures, Workshop / Problem Based Assignment / Case Analysis, Asynchronous forums and VLE	Written assignments 40%) Problem Analysis (30%) Final Examination (30%)
Computer Networks	Compulsory (C)	**7**	Lectures Workshop / Case Analysis, Asynchronous forums and VLE	Written assignments (40%) Case Analysis (30%) Final Examination (30%)
Advanced Computing Research Methods	Compulsory (C)	**7**	Lectures, Workshop / Case Analysis, Asynchronous forums and VLE	Written assignments (40%) Critical Literature Review (30%) Final Examination (30%
Data Science Foundations	Elective	**7**	Lectures, Workshop / Case Analysis, Asynchronous forums and VLE	Written assignments (40%) Virtual Lab Exercise (30%) Final Examination (30%)
Data Mining, Machine Learning and Artificial Intelligence	Elective	**7**	Lectures, Workshop /Case Analysis, Asynchronous forums and VLE	Written assignments 40%) Programming /Mini Project (30%) Final Examination (30%)
Data Analysis and Visualisation	Elective	**7**	Lectures, Workshop /Case Analysis, Asynchronous forums and VLE	Written assignments (40%) Critical Literature Review (30%) Final Examination (30%)
Probability and Statistics for Data Analysis	Elective	**7**	Lectures, Workshop / Case Analysis, Asynchronous forums and VLE	Written assignments (40%) Critical Literature Review (30%) Final Examination (30%)

Security Engineering	Elective	**7**	Lectures, Workshop/ Case Analysis, Asynchronous forums and VLE	Written assignments (40%) Programming Mini Project (30%) Final Examination (30%)
Internet of Things and Cryptography	Elective	**7**	Lectures, Workshop / Formative Knowledge Check / Case Analysis, Asynchronous forums and VLE	Written assignments 40%) Formative Knowledge Check (30%) Final Examination (30%)
Networking and Kali Linux	Elective	**7**	Lectures, Workshop / Formative Knowledge Check / Case Analysis, Asynchronous forums and VLE	Written assignments 40%) Formative Knowledge Check (30%) Final Examination (30%)
Engineering of Hacking	Elective	**7**	Lectures, Workshop / Formative Knowledge Check / Case Analysis, Asynchronous forums and VLE	Written assignments 40%) Formative Knowledge Check (30%) Final Examination (30%)
Forensic Computing	Elective	**7**	Lectures, Workshop / Case Analysis, Asynchronous forums and VLE	Written assignments 40%) Peer Review (30%) Final Examination (30%)
Application and Device Audit	Elective	**7**	Lectures, Workshop/ Case Analysis Asynchronous forums and VLE	Written assignments 40%) Peer Review (30%) Final Examination (30%)
Capstone Project	Compulsory (C)	**7**	Project and Dissertation	Dissertation and Project Work (100%)

TABLE A								
MODULES COVERED								
YEAR 1								
Module Ref. No.	Module Title	Level	ECTS	TCH	SPPH	SSH	AH	TLH
MCS701	Software programming principles and practices in Java	7	6	30	20	80	20	150
MCS702	Database & SQL Programming	7	6	30	20	80	20	150
MCS703	Computer Architecture	7	6	30	20	80	20	150
MCS704	Computer Networks	7	6	30	20	80	20	150
MCS705	Advanced Computing Research Methods	7	6	30	20	80	20	150
MCSXYZ	Elective 1	7	6	30	20	80	20	150
MCSXYZ	Elective 2	7	6	30	20	80	20	150
MCSXYZ	Elective 3	7	6	30	20	80	20	150
MCSXYZ	Elective 4	7	6	30	20	80	20	150
MCSXYZ	Elective 5	7	6	30	20	80	20	150
YEAR TOTAL			60	300	200	800	200	1500
YEAR 2								
MCS716	Capstone Project	7	30	150	150	330	120	750
MCS PROGRAMME TOTAL			90	450	350	1130	320	2250

TABLE B - ELECTIVES								
Specialization: AI & Data Science								
Module Ref. No.	**Unit title**	**Level**	**ECTS**	**TCH**	**SPPH**	**SSH**	**AH**	**TLH**
MCS706	Data Science Foundations	7	6	30	20	80	20	150
MCS707	Data Mining, Machine Learning and Artificial Intelligence	7	6	30	20	80	20	150
MCS708	Data Analysis and Visualisation	7	6	30	20	80	20	150
MCS709	Probability and Statistics for Data Analysis	7	6	30	20	80	20	150
MCS710	Security Engineering	7	6	30	20	80	20	150

TABLE C - ELECTIVES								
Specialization: Cyber Security								
Module Ref. No.	**Unit title**	**Level**	**ECTS**	**TCH**	**SPPH**	**SSH**	**AH**	**TLH**
MCS711	Internet of things and Cryptography	7	6	30	20	80	20	150
MCS712	Networking and Kali Linux	7	6	30	20	80	20	150
MCS713	Engineering of Hacking	7	6	30	20	80	20	150
MCS714	Cloud Computing and Forensic Investigation	7	6	30	20	80	20	150
MCS715	Application and Device Audit	7	6	30	20	80	20	150

TCH	Total Contact Hours. Contact Hours are hours invested In learning new content under the Direction of a tutor/lecturer (e.g. lectures participation in online forums, video-lectures)
SPPH	Supervised Placement and Practice Hours. (During these hours the learner is supervised, coached or mentored). Supervision hours are structured to provide effective virtual support for students. Initially, students engage in weekly online consultations with their supervisors via video conferencing platforms, where they clarify research objectives and set milestones. Biweekly virtual progress review meetings are scheduled to assess ongoing work and address any issues that arise. Monthly feedback and guidance sessions are conducted through online platforms where supervisors provide detailed feedback on drafts and research methodologies. Additionally, biannual online workshops and training sessions are organised to enhance research skills and academic writing. As the final submission approaches, students participate in virtual final review sessions and presentation preparations to ensure they meet all requirements and are well-prepared for their assessments. This approach ensures that students receive continuous and effective support throughout their research project, even in an online environment.
SSH	Self-Study Hours. (Estimated workload of research and study)
AH	Assessment Hours (Examinations/ presentations/ group work/ projects etc.)
TLH	Total Learning Hours

OVERALL PROGRAMME DESCRIPTION

The Master of Computer Science (MCS) offered by the Euro American Institute is an 18-month, fully online postgraduate programme designed to provide learners with advanced theoretical knowledge and applied digital skills in contemporary areas of computing, with specialisations in Artificial Intelligence & Data Science or Cybersecurity. Although a total of 120 ECTS worth of modules are submitted for MFHEA accreditation to accommodate a structured elective pool, the qualification award is strictly capped at 90 ECTS, in full compliance with MQF Level 7 requirements. The programme delivers a structured curriculum covering core computer science foundations alongside advanced study in areas such as machine learning, data analytics, network and system security, cloud computing, and DevOps practices. Content is delivered through a combination of asynchronous learning materials, live online sessions, virtual laboratories, and collaborative digital tools, ensuring academic rigour within a fully online environment. Practical learning is achieved through cloud-based virtual laboratories, simulated environments, and controlled sandbox platforms, which allow learners to design, develop, test, and evaluate software, data-driven, and security-focused solutions. While the programme does not involve physical access to on-premise ICT infrastructure, learners gain industry-relevant troubleshooting, deployment, and optimisation experience through virtualised systems, cloud platforms, and DevOps pipelines that reflect contemporary professional practice. Hands-on learning is embedded across modules through:

- Individual and group-based projects
- Collaborative coding tasks and code reviews
- Data-driven case studies
- Simulated security and system scenarios

Capstone and industry-oriented projects Advanced topics such as cloud computing, containerisation, CI/CD pipelines, and DevOps workflows are integrated at postgraduate level to ensure that learners understand modern software delivery and infrastructure management in distributed and online environments. The programme also places emphasis on research-informed practice, enabling learners to critically evaluate emerging technologies, apply appropriate methodologies, and engage with real-world problem contexts using virtual collaboration tools. Team-based activities and structured peer interaction are incorporated to reflect professional working practices in globally distributed technology teams. Graduates of the programme are prepared for technical and analytical roles in areas such as AI development, data science, cybersecurity, cloud-

based software engineering, and secure systems administration. The programme does not lead to a regulated profession or warranted occupation; however, it provides a strong academic and practical foundation for careers in advanced and evolving technology sectors, as well as progression to further research or professional development.

Learning Outcomes for Knowledge obtained at the end of the programme

After completing a Master of Computer Science (MCS) degree programme with a specialisation in Artificial Intelligence (AI) & Data Science or Cybersecurity, learners will achieve several key learning outcomes. These outcomes combine advanced technical skills, theoretical knowledge, and hands-on experience, preparing graduates for successful careers in their chosen field. On successful completion of the programme, graduates will be able to:

- **Demonstrate specialised and critical understanding of core computer science domains,** including software programming, database systems, computer architecture, computer networks, and security engineering, as applied in modern computing environments
- **Critically evaluate advanced theories, models, and architectures** underpinning artificial intelligence, data science, machine learning, and cybersecurity, including their assumptions, limitations, and applicability in real-world contexts.
- **Analyse and compare computational, analytical, and security techniques used to design,** implement, and evaluate intelligent, data-driven, and secure computing systems.
- **Demonstrate integrated knowledge of data lifecycles and data governance**, including data acquisition, modelling, storage, processing, analysis, visualisation, and protection in large-scale and security-sensitive environments.
- **Demonstrate critical awareness of ethical, legal, professional, and societal considerations** in computer science, including privacy, data protection, cybersecurity governance, algorithmic bias, accountability, and sustainability.
- **Demonstrate advanced understanding of research methodologies in computer science,** including problem formulation, literature review, data collection, and evaluation methods used in academic and industry-based research.

Mapping – KNOWLEDGE Learning Outcomes to MQF Level 7 Descriptors

Programme Learning Outcomes – Knowledge	MQF Level 7 Descriptor Coverage
K1. Demonstrate specialised and critical understanding of core computer science domains (programming, databases, architecture, networks, security).	• Uses specialised theoretical and practical knowledge at the forefront of a field of study • Has comprehensive specialised knowledge forming the basis for original thinking
K2. Critically evaluate advanced theories, models, and architectures in AI, data science, machine learning, and cybersecurity.	• Uses specialised or multi-disciplinary knowledge at the forefront of the field • Performs critical evaluations in new or unfamiliar contexts
K3. Analyse and compare computational, analytical, and security techniques used in intelligent, data-driven, and secure systems.	• Critical awareness of knowledge issues at the interface between different fields • Multi-disciplinary theoretical and practical knowledge
K4. Demonstrate integrated knowledge of data lifecycles and data governance in large-scale and security-sensitive environments.	• Integrates knowledge from different fields • Knowledge contributes to social, ethical, and organisational contexts
K5. Demonstrate critical awareness of ethical, legal, professional, and societal considerations in computer science.	• Reflects on social and ethical responsibilities linked to application of knowledge and judgement
K6. Demonstrate advanced understanding of research methodologies in computer science.	• Knowledge forms the basis of original research • Research-informed and multi-disciplinary theoretical knowledge

Learning Outcomes for Skills obtained at the end of the programme

Upon successful completion of the Master of Computer Science (MCS) programme, graduates will:

- **Design, implement, and critically evaluate advanced computing solutions**, integrating programming, database, networking, architectural, and security principles to address complex or unfamiliar problems.
- **Select, adapt, and apply advanced algorithms, analytical methods, and computational techniques** in artificial intelligence, data science, machine learning, or cybersecurity contexts, making defensible judgements where information is incomplete or uncertain.
- **Conduct research-based diagnosis of complex computing problems** by integrating interdisciplinary knowledge, analysing evidence, and evaluating alternative solutions using appropriate research methods.
- **Apply systematic testing, validation, and evaluation techniques** to assess the performance, reliability, scalability, and security of software systems, data pipelines, networks, and intelligent applications.
- **Communicate complex technical concepts, analytical findings, and system designs clearly and**

professionally to specialist and non-specialist audiences using appropriate reports, visualisations, and technical documentation.

- **Plan, manage, and take responsibility for technical tasks and projects**, making informed decisions in collaborative and professional computing environments.

Mapping – SKILLS Learning Outcomes to MQF Level 7 Descriptors

Programme Learning Outcomes – Skills	MQF Level 7 Descriptor Coverage
S1. Design, implement, and critically evaluate advanced computing solutions to complex or unfamiliar problems.	• Applies specialised problem-solving skills required in research and innovation • Solves problems in new or unfamiliar environments
S2. Select and apply advanced algorithms and computational techniques, making judgements with incomplete or uncertain information.	• Performs critical evaluations with incomplete or limited information • Makes judgements in complex and unpredictable contexts
S3. Conduct research-based diagnosis of complex computing problems by integrating interdisciplinary knowledge.	• Creates a research-based diagnosis to problems • Integrates knowledge from new or interdisciplinary fields
S4. Apply systematic testing, validation, and evaluation techniques to assess performance, scalability, and security.	• Develops new procedures and applies specialised problem-solving skills • Produces outcomes informed by research and analysis
S5. Communicate complex technical concepts and findings clearly to specialist and non-specialist audiences.	• Communicates clearly and unambiguously to specialist and non-specialist audiences • Reaches conclusions from research, self-study, or experience
S6. Plan, manage, and take responsibility for technical tasks and projects in professional computing contexts.	• Manages people and projects efficiently • Adapts to fast-changing business and technological environments
S7. Demonstrate advanced learning skills through self-directed learning and continuous professional development.	• Develops new skills in response to emerging knowledge and techniques • Demonstrates autonomy in the direction of learning • Has learning skills for continued, largely self-directed study

General Pedagogical methods used for this programme

The Master of Computer Science (MCS) (with specialisations in Artificial Intelligence & Data Science or Cybersecurity) is delivered entirely online through a structured, technology-enabled learning system designed to ensure academic rigour, learner engagement, accessibility, and practical relevance in full alignment with MQF Level 7 requirements. The online delivery model integrates synchronous and asynchronous learning, cloud-based virtual laboratories, collaborative digital tools, and continuous academic supervision. This integrated approach enables learners to achieve programme learning outcomes effectively while maintaining structured interaction, progression monitoring, and applied skills development within a fully online environment.

Online Learning Environment and Digital Infrastructure

Learning Management System (LMS) / Virtual Learning Environment (VLE)

All teaching, learning, supervision, and assessment activities are delivered through a centrally managed Learning Management System (LMS), which serves as the primary academic control and communication platform. The LMS provides:

- Access to recorded lectures, learning resources, and assessment materials
- Structured weekly learning pathways aligned with module learning outcomes
- Moderated discussion forums and academic announcements
- Assignment submission, grading, and formative and summative feedback mechanisms
- Attendance, participation, and engagement tracking for audit and quality assurance purposes

Programming, AI, and Data Science Virtual Laboratories

To support applied learning in a fully online environment, learners engage with cloud-based virtual laboratories and industry-standard software tools, including:

1. Integrated Development Environments (IDEs):
   Visual Studio Code, PyCharm, and browser-based IDEs for software development and programming activities.

2. Data Science and AI Platforms:
   Jupyter Notebooks, cloud-hosted notebook environments, Python and R ecosystems, and machine-learning libraries such as TensorFlow, PyTorch, and Scikit-learn.

3. Cloud Computing Resources:
   Virtual machines and cloud-based coding sandboxes enabling scalable experimentation, large-dataset processing, and remote access without reliance on local hardware.

4. Version Control and Collaboration:
   Git-based version control using GitHub or GitLab to support collaborative development, code review, and systematic version tracking.

These tools allow learners to apply theoretical concepts through supervised, hands-on activities within secure and controlled online environments.

Cybersecurity and Networking Virtual Laboratories

Cybersecurity and networking modules are supported through simulated and virtualised security environments that replicate realistic ICT infrastructures. These include:

- Virtual network and system laboratories for configuration, monitoring, and security testing
- Isolated sandbox environments for vulnerability analysis, threat modelling, and incident- response simulations
- Cloud-based security tools enabling controlled and ethical experimentation

All security-related activities are conducted within isolated and instructor-controlled environments, ensuring safe, ethical, and compliant practice while developing applied cybersecurity competencies.

Online Teaching and Learning Strategies

1. Synchronous Online Sessions

   Live, tutor-led online sessions are delivered using video-conferencing platforms and are formally scheduled within the academic timetable. These sessions are used to:

   - Introduce and explain complex or advanced concepts
   - Facilitate real-time interaction, questioning, and problem-solving
   - Deliver guided demonstrations, walkthroughs, and applied discussions
   - Provide structured academic support and formative feedback

   Attendance and participation are recorded through the LMS to ensure verifiable contact hours.

Minimum Synchronous Contact Hours per Module

Each 6-ECTS module within the Master of Computer Science programme includes a minimum of 30 contact hours, of which at least 12 hours are delivered through scheduled live synchronous sessions.

- Live synchronous sessions are formally timetabled and include: Tutor-led lectures
- Advanced concept walkthroughs
- Supervised practical workshops Research clinics
- Guided problem-solving sessions Structured project supervision meetings
- The remaining contact hours (where applicable) may include moderated academic forums and structured interactive engagement activities delivered through the Virtual Learning Environment (VLE).

This ensures consistent real-time academic interaction across all modules and pathways, meeting and exceeding the MFHEA minimum contact-hour requirement (5 hours per ECTS).
All live sessions are recorded, attendance is monitored, and participation is tracked through the LMS for audit and quality assurance purposes.

2. **Asynchronous Learning**

Asynchronous learning activities are designed to support flexibility while maintaining academic structure and engagement. These activities include:

- Pre-recorded lectures with captions and downloadable transcripts
- Guided tutorials, demonstrations, and worked examples
- Self-paced coding exercises and virtual laboratory tasks
- Online discussion forums moderated by academic staff

This blended online model ensures accessibility for learners across different time zones while sustaining consistent

academic interaction and progression.

3. **Asynchronous Engagement and Cohort Building**

Asynchronous learning activities are structured to promote engagement and cohort cohesion. Weekly discussion forums are moderated by academic staff and aligned to module topics. Learners participate in peer discussion, collaborative problem-solving tasks, and reflective activities. Group-based assignments and peer review exercises are embedded across selected modules to encourage sustained interaction. Cohort identity is reinforced through programme-wide announcements, shared induction activities, and synchronous touchpoints throughout the academic year.

4. **Synchronous and Asynchronous Learning Design**

The programme adopts a balanced blend of synchronous and asynchronous online learning. Synchronous sessions include live lectures, workshops, research clinics, and supervision meetings, enabling real-time interaction, immediate feedback, and academic dialogue. Asynchronous learning includes recorded lectures, guided tutorials, virtual labs, and discussion forums, allowing flexibility and deeper reflection. This design ensures pedagogical equivalence to face-to-face delivery while enhancing accessibility and learner autonomy.

Academic Capacity and Staff-to-Student Ratio Framework

To ensure high-quality delivery, effective supervision, and structured facilitation of group-based learning activities, the programme operates within a defined academic capacity framework.

2. Staff-to-Student Ratio (Taught Modules)

For synchronous and laboratory-based modules, the programme maintains a target academic ratio of:

- 1 academic staff member per 20–25 learners for lecture-based modules.
- 1 academic staff member per 15–20 learners for laboratory-intensive or technically advanced modules.

Where cohort size exceeds these thresholds, additional teaching assistants or co-facilitators are allocated to maintain effective engagement and academic oversight.

3. Group-Based Project Supervision

Group-based assignments are structured with defined supervision parameters:

- Maximum group size: 4–5 learners per group.
- Each academic staff member supervises no more than:
  - 6–8 project groups per module.
  - Scheduled supervision checkpoints are embedded within each group project timeline.

This ensures meaningful formative feedback, equitable workload distribution, and consistent academic monitoring across groups.

4. Capstone Project Supervision

For the individual Capstone Project (30 ECTS), supervision capacity is formally capped to preserve academic quality:

- Each supervisor may oversee a maximum of 8–10 capstone projects per academic cycle.
- Supervisory engagement includes:

- Structured milestone reviews,
- Methodological clinics,
- Feedback cycles prior to final submission

Where enrolment increases beyond supervisory capacity, additional qualified supervisors are appointed before new learners are accepted.

5. Maximum Cohort Size

To maintain academic integrity and supervision quality, the programme operates with:

- A recommended maximum intake of 30–40 learners per cohort.
- Expansion beyond this threshold is contingent upon proportional increase in qualified academic staff.

6. Monitoring and Workload Allocation

Academic workload allocation is monitored at programme level and reviewed each semester to ensure:

- Balanced supervision distribution,
- Sustainable marking load,
- Adequate formative engagement,
- Compliance with institutional quality assurance standards.

This structured ratio model ensures the programme's delivery capacity remains aligned with its academic rigor, particularly in modules involving advanced theoretical content, laboratory engagement, and group- based assessments.

Group-Based Online Projects

Structured group-based projects are formally embedded within selected modules. Learners collaborate remotely in small, supervised groups using:

- Microsoft Teams or Slack for structured communication and coordination
- GitHub or GitLab repositories for collaborative coding and version control
- Shared online documentation tools for planning, reporting, and reflection

Group-based assessments evaluate learners' ability to apply advanced knowledge collaboratively, address complex problems, and operate effectively in distributed professional environments, consistent with MQF Level 7 expectations.

Group-based activities form a **mandatory and assessed component** of the selected modules and are supervised by academic staff to ensure active participation, collaboration, and achievement of learning outcomes.

Module-Aligned Online Learning Activities and Tools

Online learning activities are explicitly tailored to the pedagogical and practical requirements of individual modules:

- **Core Computing Modules:**

  Online lectures, guided coding exercises, formative knowledge checks, and virtual labs supported by IDEs and version-control systems.

- **AI & Data Science Modules:**

  Cloud-based data analysis, machine-learning model development, case studies using real- world datasets, and supervised group projects.

- **Cybersecurity Modules:**

  Scenario-based learning, virtual network simulations, penetration-testing exercises, and incident-response activities conducted within controlled online environments.

- **Research and Capstone Modules:**

  Independent and collaborative research supported by structured digital supervision, scheduled virtual meetings, and cloud-based development and analysis tools.

  This approach ensures constructive alignment between module learning outcomes, online teaching and learning activities, supervision arrangements, and assessment methods across the programme.

Accessibility and Inclusive Design

The online learning environment is designed in accordance with recognised accessibility and inclusive-learning principles to ensure equitable participation for all learners. Teaching and learning materials are developed in line with the Web Content Accessibility Guidelines (WCAG) principles, with appropriate reasonable adjustments where required.

Accessibility provisions include:

- Captioned video lectures and downloadable transcripts;
- Screen-reader-compatible learning materials and structured documents;
- Low-bandwidth alternatives, including downloadable resources and asynchronous participation options;
- Flexible engagement pathways to support learners across different time zones and connectivity contexts.

These measures ensure that the fully online mode of delivery is accessible, inclusive, and robust in practice.

Support for Disabled Students and Inclusivity Measures

The Master of Computer Science programme is delivered in accordance with the Institute's Equality, Diversity, and Inclusion Policy, which includes specific provisions to support learners with disabilities and additional learning needs. The programme adopts an inclusive design approach, ensuring that learning materials, teaching methods, and assessment practices are accessible and flexible.

Learners with disabilities or specific learning needs may request **reasonable adjustments**, which may include extended assessment deadlines, alternative assessment formats where appropriate, accessible learning materials, assistive technologies, and tailored academic support. All requests are assessed on an individual basis to ensure that academic standards and learning outcomes are maintained while enabling full and equitable participation.

Given the fully online delivery of the programme, accessibility is further supported through recorded lectures, asynchronous learning resources, flexible engagement with virtual laboratories, and multiple communication channels with academic staff and student support services. The Institute works proactively with learners to identify and implement appropriate support measures throughout the programme lifecycle.

Inclusive and Flexible Teaching Approach

The programme's teaching methods are deliberately diversified to support learners with different educational backgrounds, learning preferences, and professional commitments. Lecture-based instruction supports conceptual understanding, while problem-based and project-based learning enables experiential learning and applied problem-solving. Case studies and simulations provide contextualised learning for industry-oriented learners, while asynchronous materials support self-paced study for working and international students. Live sessions, collaborative activities, and guided supervision ensure academic interaction and inclusion across learner profiles.

Learner Progress Monitoring and Academic Support

Regular formative progress checkpoints and tutor feedback sessions are embedded across modules to **monitor learner engagement, assess progression, and provide early academic intervention**, with particular support for part-time and mature learners studying over an extended duration.

Structured Monitoring Framework for Mature and Part-Time Learners

Given the inclusion of mature learners (ages 31–65) and potential part-time study pathways, the programme implements a structured academic monitoring framework designed to support sustained engagement and timely progression.

Monitoring mechanisms include:

1. **Early Engagement Tracking**
    - Weekly LMS activity monitoring
    - Attendance tracking for live sessions
    - Automated alerts for inactivity exceeding 7 days
2. **Scheduled Academic Checkpoints**
    - Mid-module progress reviews
    - Formative assessment diagnostics
    - Structured tutor feedback sessions
3. **Risk Identification and Intervention**

    Learners identified as:
    - Missing live sessions,
    - Submitting late assignments,
4. Underperforming in formative assessments are flagged for targeted academic intervention.
5. **Individual Academic Support Plans**

    Where necessary, learners receive:
    - Individual advisory meetings
    - Adjusted pacing plans
    - Reinforcement clinics
    - Structured milestone planning

6. Capstone Readiness Review

Prior to commencement of the Capstone Project, learners undergo a formal readiness review to ensure academic preparedness, particularly for those studying part-time or returning after extended duration.

All monitoring processes are documented through the VLE and retained for internal quality assurance and audit review.

This structured monitoring framework ensures that mature and part-time learners receive proactive academic support while maintaining MQF Level 7 academic standards.

Structured Academic Pace Adjustment and Support Framework

Recognising that certain advanced theoretical modules (e.g., Probability and Statistics, Machine Learning, Cryptography, and Research Methods) may present heightened cognitive and analytical demands consistent with MQF Level 7 expectations, the programme incorporates a structured Academic Pace Adjustment and Support Framework to ensure equitable progression while maintaining academic rigor.

This framework does not dilute learning outcomes or reduce academic standards. Rather, it provides structured academic scaffolding, staged learning reinforcement, and controlled progression flexibility.

1. Early Diagnostic Monitoring

During the first four weeks of each advanced module, learners complete:

- Diagnostic formative knowledge checks;
- Structured low-stakes problem-solving exercises;
- Tutor-monitored discussion participation.

These diagnostics allow academic staff to identify learners requiring additional support at an early stage.

2. Staged Content Scaffolding

Advanced theoretical modules are structured using:

- Concept layering (fundamental → intermediate → advanced);
- Scaffolded laboratory activities;
- Worked problem walkthrough sessions;
- Guided analytical frameworks prior to independent tasks.

This approach ensures cognitive progression rather than abrupt exposure to abstract theoretical constructs.

3. Academic Reinforcement Clinics

Where required, learners may attend:

- Optional synchronous reinforcement clinics;
- Problem-solving workshops;
- Statistical or mathematical refresher sessions;
- Research design clinics (for Research Methods).

These sessions are formally scheduled and recorded within the VLE and do not replace contact hours but supplement them.

4. Controlled Assignment Staging

Major assignments in advanced modules are structured in stages:

- Proposal submission;
- Interim technical checkpoint;
- Draft feedback;
- Final submission.

This staged assessment design allows iterative academic feedback and prevents cumulative overload.

Flexible Progression Without Credit Reduction Where a learner demonstrates temporary academic difficulty:

- Module reassessment opportunities remain aligned with institutional regulations;
- The learner may shift from accelerated pacing to standard pacing within the same academic year;
- In exceptional cases, learners may convert to a structured part-time pathway without loss of earned credits.

Academic standards, learning outcomes, ECTS volume, and assessment criteria remain unchanged.

6. Supervisor-Guided Capstone Preparation

Entry to the Capstone Project requires successful completion of Research Methods. Learners identified as requiring reinforcement receive structured pre-capstone supervision sessions to strengthen methodological readiness prior to project commencement.

7. Preservation of MQF Level 7 Standards

All pace adjustments preserve:

- Contact hour requirements;
- Supervised practice hours;
- Assessment integrity;
- Learning outcome achievement;
- MQF Level 7 descriptor alignment.

The framework ensures that academic rigor is maintained while providing structured support mechanisms for learners encountering difficulty in advanced theoretical domains.

Recording and Monitoring of Contact and Supervised Hours

All live contact hours and supervised placement and practice activities are scheduled, recorded, and tracked through the Virtual Learning Environment. Attendance, participation, and supervision records are maintained to ensure transparency, quality assurance, and compliance with MFHEA requirements for online delivery.

All synchronous contact sessions are recorded, retained, and auditable through the Virtual Learning Environment in line with MFHEA quality assurance requirements.

These hours do not involve external placements or Work-Based Learning; they consist of supervised online

laboratories, guided tutorials, project clinics, and scheduled supervision recorded in the VLE.

Access to Digital Library Resources and Scientific Databases

All learning resources for the Master of Computer Science programme are provided in digital format, consistent with the fully online mode of delivery. Learners are granted access to a range of e-book repositories and scientific journal databases through the institution's digital library services.

Learners **may be provided with access to a range of academic and professional resources**, depending on programme needs, including selected publishers and repositories relevant to computer science, artificial intelligence, data science, and cybersecurity (e.g., IEEE Xplore, ACM Digital Library, SpringerLink, Elsevier ScienceDirect, and open-access journals and conference proceedings).

Access is provided either through institutional library subscriptions, licensed electronic resources, or recognised open-access platforms. All core and supplementary reading materials listed in the modules are available digitally to ensure equitable access for all learners.

DETAILED

CURRICULUM

MCS701

Software programming principles and practices in Java

Module Description

The aim of this module is to develop learners' understanding on what a programming language is, how it works and how to interact with computers using a programming language. The learner will cover all the basic concepts of a programming language and is taught through real world coding examples; the learner will have regular coding assignments for better understanding through practice. Students engage with current research literature and professional sources on modern programming practices, including software maintainability, performance optimisation, and secure coding. Emerging topics such as concurrent programming, memory management in managed runtimes, and evolving Java frameworks are explored through reference to peer-reviewed articles and industry research.

Learning Outcomes

Competences:

At the end of the Module the learner will have acquired the responsibility and autonomy to:

- **Manage and take responsibility for complex software development activities**, including the design, optimisation, and deployment of Java applications in unpredictable technical contexts.
- **Exercise leadership and professional accountability in programming projects**, guiding teams in the application of advanced programming principles, best practices, and ethical standards.
- **Independently utilise and adapt advanced programming tools and environments** (including JVM-based toolchains) to respond effectively to evolving project requirements and technological change.
- **Integrate interdisciplinary knowledge and advanced professional judgement** to develop innovative and resilient software solutions, particularly where requirements are incomplete, evolving, or contested

Knowledge:

At the end of the Module the learner will have been exposed to the following:

- **Demonstrate highly specialised and critical understanding of object-oriented**

programming principles in Java, synthesising knowledge of data types, operators, control structures, and execution models as a basis for original and informed software development.

- **Critically evaluate Java compilation and execution mechanisms**, including bytecode generation, compiler behaviour, and Java Virtual Machine (JVM) architecture, with particular attention to performance, portability, and optimisation in complex software systems.
- **Integrate advanced theoretical knowledge of programming** constructs and runtime environments to analyse how programming decisions influence scalability, maintainability, and efficiency in contemporary software applications.
- **Critically analyse the interaction between programming principles and emerging computing contexts**, including data-intensive systems, automation, and security-sensitive environments, demonstrating awareness of limitations and unresolved challenges at the interface of multiple domains.
- **Demonstrate critical awareness of ethical, professional, and societal considerations** arising from advanced software development, including reliability, accountability, and responsible use of computational resources.

Skills:

At the end of the Module the learner will have acquired the following skills:

- **Design, implement, and critically evaluate advanced Java-based computational solutions,** integrating data structures, operators, and control mechanisms to address complex or unfamiliar programming problems using research-informed judgement.
- **Critically evaluate alternative programming strategies and execution pathways**, making defensible technical decisions under conditions of uncertainty, incomplete information, or competing performance constraints.
- **Apply sophisticated debugging, testing, and performance-analysis techniques** to diagnose and resolve non-trivial programming errors, proposing original improvements that extend beyond routine coding practices.
- **Optimise Java programs for performance and scalability**, critically assessing the impact of programming constructs, memory management, and execution models on

system behaviour in dynamic environments.

- **Communicate complex programming designs, execution logic, and optimisation decisions** clearly and unambiguously to specialist and non-specialist audiences, justifying solutions through structured technical reasoning.
- **Demonstrate advanced learning skills by independently identifying emerging programming paradigms,** Java frameworks, tools, and development methodologies, critically evaluating their relevance to professional practice, and undertaking self-directed learning to maintain and enhance specialised programming competence.

Module-Specific Learner Skills

Upon completion of the module, learners will demonstrate enhanced abilities in

- Enhanced ability to troubleshoot and debug Java code effectively.
- Improved capacity to analyse and optimise code for efficiency and performance.
- Ability to apply Java concepts to different programming scenarios and environments.
- Heightened attention to detail in writing and reviewing Java code for accuracy and correctness.
- Enhanced skills in collaborating with peers on coding projects and problem-solving tasks.

Module-Specific Digital Skills and Competences

Learners will develop digital skills and competencies including

- Proficiency in using version control systems such as Git for collaborative coding and code management.
- Competence in utilising IDEs like IntelliJ IDEA or Eclipse for Java development, including code editing, debugging, and project management.
- Skill in writing and executing unit tests using frameworks like JUnit to ensure code quality and functionality.
- Ability to create comprehensive documentation for Java code, including comments, README files, and API documentation.

Hours of Total Learning for this Module

- **Total Contact Hours: 30**

Contact Hours are hours invested in learning new content under the Direction of a tutor/lecturer e.g. lectures participation in online forums

- **Supervised Placement and Practice Hours: 20**

  During these hours the learner is supervised, coached, or mentored.

- **Self-Study Hours: 80**

  Estimated workload of research and study

- **Assessment Hours: 20**

  Examinations/ presentations/ group work/ projects etc.

- **Total Number of ECTS of this Module/Unit: 6 ECTS**

Total Learning Hours of this Module: 150 Hours

Pedagogy for this Module

In this module, students will immerse themselves in a dynamic online learning environment, integrating diverse instructional methods to foster a comprehensive grasp of Java programming. Interactive lectures, whether live or pre-recorded, will cover foundational principles and syntax, encouraging active participation and collaboration. Hands-on coding labs will offer practical experience within integrated development environments (IDEs), allowing students to experiment with data types and algorithms. Demonstrations and examples will provide real-world context, while assignments and projects will challenge students to apply their skills and problem-solving abilities. Online discussions and peer interaction will further deepen comprehension, supplemented by continuous feedback and assessments. Guest speakers and industry insights will offer valuable perspectives on current practices, enriching students' understanding and readiness for professional applications. Supported by self-paced resources, students will have the flexibility to reinforce their learning and emerge as proficient Java programmers. This module includes regular live synchronous sessions, such as supervised practical workshops, tutor-led demonstrations, live problem-solving sessions, and scheduled progress reviews. These activities form part of the module's contact hours and supervised placement and practice (non-WBL) hours and are delivered via video-conferencing tools integrated into the Virtual Learning Environment (VLE).

Assessment method for this particular module

Assessment Weightings:

- Written assignments (40%) (It should not be more than 1250-word count)
- Programming/ Mini Project/Lab work (30%)
- Final Examination (30%)

Learners must achieve a minimum of 50% overall and 50% in each assessment component; authenticity is verified through Turnitin (similarity and AI-writing indicators), VLE audit trails, and a recorded online viva and/or timed proctored task where appropriate, in accordance with institutional assessment regulations.

Digital learning tools like online submission platforms, code repositories, and video conferencing software will facilitate assessment

Reading List

- Schildt, H. (2021). Java: The Complete Reference (12th ed.). McGraw-Hill Education.
- Goodrich, M. T., Tamassia, R., & Goldwasser, M. H. (2021). Data Structures and Algorithms in Python. John Wiley & Sons.
- Mitchell, M. (2020). Artificial Intelligence: A Guide for Thinking Humans. Farrar, Straus and Giroux.
- Filho, W. F. (2021). Computer Science Distilled: Learn the Art of Solving Computational Problems. Code Energy.
- Müller, A. C., & Guido, S. (2021). Introduction to Machine Learning with Python: A Guide for Data Scientists (2nd ed.). O'Reilly Media.
- Eckel, B. (1998). Thinking in Java, Mind View. Inc.
- Horstmann, S., Cornell, G., & Java, C. (2). Volume I-Fundamentals.

Suggested Research Oriented reading:

- Bloch, J. (2008). Effective java (the java series). Prentice Hall PTR.
- Burd, B. (2017). Beginning programming with Java for Dummies. John Wiley & Sons.
- Schildt, H. (2022). Java: a beginner's guide. McGraw-Hill Education.

- Sierra, K., & Bates, B. (2003). Headfirst Java; covers Java 5.0. A Brain Friendly Guide, O'REILLY Publication, 2nd Edition, ISBN-10, 596009208.

MCS702

Database & SQL Programming

Module Description

The aim of this module is to develop the learner's ability to understand the shortfalls of traditional storage systems and how modern relational database systems overcome the challenges. Learner will also develop the programming skills required to communicate with database systems for accessing, transforming, and persisting the data using Structured Query Language. The module incorporates engagement with contemporary research on data modelling, transaction management, database optimisation, and data governance. Students examine emerging research topics such as scalable database architectures, data consistency in distributed systems, and ethical data management through academic journals and professional publications.

Learning Outcomes

Competences:

At the end of the Module the learner will have acquired the responsibility and autonomy to:

- **Manage and take responsibility for complex database design and implementation activities**, making informed decisions in unpredictable technical and organisational environments.
- **Independently configure, manage, and optimise database systems and client–server architectures**, adapting strategies in response to performance constraints, security risks, and evolving business requirements.
- **Exercise leadership and professional responsibility in data-driven projects**, guiding teams in the application of best practices for SQL programming, data governance, and ethical data management.
- **Integrate interdisciplinary knowledge and professional judgement** to develop innovative and resilient database solutions, particularly where requirements are incomplete, contested, or rapidly changing.

Knowledge:

At the end of the Module the learner will have been exposed to the following:

- **Demonstrate highly specialised and critical understanding of contemporary data management paradigms,** synthesising knowledge of the evolution from traditional storage

systems to advanced relational database management systems (RDBMS) as a foundation for original and informed database design.

- **Critically evaluate the theoretical and architectural principles underpinning RDBMS,** including logical and physical data structures, client–server architectures, and metadata frameworks, with particular attention to scalability, performance, security, and governance in complex organisational contexts.

- **Integrate advanced theoretical knowledge of SQL and relational theory** (DDL, DML, DQL, TCL) to critically assess how database schemas, transactions, and query mechanisms support complex computational, analytical, and business requirements.

- **Critically analyse data modelling approaches** (conceptual, logical, physical, and business models), evaluating their strengths, limitations, and applicability across interdisciplinary contexts, including data-intensive, analytical, and security-sensitive environments.

Skills:

At the end of the Module the learner will have acquired the following skills:

- **Design, implement, and critically evaluate advanced database solutions and computational workflows,** integrating data modelling, SQL programming, and transaction management to address complex or unfamiliar data problems using research-informed judgement.

- **Critically evaluate and optimise database structures and SQL operations**, applying advanced techniques in normalization, indexing, transaction control, and performance tuning in environments characterised by uncertainty, scale, or incomplete information.

- **Apply sophisticated data manipulation and retrieval strategies**, including complex joins, subqueries, aggregations, and metadata interrogation, to extract reliable and actionable insights from large-scale or heterogeneous datasets.

- **Exercise critical judgement in managing database transactions and enforcing data integrity,** balancing technical, security, and ethical considerations in dynamic and interdisciplinary contexts.

- **Communicate complex database designs, analytical outcomes, and technical decisions** clearly and unambiguously to specialist and non-specialist audiences, justifying approaches

through evidence-based reasoning.

- **Demonstrate advanced learning skills by independently identifying emerging database technologies,** SQL standards, data-management methodologies, and governance challenges, critically evaluating their relevance to professional practice, and undertaking self-directed learning to maintain and enhance specialized database competence.

Module-Specific Learner Skills

Upon completion of the module, learners will demonstrate enhanced abilities in

- Proficiency in designing and implementing relational databases.
- Ability to write and execute SQL queries for data manipulation and retrieval.
- Skill in ensuring data quality and integrity through effective data auditing techniques.
- Competence in managing database performance and transactions.
- Proficiency in utilising metadata for database management and optimization.

Module-Specific Digital Skills and Competences

Learners will develop digital skills and competencies including

- Skill in writing Structured Query Language (SQL) queries for database manipulation and management.
- Competence in designing and implementing database schemas to organise and structure data effectively.
- Ability to optimise database performance and ensure data integrity through advanced techniques.
- Proficiency in utilising metadata and data auditing tools for effective database management.

Hours of Total Learning for this Module

- **Total Contact Hours: 30**

  Contact Hours are hours invested 2in learning new content under the Direction of a tutor/lecturer e.g. lectures participation in online forums

- **Supervised Placement and Practice Hours:20**

During these hours the learner is supervised, coached, or mentored.

- **Self-Study Hours: 80**

  Estimated workload of research and study

- **Assessment Hours: 20**

  Examinations/ presentations/ group work/ projects etc.

- **Total Number of ECTS of this Module/Unit: 6 ECTS**

Total Learning Hours of this Module: 150 Hours

Pedagogy for this Module

This module will employ interactive lectures, hands-on workshops, and practical exercises to teach Database & SQL Programming. Through real-world case studies and projects, students will apply theoretical concepts. Online resources and discussion forums will supplement learning, fostering peer collaboration. Continuous feedback and assessments will ensure mastery of key concepts for real-world application in database management and SQL programming. This module includes regular live synchronous sessions, such as supervised practical workshops, tutor-led demonstrations, live problem-solving sessions, and scheduled progress reviews. These activities form part of the module's contact hours and supervised placement and practice (non-WBL) hours and are delivered via video-conferencing tools integrated into the Virtual Learning Environment (VLE).

Assessment method for this particular Module

Assessment Weightings:

- Assignments (40%) (It should not be more than 1250-word count)
- Problem Analysis (30%)
- Final Examination (30%)

Learners must achieve a minimum of 50% overall and 50% in each assessment component; authenticity is verified through Turnitin (similarity and AI-writing indicators), VLE audit trails, and a recorded online viva and/or timed proctored task where appropriate, in accordance with institutional assessment regulations.

Assessment Methods:

Digital learning tools like online submission platforms, code repositories, and video conferencing software will facilitate assessment.

Reading List

- Thomas Connolly & Caroline Begg, Database Systems: A Practical Approach to Design, Implementation, and Management, Pearson, 6th edition, 2021.
- Peter Rob & Carlos Coronel, Database Systems: Design, Implementation, & Management, Cengage Learning, 13th edition, 2021.
- Michael J. Hernandez, Database Design for Mere Mortals: Using Entity-Relationship Diagrams, Addison-Wesley, 3rd edition, 2020.
- Ramez Elmasri & Shamkant B. Navathe, Fundamentals of database systems, Pearson, 7th edition, 2021.
- Alan Beaulieu, Learning SQL, O'Reilly Media, Inc., 3rd edition, 2020.
- Thomas M. Connolly & Carolyn E. Begg, Database systems: a practical approach to design, implementation and management, Pearson, 6th edition, 2015.
- Chris Ruel, Michael Wessler, Oracle 12c For Dummies, John Wiley & Sons Inc, 1st edition, 2013

Suggested Research Oriented reading:

- Eric J. Gruber, SQL Essentials, O'Reilly Media, 2nd edition, 2022.
- Ben Forta, SQL in 10 Minutes, Sams Teach Yourself, Sams Publishing, 5th edition, 2021.
- Bill Karwin, SQL Antipatterns: Avoiding the Pitfalls of Database Programming, Pragmatic Bookshelf, 1st edition, 2017
- Anthony Molinaro, SQL Cookbook, O'Reilly Media, Inc., 1st edition, 2000

MCS703

Computer Architecture

Module Description

This module provides an in-depth understanding of computer hardware and the fundamental principles behind system architecture. Topics include processor design, memory hierarchy, input/output systems, and instruction set architectures. Students will learn how computer systems are structured and how components interact to execute programs efficiently. Practical applications and performance optimization techniques will also be explored. Students engage with current research literature in computer architecture, including advances in multi-core processing, energy-efficient architectures, parallel computing, and hardware–software co-design. Research findings from academic journals and conferences are used to contextualise architectural trade-offs and performance considerations.

Learning Outcomes

Competences:

At the end of the Module the learner will have acquired the responsibility and autonomy to:

- **Manage and take responsibility for complex computer architecture projects**, making informed decisions in unpredictable technical, organisational, or regulatory environments.
- **Exercise leadership and professional accountability in architectural design activities,** supervising and guiding others in the application of advanced architectural principles and best practices.
- **Advise stakeholders on architectural strategies and system selection**, balancing technical performance, cost, operational constraints, and long-term sustainability considerations.
- **Integrate interdisciplinary knowledge and professional judgement** to develop innovative and resilient hardware system solutions, particularly where requirements are evolving, contested, or incomplete.

Knowledge:

At the end of the Module the learner will have been exposed to the following:

- **Demonstrate highly specialised and critical understanding of contemporary computer architecture principles**, synthesising knowledge of processors, memory hierarchies, instruction set architectures, and input/output subsystems as a basis for original architectural analysis and design.
- **Critically evaluate architectural models and execution paradigms**, including pipelined, parallel, and multi-core architectures, assessing their implications for performance, scalability, energy efficiency, and reliability in modern computing systems.
- **Analyse and critique alternative architectural design approaches**, including Von Neumann, Harvard, and hybrid models, identifying their limitations and suitability across diverse and evolving application domains.
- **Integrate advanced theoretical knowledge of hardware–software interaction**, examining how architectural decisions influence operating systems, compilers, and application-level performance in complex computational environments.
- **Demonstrate critical awareness of professional, ethical, and regulatory** considerations in computer architecture design, including sustainability, security, safety, and compliance with industry standards.

Skills:

At the end of the Module the learner will have acquired the following skills:

- **Design, implement, and critically evaluate computer** architecture solutions that meet complex and evolving performance, scalability, and reliability requirements using research-informed judgement.
- **Critically assess and optimise architectural components,** including processor pipelines, memory hierarchies, and interconnects, making defensible design decisions under conditions of uncertainty or incomplete technical information.
- **Apply advanced system-level optimisation strategies,** such as parallelism, load balancing, and resource allocation, to improve overall system efficiency in unfamiliar or high-demand computing contexts.

- **Employ architectural modelling, simulation, and analysis tools** to test, validate, and refine architectural designs, interpreting results to support evidence-based decision-making.

- **Communicate complex architectural designs, trade-offs, and performance analyses** clearly and unambiguously to specialist and non-specialist audiences, justifying recommendations using structured technical reasoning.

- **Demonstrate advanced learning skills by independently identifying emerging architectural trends,** technologies, standards, and research developments, critically evaluating their relevance to professional practice, and undertaking self-directed learning to maintain and enhance specialised architectural competence.

Module-Specific Learner Skills

Upon completion of the module, learners will demonstrate enhanced abilities in

- Analyse complex computer architecture problems and develop innovative solutions by evaluating different processor and memory system designs.
- Apply principles of computer architecture to design, optimise, and implement efficient systems that meet specific performance and resource constraints.
- Communicate technical concepts clearly and effectively in both written and oral formats, including the preparation of detailed reports and presentations on system designs and optimizations.
- Demonstrate proficiency in using simulation tools and hardware components to design, test, and optimise computer systems.
- Work effectively in team-based projects, taking initiative in leadership roles, managing tasks, and guiding peers in the application of computer architecture concepts.

Module-Specific Digital Skills and Competences

Learners will develop digital skills and competencies including

- Use simulation software to design and model processor architectures, memory hierarchies, and I/O systems.
- Apply VHDL or Verilog to design and implement digital circuits and processor components.
- Utilise performance analysis and benchmarking tools to evaluate the efficiency and

performance of computer systems and architecture designs.

- Write low-level code to interact with hardware components and optimise system performance.
- Employ tools and techniques for parallel processing, including multi-core processing and optimization techniques for enhancing the throughput of systems.
- Use design software to construct and simulate digital circuits that contribute to system architecture.
- Integrate computer architecture concepts with operating systems (e.g., Linux kernel programming) to enhance system performance and resource management.
- Utilise software tools to create visual representations of system performance data, helping to analyse bottlenecks and optimise architecture components.

Hours of Total Learning for this Module

- **Total Contact Hours: 30**
  Contact Hours are hours invested in learning new content under the Direction of a tutor/lecturer e.g. lectures participation in online forums
- **Supervised Placement and Practice Hours: 20**
  During these hours the learner is supervised, coached, or mentored.
- **Self-Study Hours: 80**
  Estimated workload of research and study
- **Assessment Hours: 20**
  Examinations/ presentations/ group work/ projects etc.
- **Total Number of ECTS of this Module/Unit: 6 ECTS**

Total Learning Hours of this Module: 150 Hours

Pedagogy for this Module

The Computer Architecture module will be taught through a blend of lectures, hands-on labs, and project-based learning. Lectures will introduce core concepts, while practical sessions will use tools like Model Sim, Xilinx, and MATLAB for simulating and testing architecture designs. Students will apply their knowledge in group projects, developing and optimising computer systems. The module will be supported by online learning tools such as Moodle for assignments and Microsoft Teams for collaboration, ensuring a flexible and interactive learning experience.

Assessment method for this particular Module

Assessment Weightings:

- Written assignments (40%) (It should not be more than 1250-word count)
- Simulation Assessment (30%)
- Final Examination (30%)

Learners must achieve a minimum of 50% overall and 50% in each assessment component; authenticity is verified through Turnitin (similarity and AI-writing indicators), VLE audit trails, and a recorded online viva and/or timed proctored task where appropriate, in accordance with institutional assessment regulations.

Digital learning tools like online submission platforms, code repositories, and video conferencing software will facilitate assessment.

Reading List

- Hennessy, J. L., & Patterson, D. A. (2020). Computer Architecture: A Quantitative Approach (6th ed.). Elsevier.
- Harris, D. M., & Harris, S. L. (2021). Digital Design and Computer Architecture (2nd ed.). Morgan Kaufmann.
- Patterson, D. A., & Hennessy, J. L. (2020). Computer Organization and Design RISC-V Edition: The Hardware Software Interface.

Suggested Research Oriented reading:

- Hwang, K. (2021). Advanced Computer Architecture: A Systems Design Approach. McGraw-Hill.
- Burgess, A., & Brewer, A. (2020). Modern Processor Design: Fundamentals of Superscalar Processors (2nd ed.). Springer.
- Dong, L., & Zhang, Z. (2021). Parallel Computer Architecture: A Hardware/Software Approach. Elsevier.
- Liu, C., & Xu, S. (2021). Low-Power Design for Embedded Multimedia Systems. Springer.

MCS704

Computer Networks

Module Description

The Computer Networks module in the Master of Computer Science (MCS) programme provides an in-depth exploration of network architectures, protocols, and technologies. It covers topics such as data transmission, network topologies, routing algorithms, and security mechanisms. Students will gain practical skills in designing, managing, and securing network infrastructures through hands-on projects and case studies. The module integrates contemporary research on network architectures, protocols, and security, including topics such as software-defined networking, network automation, and resilient network design. Students engage with peer-reviewed research and industry white papers to analyse evolving networking challenges.

Learning Outcomes

Competences:

At the end of the Module the learner will have acquired the responsibility and autonomy to:

- **Manage and take responsibility for complex networking projects,** making informed technical and strategic decisions in unpredictable organisational, regulatory, or technological contexts.
- **Exercise leadership and professional accountability in network design and operations,** supervising teams and guiding the implementation of secure, reliable, and standards-compliant network solutions.
- **Advise stakeholders on strategic network decisions,** balancing performance, security, cost, regulatory obligations, and long-term sustainability considerations.
- **Integrate interdisciplinary knowledge and professional judgement** to develop innovative and resilient network solutions, particularly where requirements are evolving, contested, or risk-sensitive.

Knowledge:

At the end of the Module the learner will have been exposed to the following:

- **Demonstrate highly specialised and critical understanding of contemporary computer networking architectures,** synthesising knowledge of layered network models, distributed systems, and communication paradigms as a basis for advanced

network design and analysis.

- **Critically evaluate networking protocols and standards** across the OSI and TCP/IP models, assessing their implications for scalability, performance, interoperability, and security in complex and evolving networked environments.
- **Analyse and critique data transmission and communication mechanisms** in wired, wireless, and virtualised networks, evaluating architectural trade-offs in reliability, latency, throughput, and resilience.
- **Integrate advanced theoretical knowledge of network security principles,** critically examining threat models, attack surfaces, and defensive strategies within enterprise and large-scale network infrastructures.
- **Demonstrate critical awareness of legal, ethical, and professional responsibilities** associated with network design and operation, including data protection, regulatory compliance, risk management, and sustainability.

Skills:

At the end of the Module the learner will have acquired the following skills:

- **Design, implement, and critically evaluate scalable and secure network infrastructures,** applying research-informed judgement to address complex or unfamiliar networking challenges.
- **Critically assess and optimise routing, switching, and traffic-management strategies,** making defensible decisions under conditions of uncertainty, scale, or incomplete technical information.
- **Diagnose and resolve complex network faults and security incidents**, employing advanced monitoring, analysis, and troubleshooting methodologies in dynamic operational environments.
- **Apply advanced network virtualisation, simulation, and testing techniques** to model, validate, and refine network configurations and security controls prior to deployment.
- **Communicate complex network designs, risk assessments, and operational decisions** clearly and unambiguously to specialist and non-specialist audiences, justifying recommendations through evidence-based technical reasoning.
- **Demonstrate advanced learning skills by independently identifying emerging networking technologies,** standards, architectures, and threat vectors, critically

evaluating their relevance to professional practice, and undertaking self-directed learning to maintain and enhance specialised networking competence.

Module-Specific Learner Skills

Upon completion of the module, learners will demonstrate enhanced abilities in

- Demonstrate proficiency in designing network topologies that balance performance, scalability, and security requirements.
- Apply critical thinking to identify and resolve network connectivity and performance issues efficiently.
- Implement and manage network security measures, including firewalls, intrusion detection systems, and encryption protocols.
- Analyse and optimise the use of routing and switching protocols to enhance network efficiency and reliability.
- Create detailed and accurate network documentation, including configuration guides, security policies, and operational procedures.
- Use advanced configuration management tools and techniques to automate and standardise network setup and maintenance.
- Collaboration and Teamwork: Work collaboratively with cross-functional teams to plan, implement, and monitor network projects in real-world scenarios.

Module-Specific Digital Skills and Competences

Learners will develop digital skills and competencies including

- Demonstrate expertise in configuring routers, switches, and firewalls using command-line interfaces (CLI) and network management software.
- Use virtualization platforms to create and manage virtual networks for testing and deployment purposes.
- Operate and interpret data from network monitoring and analysis tools to ensure optimal network performance and security.
- Apply scripting languages to automate network configuration, monitoring, and management tasks.

- Implement and monitor cybersecurity protocols to detect and mitigate threats, including using penetration testing tools and vulnerability scanners.
- Manage and optimise network connections within cloud platforms (e.g., AWS, Azure) to support cloud-based services.
- Analyse network traffic data to identify trends, performance issues, and potential security breaches.
- Use documentation and diagramming tools (e.g., Microsoft Visio, Lucidchart) to visually represent and document network structures and changes.

Hours of Total Learning for this Module

- **Total Contact Hours: 30**

  Contact Hours are hours invested in learning new content under the Direction of a tutor/lecturer e.g. lectures participation in online forums

- **Supervised Placement and Practice Hours: 20**

  During these hours the learner is supervised, coached, or mentored.

- **Self-Study Hours: 80**

  Estimated workload of research and study

- **Assessment Hours: 20**

  Examinations/ presentations/ group work/ projects etc.

- **Total Number of ECTS of this Module/Unit: 6 ECTS**

Total Learning Hours of this Module: 150 Hours

Pedagogy for this Module

The Computer Networks module will be taught through a combination of lectures, lab-based practical sessions, and digital tools to provide both theoretical knowledge and hands-on experience. Students will engage with network simulation software like Cisco Packet Tracer and GNS3 to practise network configuration in a controlled, virtual environment. The use of an LMS (e.g., Moodle) will facilitate access to course materials, assignments, and discussions, while video conferencing tools such as Zoom will support virtual lectures and interactive sessions. Practical

learning will be reinforced with cybersecurity exercises using Wireshark and Kali Linux to build real-world skills in network monitoring and security practices. This module includes regular live synchronous sessions, such as supervised practical workshops, tutor-led demonstrations, live problem-solving sessions, and scheduled progress reviews. These activities form part of the module's contact hours and supervised placement and practice (non-WBL) hours and are delivered via video-conferencing tools integrated into the Virtual Learning Environment (VLE).

Assessment method for this particular Module Assessment Weightings:

- Written assignments (40%) (It should not be more than 1250-word count)
- Case Analysis (30%)
- Final Examination (30%)

Learners must achieve a minimum of 50% overall and 50% in each assessment component; authenticity is verified through Turnitin (similarity and AI-writing indicators), VLE audit trails, and a recorded online viva and/or timed proctored task where appropriate, in accordance with institutional assessment regulations.

Digital learning tools like online submission platforms, code repositories, and video conferencing software will facilitate assessment.

Reading List

- Kurose, J., & Ross, K. (2021). Computer Networking: A Top-Down Approach (8th ed.). Pearson.
- Edelman, J., Lowe, S., & Oswalt, M. (2022). Network Programmability and Automation: Next-Generation Routing, Control, and Services (2nd ed.). Pearson.
- Ratan, A. (2021). Practical Network Automation. Packt Publishing.
- Lucas, M. W. (2022). Networking for Systems Administrators. No Starch Press

Suggested Research Oriented reading:

- Forouzan, B. A. (2021). Data Communications and Networking (6th ed.). McGraw-Hill Education.
- Comer, D. E. (2021). Internetworking with TCP/IP Volume One: Principles, Protocols, and Architecture (7th ed.). Pearson.
- Schulzrinne, H., & Rao, S. (2021). Voice over IP (VoIP): A Practical Guide to the VoIP Revolution. Springer.

- Tanenbaum, A. S., & Wetherall, D. J. (2022). Computer Networks (6th ed.). Pearson.
- Lammle, T. (2022). CCNA 200-301 Official Cert Guide, Volume 2. Cisco Press.

MCS705

Advanced Computing Research Methods

Module Description

The aim of this module is to develop learners' ability to prepare for various types of academically based computing research through the development and design of a research proposal. Learners will develop a critical understanding of the philosophical, practical, and ethical concepts of research within the context of computing discipline. This module is explicitly research-focused and requires sustained engagement with contemporary computing research literature. Students analyse peer-reviewed journal articles and conference papers to develop research questions, methodological approaches, and ethically grounded research designs.

Learning Outcomes

Competences:

At the end of the Module the learner will have acquired the responsibility and autonomy to:

- **Manage and take responsibility for complex research activities and projects** in computing, making informed methodological and strategic decisions in unpredictable academic, professional, or organisational contexts.
- **Exercise leadership and professional accountability in research environments,** guiding others in the application of sound research practices, ethical decision-making, and quality standards.
- **Create research-based diagnoses of complex computing problems,** integrating interdisciplinary knowledge and making judgements where information is incomplete, contested, or evolving.
- **Contribute responsibly to professional and scholarly knowledge,** recognising personal, social, and ethical responsibilities associated with original research and its impact within wider academic and societal contexts.

Knowledge:

At the end of the Module the learner will have been exposed to the following:

- **Demonstrate highly specialised and critical understanding of advanced research paradigms in computing**, synthesising contemporary theoretical frameworks to conceptualise, frame, and justify complex research problems within evolving knowledge

contexts.

- **Critically evaluate quantitative, qualitative, and mixed-methods research methodologies** used in computing research, assessing their epistemological foundations, strengths, limitations, and suitability for addressing complex or novel research questions.
- **Analyse and critique principles of research design, validity, reliability, and rigour,** evaluating how methodological choices influence the credibility, generalisability, and impact of research outcomes.
- **Integrate interdisciplinary knowledge** from computing and related fields to inform research problem formulation, methodological selection, and interpretation of findings at the interface of multiple domains.
- **Demonstrate critical awareness of ethical, professional, and societal considerations** in computing research, including research integrity, responsible data use, governance, and the ethical implications of knowledge production.

Skills:

At the end of the Module the learner will have acquired the following skills:

- **Design, implement, and critically evaluate research projects in computing,** integrating appropriate methodologies, data collection strategies, and analytical techniques to address complex or unfamiliar problems using research-informed judgement.
- **Apply advanced data collection and analysis techniques,** critically assessing data sufficiency, reliability, validity, and limitations when working with primary and secondary sources under conditions of uncertainty or incomplete information.
- **Conduct systematic and critical literature reviews**, evaluating the credibility, relevance, and scholarly contribution of sources and synthesising findings to inform research direction and originality.
- **Develop and apply rigorous project-planning and research-management techniques**, including timelines, milestones, and resource allocation, to support effective execution of complex research initiatives.
- **Communicate research designs, findings, and recommendations** clearly and unambiguously to specialist and non-specialist audiences through well-structured reports and presentations, adhering to recognised academic conventions and ethical referencing

standards.

- **Demonstrate advanced learning skills by critically reflecting on learning processes,** independently identifying gaps in research knowledge or capability, and undertaking self-directed learning to acquire new research methods, analytical techniques, and scholarly competencies in response to emerging knowledge and practices.

Module-Specific Learner Skills

Upon completion of the module, learners will demonstrate enhanced abilities in

- Advanced research design proficiency integrating qualitative and quantitative approaches.
- Enhanced critical analysis and evaluation of research methodologies and theoretical frameworks.
- Proficiency in project management, including setting SMART objectives and managing timelines.
- Advanced data collection, analysis, and interpretation skills in computing research.
- Improved communication skills for presenting research findings effectively in written and oral formats.

Module-Specific Digital Skills and Competences

Learners will develop digital skills and competencies including

- Proficiency in advanced data analysis using software like SPSS or Python.
- Skill in creating compelling data visualisations with tools like Tableau.
- Familiarity with specialised research software.
- Ability to leverage online resources for research purposes effectively.

Hours of Total Learning for this Module

- **Total Contact Hours: 30**

  Contact Hours are hours invested in learning new content under the Direction of a tutor/lecturer e.g. lectures participation in online forums

- **Supervised Placement and Practice Hours: 20**

  During these hours the learner is supervised, coached, or mentored.

- **Self-Study Hours: 80**

Estimated workload of research and study

- **Assessment Hours: 20**

  Examinations/ presentations/ group work/ projects etc.

- **Total Number of ECTS of this Module/Unit: 6 ECTS**

Total Learning Hours of this Module: 150 Hours

Pedagogy for this Module

The Advanced Computing Research Methods module will involve a multifaceted approach. Theoretical lectures will elucidate fundamental concepts and methodologies, providing learners with a strong theoretical foundation. Practical workshops will complement theoretical learning, offering hands-on experience with research tools and techniques. Interactive discussions and case studies will encourage critical thinking and application of concepts to real-world scenarios, fostering a deeper understanding of research methodologies in computing. Additionally, guest lectures from industry experts may provide insights into current trends and applications in computing research. Overall, the teaching methodology aims to equip learners with the necessary skills and knowledge to undertake advanced research projects effectively in the field of computing.

Assessment method for this particular Module

Assessment Weightings:

- Written assignments (40%) (It should not be more than 1250-word count)
- Critical Literature Review (30%)
- Final Examination (30%)

Learners must achieve a minimum of 50% overall and 50% in each assessment component; authenticity is verified through Turnitin (similarity and AI-writing indicators), VLE audit trails, and a recorded online viva and/or timed proctored task where appropriate, in accordance with institutional assessment regulations.

Digital learning tools like online submission platforms, code repositories, and video conferencing software will facilitate assessment.

Reading List

- Moore, Creswell, J. W. (2022). Research Design: Qualitative, Quantitative, and Mixed Methods Approaches. Sage Publications.
- Robson, C., & McCartan, K. (2022). Real World Research. Wiley.
- Flick, U. (2022). An Introduction to Qualitative Research. Sage Publications.

Suggested Research Oriented reading:

- Field, A. (2023). Discovering Statistics Using SPSS. Sage Publications.
- Silverman, D. (2023). Doing Qualitative Research. Sage Publications.

MCS706

Data Science Foundations

Module Description

Data science combines powerful computing technology, sophisticated statistical methods, and expert domain knowledge to analyse and gain practical insights from huge amounts of data produced by organisations in the present business environment. The aim of this module is to introduce a range of data science concepts, data administration and governance and big data sources. The module introduces learners to contemporary research in data science, including data governance, scalable analytics, and ethical data use. Students engage with peer-reviewed research on data-driven decision-making and emerging analytical techniques relevant to organisational and societal contexts.

Learning Outcomes

Competences:

At the end of the Module the learner will have acquired the responsibility and autonomy to:

- **Manage and take responsibility for complex data science activities and projects**, making informed analytical and methodological decisions in unpredictable technical, organisational, or business environments.
- **Integrate interdisciplinary knowledge and professional judgement** to develop innovative, scalable, and ethically responsible data-driven solutions where requirements or data constraints are evolving or contested.
- **Exercise leadership and professional accountability in data-driven initiatives,** guiding teams in the application of best practices in analytics, modelling, and ethical data use.
- **Apply cloud-based and scalable data technologies strategically,** adapting analytical solutions in response to rapidly changing technological and organisational contexts.

Knowledge:

At the end of the Module the learner will have been exposed to the following:

- **Demonstrate highly specialised and critical understanding of data science principles,** synthesising advanced knowledge of statistics, machine learning, data

analytics, and computational methods as a basis for original data-driven inquiry.

- **Critically evaluate machine learning models and analytical approaches**, assessing their assumptions, limitations, and suitability for predictive analysis, segmentation, and decision-making across diverse application domains.
- **Analyse and critique big data paradigms,** including volume, velocity, and variety, evaluating their implications for analytical strategy, system design, and organisational decision-making in contemporary data-intensive environments.
- **Integrate advanced theoretical knowledge of data analytics tools and platforms**, critically assessing their capabilities, constraints, and appropriateness for complex analytical challenges and interdisciplinary problem contexts.
- **Demonstrate critical awareness of ethical, legal, and societal considerations in data** science, including data protection, privacy, consent, bias, and responsible data governance, and evaluate their impact on analytical practice.

Skills:

At the end of the Module the learner will have acquired the following skills:

- **Design, implement, and critically evaluate data-driven analytical workflows,** integrating statistical analysis, machine learning techniques, and programming approaches to address complex or unfamiliar problems using research-informed judgement.
- **Apply advanced analytical and statistical techniques** to large or complex datasets, critically interpreting results to generate reliable, evidence-based insights under conditions of uncertainty or incomplete information.
- **Develop and evaluate predictive and exploratory models**, exercising critical judgement in model selection, validation, and performance assessment across dynamic or interdisciplinary contexts.
- **Create and communicate advanced data visualisations and analytical narratives,** translating complex findings into clear, persuasive insights for both specialist and non-specialist audiences.
- **Communicate analytical decisions, assumptions, and outcomes** clearly and unambiguously through reports, dashboards, and presentations, justifying conclusions using structured, evidence-based reasoning.

- **Demonstrate advanced learning skills by independently identifying emerging data-science methodologies,** tools, and ethical challenges, critically evaluating their relevance to professional practice, and undertaking self-directed learning to maintain and enhance specialised analytical competence.

Module-Specific Learner Skills

Upon completion of the module, learners will demonstrate enhanced abilities in

- Advanced data manipulation and preprocessing skills.
- Proficiency in advanced statistical analysis and modelling techniques.
- Ability to create sophisticated data visualisations for effective communication.
- Proficiency in advanced programming languages and frameworks for implementing machine learning algorithms.

Module-Specific Digital Skills and Competences

Learners will develop digital skills and competencies including

- Learners will gain expertise in data engineering techniques, including data integration, transformation, and pipeline automation using advanced tools
- Learners will develop skills in deploying and managing data science workflows on cloud platforms.
- Learners will understand and apply DevOps practices such as continuous integration, continuous delivery (CI/CD), and infrastructure as code (IaC) to streamline the development, testing, and deployment of data science solutions.

Hours of Total Learning for this Module

- **Total Contact Hours: 30**

  Contact Hours are hours invested in learning new content under the Direction of a tutor/lecturer e.g. lectures participation in online forums

- **Supervised Placement and Practice Hours: 20**

  During these hours the learner is supervised, coached, or mentored.

- **Self-Study Hours: 80**

Estimated workload of research and study

- **Assessment Hours: 20**

  Examinations/ presentations/ group work/ projects etc.

- **Total Number of ECTS of this Module/Unit: 6 ECTS**

Total Learning Hours of this Module: 150 Hours

Pedagogy for this Module

The Data Science Foundations module will employ a multifaceted approach to teaching, including lectures, hands-on workshops, case studies, group projects, and guest lectures. Lectures will cover essential theoretical concepts in data science, while hands-on workshops will provide practical experience with coding and data analysis tools. Case studies and group projects will allow learners to apply their knowledge to real-world scenarios, promoting collaboration and problem-solving skills. Guest lectures by industry experts will offer insights into current trends and best practices. This comprehensive approach aims to provide learners with a solid foundation in data science principles and practical skills for their future endeavours.

Assessment method for this particular Module

Assessment Weightings:

- Written assignments (40%) (It should not be more than 1250-word count)
- Virtual Lab Exercise (30%)
- Final Examination (30%)

Learners must achieve a minimum of 50% overall and 50% in each assessment component; authenticity is verified through Turnitin (similarity and AI-writing indicators), VLE audit trails, and a recorded online viva and/or timed proctored task where appropriate, in accordance with institutional assessment regulations.

Digital learning tools like online submission platforms, code repositories, and video conferencing software will facilitate assessment.

Reading List

- Miller, A. J., & Harrison, P. (2021). Data Science for Business: How to Use Data for

Business Success. O'Reilly Media.

- Shmueli, G., & Koppius, O. (2021). An Introduction to Data Science: A Modeling Approach. Wiley.
- García, J., & Díaz, J. (2022). Practical Data Science: A Guide to Building Data-Driven Applications. Springer.
- Kotu, V, & Deshpande, B. (2019). Data Science: Concepts and Practice. Morgan Kaufmann Publishers, an imprint of Elsevier.
- Python for data analysis (2007) William Wes- ley McKinney

Suggested Research Oriented reading:

- Chakraborty, A., & Dey, A. (2023). Data Analytics for Decision Making: A Practical Guide for Managers. Business Expert Press.
- Marmol, F. J. (2022). Data Science with Python and Dask: A Comprehensive Guide for Data Professionals. Packt Publishing.

MCS707

Data Mining, Machine Learning and Artificial Intelligence

Module Description

This module is designed to introduce the science behind machine intelligence and the philosophical debate around the ambitions of simulating human intelligence to solve real-world problems. Students will be guided to appreciate AI types and applications and develop a better understanding of aspects related to intelligent agents. In this module students will master key concepts and gain the practical knowledge to apply machine learning principles to challenging real-world problems. Students engage with contemporary research topics including explainable artificial intelligence, ethical machine learning, model interpretability, and large-scale data analytics. The module draws on peer-reviewed journal articles and conference proceedings to contextualise theoretical and applied developments in AI and machine learning.

Learning Outcomes

Competences:

At the end of the Module the learner will have acquired the responsibility and autonomy to:

- **Manage and take responsibility for complex AI and data-driven initiatives,** making informed technical, ethical, and strategic decisions in unpredictable technological and organisational environments.
- **Exercise leadership and professional accountability in AI-related projects**, guiding teams in the responsible design, evaluation, and deployment of intelligent systems.
- **Integrate interdisciplinary knowledge and professional judgement** to develop innovative and ethically responsible AI solutions, particularly where requirements, data availability, or societal implications are contested or evolving.
- **Critically assess and address ethical, environmental, and societal challenges** associated with AI technologies, balancing innovation with responsibility, regulation, and public trust.

Knowledge:

At the end of the Module the learner will have been exposed to the following:

- **Demonstrate highly specialised and critical understanding of artificial intelligence paradigms**, synthesising theoretical foundations of artificial intelligence, machine learning,

and deep learning as a basis for original analysis and informed application.

- **Critically evaluate the interdisciplinary foundations of AI,** integrating knowledge from computer science, mathematics, statistics, psychology, linguistics, and engineering to assess how these disciplines shape intelligent systems and their capabilities.
- **Analyse and critique core AI problem domains,** including reasoning, learning, planning, perception, and natural language processing, assessing their theoretical limitations, unresolved challenges, and implications for real-world deployment.
- **Critically examine classifications of intelligence** (Artificial Narrow Intelligence, Artificial General Intelligence, Artificial Superintelligence), evaluating their technical feasibility, societal impact, and ethical consequences in contemporary and future contexts.
- **Demonstrate critical awareness of ethical, environmental, and societal considerations** associated with AI and data-driven systems, including bias, transparency, sustainability, accountability, and socio-economic impact.

Skills:

At the end of the Module the learner will have acquired the following skills:

- **Design, implement, and critically evaluate data-driven and AI-based analytical workflows,** integrating data mining techniques, machine learning algorithms, and evaluation methodologies to address complex or unfamiliar problems using research-informed judgement.
- **Critically select, apply, and assess machine learning and data mining techniques,** evaluating model performance, assumptions, limitations, and suitability across diverse application contexts and datasets.
- **Apply advanced data acquisition, preprocessing, and validation techniques, critically** assessing data quality, reliability, and bias to support robust and trustworthy AI-based solutions.
- **Conduct rigorous testing, validation, and evaluation of AI-enabled systems,** employing appropriate tools, metrics, and documentation practices to ensure reliability, compliance, and ethical integrity.
- **Communicate complex AI concepts, system designs, and analytical outcomes** clearly and unambiguously to specialist and non-specialist audiences, justifying conclusions through structured, evidence-based reasoning.

- **Demonstrate advanced learning skills by independently identifying emerging AI methodologies,** data-mining techniques, tools, risks, and regulatory developments, critically evaluating their relevance to professional practice, and undertaking self-directed learning to maintain and enhance specialised competence.

Module-Specific Learner Skills

Upon completion of the module, learners will demonstrate enhanced abilities in

- Learners will demonstrate refined abilities in interpreting complex datasets, identifying patterns, and extracting meaningful insights using sophisticated data mining, machine learning, and artificial intelligence techniques.
- Learners will exhibit mastery in implementing and fine-tuning algorithms, leveraging advanced statistical methods and machine learning models to derive actionable insights from data.
- Learners will showcase innovative problem-solving skills, applying creative approaches and leveraging cutting-edge AI techniques to address complex challenges in diverse domains.

Module-Specific Digital Skills and Competences

Learners will develop digital skills and competencies including

- Proficiency in advanced AI tools like TensorFlow and Azure Machine Learning.
- Expertise in deep learning techniques such as CNNs and RNNs.
- Skills in big data analytics with platforms like Apache Spark.
- Understanding of ethical considerations in AI development.
- Ability to interpret and explain AI model decisions effectively.

Hours of Total Learning for this Module

- **Total Contact Hours: 30**

  Contact Hours are hours invested in learning new content under the Direction of a tutor/lecturer e.g. lectures participation in online forums

- **Supervised Placement and Practice Hours: 20**

  During these hours the learner is supervised, coached, or mentored.

- **Self-Study Hours: 80**

  Estimated workload of research and study

- **Assessment Hours: 20**

  Examinations/ presentations/ group work/ projects etc.

- **Total Number of ECTS of this Module/Unit: 6 ECTS**

Total Learning Hours of this Module: 150 Hours

Pedagogy for this Module

The "Data Mining, Machine Learning, and Artificial Intelligence" module, teaching will integrate theoretical concepts with practical applications. Lectures will elucidate fundamental principles, while hands-on workshops will allow learners to implement algorithms and techniques using relevant tools. Guest speakers from industry will provide insights into real-world applications. Collaborative projects and case studies will foster problem-solving skills, while discussions will encourage critical thinking and exploration of AI advancements.

Assessment Weightings:

- Written assignments (40%) (It should not be more than 1250-word count)
- Programming/ Mini Project (30%)
- Final Examination (30%)

Learners must achieve a minimum of 50% overall and 50% in each assessment component authenticity is verified through Turnitin (similarity and AI-writing indicators), VLE audit trails, and a recorded online viva and/or timed proctored task where appropriate, in accordance with institutional assessment regulations.

Assessment tasks will leverage digital learning tools such as online submission platforms, video conferencing for presentations, and collaborative document editing tools.

Reading List

- Russell, S., & Norvig, P. (2021). Artificial Intelligence: A Modern Approach (4th ed.). Pearson.

- Goodfellow, I., Bengio, Y., & Courville, A. (2020). Deep Learning. MIT Press.
- Murphy, K. P. (2022). Machine Learning: A Probabilistic Perspective. MIT Press.
- Deisenroth, M. P., Faisal, A. A., & Ong, C. S. (2020). Mathematics for Machine Learning. Cambridge University Press.
- Russell, S. J., & Norvig, P. (2022). Artificial Intelligence: A modern approach. Pearson.

Suggested Research Oriented reading:

- Chollet, F. (2021). Deep Learning with Python (2nd ed.). Manning Publications.
- O'Reilly, T. (2021). AI Ethics: A Guide for the Responsible Use of Artificial Intelligence. O'Reilly Media.
- Introduction to Data Mining (2005) by Pang-Ning Tan, Michael Steinbach, and Vipin Kumar
- Pattern Recognition and Machine Learning (2006) by Christopher M. Bishop
- Artificial Intelligence: A Modern Approach (2009) by Stuart Russell and Peter Norvig.

MCS708

Data Analysis and Visualisation

Module Description

The Data Analysis and Visualization module equips students with the skills to analyse complex data sets and present insights in a clear and compelling visual format. The course covers various data analysis techniques, including descriptive and inferential statistics, as well as data cleaning and transformation methods. Students will learn to use software tools such as Excel, Python (with libraries like Pandas, NumPy, and Matplotlib), and Tableau to manipulate, analyse, and visualise data effectively. By the end of the module, students will be able to identify patterns, trends, and anomalies in data, and communicate their findings through impactful visual representations, supporting decision-making processes in business and research contexts. The module integrates engagement with current research on data interpretation, visual analytics, and evidence-based communication. Emerging research topics such as visual bias, transparency in data storytelling, and interactive visualisation are explored through academic literature and professional research.

Learning Outcomes

Competences:

At the end of the Module the learner will have acquired the responsibility and autonomy to:

- **Manage and take responsibility for complex data analysis and visualisation** projects, making informed methodological and communicative decisions in unpredictable organisational or business contexts.
- **Exercise leadership and professional accountability in analytical teams,** guiding others in the application of best practices in data preparation, analysis, and visual communication.
- **Advise stakeholders on strategic data-driven decisions**, balancing analytical rigor, clarity of communication, ethical considerations, and organisational objectives.
- **Integrate interdisciplinary knowledge and professional judgement** to develop innovative, transparent, and responsible analytical solutions where data requirements or stakeholder expectations are evolving or contested.

Knowledge:

At the end of the Module the learner will have been exposed to the following:

- **Demonstrate highly specialised and critical understanding of data analysis and visualisation principles**, synthesising statistical theory, data transformation methods, and visual communication models as a basis for original analytical insight.
- **Critically evaluate analytical and statistical techniques** used in data exploration, modelling, and interpretation, assessing their assumptions, limitations, and appropriateness in complex or uncertain analytical contexts.
- **Analyse and critique visualisation paradigms and design frameworks**, evaluating how visual choices influence interpretation, bias, transparency, and decision-making in data-driven environments.
- **Integrate advanced theoretical knowledge of analytical tools and platforms** (e.g. programming-based and visual analytics environments), critically assessing their capabilities and constraints for large-scale or interdisciplinary data analysis.
- **Demonstrate critical awareness of ethical, professional, and societal considerations** in data analysis and visualisation, including data integrity, misrepresentation, accessibility, and responsible communication of insights.

Skills:

At the end of the Module the learner will have acquired the following skills:

- **Design, implement, and critically evaluate end-to-end data analysis workflows**, integrating data preparation, statistical analysis, and visualisation to address complex or unfamiliar problems using research-informed judgement.
- **Apply advanced data cleaning, transformation, and validation techniques,** critically assessing data quality, reliability, and bias prior to analysis and interpretation.
- **Develop and evaluate advanced statistical analyses**, interpreting results critically to generate robust, evidence-based insights under conditions of uncertainty or incomplete information.
- **Create and critically assess advanced data visualisations**, selecting and adapting visual techniques to communicate complex patterns, trends, and relationships effectively to diverse audiences.
- **Communicate analytical findings, assumptions, and limitations** clearly and

unambiguously through reports, dashboards, and presentations, justifying conclusions using structured, evidence-based reasoning.

- **Demonstrate advanced learning skills by independently identifying emerging data-analysis methods**, visualisation techniques, standards, and ethical challenges, critically evaluating their relevance to professional practice, and undertaking self-directed learning to maintain and enhance specialised analytical competence.

Module-Specific Learner Skills

Upon completion of the module, learners will demonstrate enhanced abilities in

- Ability to preprocess raw data, handle missing values, and format data for analysis using Python and Excel.
- Skill in applying descriptive and inferential statistical methods to interpret and analyse datasets.
- Proficiency in creating various types of visualisations (e.g., bar charts, scatter plots, heat maps) to present data insights effectively using tools like Matplotlib, Seaborn, and Tableau.
- Ability to identify key patterns, trends, and anomalies in datasets and apply appropriate techniques to solve data-related problems.
- Skill in writing clear and actionable reports that combine statistical analysis and visualisations to communicate findings to diverse audiences.
- Competence in using software and programming tools (e.g., Python, Excel, Tableau) for data analysis and visualisation tasks

Module-Specific Digital Skills and Competences

Learners will develop digital skills and competencies including

- Proficiency in using Python (with libraries like Pandas, NumPy, and Matplotlib) for data analysis, manipulation, and visualisation.
- Competence in using Excel for performing basic statistical analysis, data aggregation, and visualisation.
- Ability to design and create dynamic visualisations using Tableau to present complex data insights clearly and interactively.
- Skill in writing Python scripts to automate data cleaning, transformation, and analysis workflows.

- Ability to create interactive dashboards in Tableau or Power BI, enabling real-time data exploration and decision-making.
- Proficiency in querying and extracting data from databases using SQL, and integrating it with analysis tools for further processing and visualisation.

Hours of Total Learning for this Module

- **Total Contact Hours: 30**

  Contact Hours are hours invested in learning new content under the Direction of a tutor/lecturer e.g. lectures participation in online forums

- **Supervised Placement and Practice Hours: 20**

  During these hours the learner is supervised, coached, or mentored.

- **Self-Study Hours: 80**

  Estimated workload of research and study

- **Assessment Hours: 20**

  Examinations/ presentations/ group work/ projects etc.

- **Total Number of ECTS of this Module/Unit: 6 ECTS**

Total Learning Hours of this Module: 150 Hours

Pedagogy for this Module

The Data Analysis and Visualization module will be taught through a mix of lectures, practical labs, and project-based learning. Students will use Python (Pandas, NumPy, Matplotlib), Excel, and Tableau to clean, analyse, and visualise data. Practical sessions will allow students to apply theoretical concepts to real datasets, while projects will help them communicate insights through visualisations and reports. Digital learning tools, including Jupyter Notebooks and Google Colab, will support collaborative learning and hands-on practice.

Assessment Weightings:

- Written assignments (40%) (It should not be more than 1250-word count)
- Critical Literature Review (30%)
- Final Examination (30%)

Learners must achieve a minimum of 50% overall and 50% in each assessment component; authenticity is verified through Turnitin (similarity and AI-writing indicators), VLE audit trails, and a recorded online viva and/or timed proctored task where appropriate, in accordance with institutional assessment regulations.

Digital learning tools like online submission platforms, code repositories, and video conferencing software will facilitate assessment.

Reading List

- Python for Data Analysis" by Wes McKinney (2021) Publisher: O'Reilly Media
- Data Visualization: A Practical Introduction" by Kieran Healy (2020) Publisher: Princeton University Press
- "Storytelling with Data: A Data Visualization Guide for Business Professionals" by Cole Nussbaumer Knaflic (2020) Publisher: Wiley
- "Tableau Your Data! Fast and Easy Visual Analysis with Tableau Software" by Dan Murray (2021) Publisher: Wiley
- "The Art of Data Science" by Roger D. Peng and Elizabeth Matsui (2020) Publisher: Lean pub.

Suggested Research Oriented reading:

- "Data Science for Business: What You Need to Know about Data Mining and Data-Analytic Thinking" by Foster Provost and Tom Fawcett (2021) Publisher: O'Reilly Media
- "Practical Statistics for Data Scientists: 50 Essential Concepts" by Peter Bruce and Andrew Bruce (2020) Publisher: O'Reilly Media
- "Data Wrangling with Python" by Jacqueline Kazil and Katharine Jarmul (2021) Publisher: O'Reilly Media
- "Visualising Data: Exploring and Explaining Data with the Processing Environment" by Ben Fry (2020) Publisher: O'Reilly Media

- "Data Visualization with Python and JavaScript" by Kyran Dale (2020) Publisher: O'Reilly Media
- "The Big Book of Dashboards: Visualising Your Data Using Real-World Business Scenarios" by Steve Wexler, Jeffrey Shaffer, and Andy Cotgreave (2020) Publisher: Wiley.

MCS709

Probability and Statistics for Data Analysis

Module Description

The Probability and Statistics for Data Analysis module provides students with foundational knowledge in probability theory and statistical methods, focusing on their application in data analysis. Topics include probability distributions, hypothesis testing, regression analysis, and statistical inference techniques. The module emphasises the practical use of statistical tools to analyse and interpret data, helping students develop the skills necessary for making data-driven decisions. Real-world case studies and hands-on exercises using software such as R or Python will be incorporated to enhance students' ability to perform statistical analysis and draw meaningful conclusions from data. Students engage with contemporary research in statistical modelling, uncertainty quantification, and data-driven inference. The module draws on peer-reviewed studies to examine the application of statistical reasoning in complex and uncertain analytical environments.

Learning Outcomes

Competences:

At the end of the Module the learner will have acquired the responsibility and autonomy to:

- **Manage and take responsibility for complex statistical analysis activities and projects,** making informed methodological decisions in unpredictable research, organisational, or business contexts.
- **Exercise leadership and professional accountability in statistical practice,** guiding others in the correct application, interpretation, and communication of probabilistic and statistical methods.
- **Advise stakeholders on data-driven decisions**, balancing statistical rigour, uncertainty, ethical considerations, and practical constraints.
- **Integrate interdisciplinary knowledge and professional judgement** to develop robust, transparent, and context-appropriate statistical models where data quality or research conditions are evolving or contested.

Knowledge:

At the end of the Module the learner will have been exposed to the following:

- **Demonstrate highly specialised and critical understanding of probability theory and statistical inference,** synthesising concepts such as probability distributions, random variables, and conditional probability as a foundation for advanced data-driven analysis.
- **Critically evaluate statistical models and inferential techniques,** including hypothesis testing, regression analysis, and predictive modelling, assessing their assumptions, limitations, and appropriateness for complex or uncertain analytical contexts.
- **Analyse and critique the theoretical underpinnings of statistical estimation and modelling**, examining issues of bias, variance, uncertainty, and robustness in real-world data analysis scenarios.
- **Integrate advanced theoretical knowledge of statistical reasoning with data-analytic practice,** assessing how methodological choices influence interpretation, validity, and decision-making outcomes.
- **Demonstrate critical awareness of ethical, professional, and societal considerations** in statistical analysis, including data integrity, misuse of statistics, transparency, and responsible interpretation of results.

Skills:

At the end of the Module the learner will have acquired the following skills:

- **Design, implement, and critically evaluate statistical analysis workflows,** integrating probability models, inferential techniques, and computational tools to address complex or unfamiliar data problems using research-informed judgement.
- **Apply advanced statistical and probabilistic methods** to real-world datasets, critically interpreting results and quantifying uncertainty under conditions of incomplete, noisy, or biased data.
- **Develop, validate, and assess predictive and inferential models**, exercising critical judgement in model selection, assumption testing, and performance evaluation across dynamic analytical contexts.
- **Design statistically sound experiments and data-collection strategies**, ensuring methodological rigour, reproducibility, and alignment with research or organisational

objectives.

- **Communicate statistical findings, assumptions, and limitations** clearly and unambiguously to specialist and non-specialist audiences, using appropriate visualisations, reports, and narrative explanations.
- **Demonstrate advanced learning skills by independently identifying emerging statistical methodologies**, analytical tools, and ethical challenges, critically evaluating their relevance to professional practice, and undertaking self-directed learning to maintain and enhance specialised competence.

Module-Specific Learner Skills

Upon completion of the module, learners will demonstrate enhanced abilities in

- Ability to interpret and analyse data using statistical methods, drawing conclusions and making data-driven decisions.
- Skill in using software tools like R or Python for performing data analysis and visualising results.
- Ability to construct, validate, and interpret various statistical models, such as regression analysis and hypothesis testing.
- Develop critical thinking skills to solve complex data analysis problems, applying the appropriate statistical techniques.
- Skill in presenting statistical findings clearly and effectively through reports and visualisations, making complex concepts accessible to both technical and non-technical audiences.
- Competence in preparing and cleaning raw data for analysis, ensuring data quality and reliability before applying statistical methods.

Module-Specific Digital Skills and Competences

Learners will develop digital skills and competencies including

- Competence in using statistical software such as R, Python, or SPSS for data manipulation, analysis, and visualisation.
- Ability to use tools like Matplotlib, Seaborn, or ggplot2 to create meaningful visualisations (e.g., histograms, scatter plots, box plots) that convey statistical insights.

- Skill in writing and debugging scripts in Python or R to perform statistical analysis, including data cleaning, transformation, and modelling.
- Ability to handle large datasets, perform data wrangling tasks, and use databases (e.g., SQL) to extract and manage data for analysis.
- Competence in interpreting the results of statistical tests and models using digital tools, ensuring accurate insights and recommendations.
- Proficiency in using digital collaboration tools (e.g., Google Sheets, Jupyter Notebooks, RStudio Cloud) for teamwork, sharing results, and conducting collaborative data analysis projects.

Hours of Total Learning for this Module

- **Total Contact Hours: 30**

  Contact Hours are hours invested in learning new content under the Direction of a tutor/lecturer e.g. lectures participation in online forums

- **Supervised Placement and Practice Hours: 20**

  During these hours the learner is supervised, coached, or mentored.

- **Self-Study Hours: 80**

  Estimated workload of research and study

- **Assessment Hours: 20**

  Examinations/ presentations/ group work/ projects etc.

- **Total Number of ECTS of this Module/Unit: 6 ECTS**

Total Learning Hours of this Module: 150 Hours

Pedagogy for this Module

The Probability and Statistics for Data Analysis module will be taught through a combination of lectures, hands-on lab sessions, and case studies, emphasising both theoretical concepts and practical application. Students will learn to use statistical software such as R and Python for data analysis, applying these tools to real-world datasets. Interactive online platforms like Jupyter Notebooks will be used for coding exercises and data visualisation tasks. In addition, digital

resources such as online tutorials, video lectures, and peer collaboration tools will support student learning and engagement. The course will also include quizzes and assignments to assess understanding and application of statistical techniques.

Assessment Weightings:

- Written assignments (40%) (It should not be more than 1250-word count)
- Critical Literature Review (30%)
- Final Examination (30%)

Learners must achieve a minimum of 50% overall and 50% in each assessment component; authenticity is verified through Turnitin (similarity and AI-writing indicators), VLE audit trails, and a recorded online viva and/or timed proctored task where appropriate, in accordance with institutional assessment regulations.

Digital learning tools like online submission platforms, code repositories, and video conferencing software will facilitate assessment.

Reading List

- James, G., Witten, D., Hastie, T., & Tibshirani, R. (2021). An Introduction to Statistical Learning: with Applications in R (2nd ed.). Springer.
- Field, A. (2023). Discovering Statistics Using IBM SPSS Statistics (6th ed.). SAGE Publications.
- Cheng, Y., & Wang, G. (2021). Statistical Data Analysis: An Introduction with R (2nd ed.). Springer.
- Bishop, C. M. (2022). Pattern Recognition and Machine Learning. Springer.
- Wickham, H., & Grolemund, G. (2021). R for Data Science: Import, Tidy, Transform, Visualise, and Model Data (2nd ed.). O'Reilly Media.
- Fitzpatrick, T., & Gnanadesikan, M. (2022). Practical Statistics for Data Scientists: 50+ Essential Concepts Using R and Python (2nd ed.). O'Reilly Media.

Suggested Research Oriented reading:

- Yang, L. (2021). Statistics for Data Science: A Step-by-Step Approach (1st ed.). Wiley.
- Pindyck, R. S., & Rubinfeld, D. L. (2020). Microeconomics (9th ed.). Pearson.
- Crawley, M. J. (2023). Statistics: An Introduction Using R (2nd ed.). Wiley.

- Gareth, J., Daniela, W., Trevor, H., & Robert, T. (2020). An Introduction to Statistical Learning: with Applications in R (2nd ed.). Springer.

MCS710

Security Engineering

Module Description

The aim of this module is to develop learners' understanding and skills in secure software development life cycle, system hardening techniques, authentication and authorisation processes, encryption techniques, network security measures to analyse, evaluate security of systems and design web applications architecture. The learner can critically evaluate various security tools and standards for security engineering in a range of data security measures, social engineering attacks, to explore and implement system hardening techniques and acquire the knowledge and skills to be able to design a secure system. Students engage with current research literature in security engineering, including vulnerability management, secure system design, threat modelling, and cryptographic applications. Emerging research topics such as zero-trust architectures and secure cloud infrastructures are examined through academic and professional sources.

Learning Outcomes

Competences:

At the end of the Module the learner will have acquired the responsibility and autonomy to:

- **Manage and take responsibility for complex security engineering activities,** including vulnerability assessment, system hardening, and security strategy implementation in unpredictable technical and organisational contexts.
- **Exercise leadership and professional accountability in security-critical environments,** guiding teams in the application of secure design principles, ethical decision-making, and industry best practices.
- **Advise stakeholders on strategic security decisions,** balancing technical risk, legal and regulatory obligations, organisational constraints, and societal impact.
- **Integrate interdisciplinary knowledge and professional judgement** to develop innovative and resilient security solutions, particularly where threats, technologies, and requirements are rapidly evolving or contested.

Knowledge:

At the end of the Module the learner will have been exposed to the following:

- **Demonstrate highly specialised and critical understanding of security engineering principles,** synthesising knowledge of system, network, and web application architectures as a basis for original security analysis and design.
- **Critically evaluate contemporary threat models and vulnerability frameworks,** including OWASP risk classifications, assessing their relevance, limitations, and implications for secure system and application development.
- **Analyse and critique security models and architectural approaches**, evaluating their effectiveness across diverse technological and organisational contexts, including cloud-based, distributed, and data-intensive environments.
- **Integrate advanced theoretical knowledge of cryptography and data protection,** critically assessing encryption algorithms, key management practices, and secure data handling mechanisms in relation to confidentiality, integrity, and availability.
- **Demonstrate critical awareness of ethical, legal, and societal considerations** in security engineering, including privacy, compliance, governance, human factors, and professional accountability in the protection of digital systems.

Skills:

At the end of the Module the learner will have acquired the following skills:

- **Design, implement, and critically evaluate security controls and countermeasures** for systems and web applications, applying research-informed judgement to mitigate complex or unfamiliar security risks.
- **Critically assess authentication, authorisation, and identity-management mechanisms,** including Single Sign-On (SSO) solutions, making defensible decisions under conditions of uncertainty, evolving threats, or incomplete information.
- **Apply advanced security testing, analysis, and validation techniques** to identify vulnerabilities and evaluate the effectiveness of security controls within dynamic and adversarial environments.
- **Evaluate and select appropriate security tools and frameworks,** balancing technical effectiveness, usability, regulatory compliance, and ethical considerations to support organisational security objectives.

- **Communicate complex security assessments, risk analyses, and mitigation strategies** clearly and unambiguously to specialist and non-specialist audiences, justifying recommendations through evidence-based reasoning.
- **Demonstrate advanced learning skills by independently identifying emerging security threats,** technologies, standards, and regulatory developments, critically evaluating their relevance to professional practice, and undertaking self-directed learning to maintain and enhance specialised security-engineering competence.

Module-Specific Learner Skills

Upon completion of the module, learners will demonstrate enhanced abilities in

- Enhanced ability to critically analyse security architectures and assess potential risks.
- Proficiency in identifying and addressing security vulnerabilities through practical solutions.
- Improved capability to articulate security concepts and recommendations clearly and effectively.
- Skill in working collaboratively in virtual environments to address complex security challenges.
- Ability to adapt to evolving cybersecurity threats and technologies to ensure effective security measures.

Module-Specific Digital Skills and Competences

Learners will develop digital skills and competencies including

- Proficiency in using security tools to detect and address vulnerabilities.
- Ability to analyse data to assess security risks and patterns effectively.
- Understanding and application of cybersecurity principles and compliance standards.
- Technical skill in configuring systems to enhance security measures.
- Competence in digital forensics for investigating security incidents.

Hours of Total Learning for this Module

- **Total Contact Hours: 30**

  Contact Hours are hours invested in learning new content under the Direction of a tutor/lecturer e.g. lectures participation in online forums

- **Supervised Placement and Practice Hours: 20**

During these hours the learner is supervised, coached, or mentored.

- **Self-Study Hours: 80**

  Estimated workload of research and study

- **Assessment Hours: 20**

  Examinations/ presentations/ group work/ projects etc.

- **Total Number of ECTS of this Module/Unit: 6 ECTS**

Total Learning Hours of this Module: 150 Hours

Pedagogy for this Module

The Security Engineering module would be taught through a combination of interactive lectures, practical labs, assignments, and collaborative discussions. Online lectures, delivered via video conferencing or recorded videos, would cover foundational concepts and theories. These lectures would be supplemented with interactive discussions facilitated through online forums or chat platforms, encouraging students to engage in critical analysis of security breaches, ethical considerations, and emerging trends. Practical labs conducted in virtual environments allow students to gain hands-on experience in configuring security tools, conducting assessments, and implementing security measures. Assignments and projects, designed to assess comprehension and application of concepts, would be submitted online, with feedback provided digitally. Additionally, guest lectures by industry professionals or academic experts would offer valuable insights into real-world challenges and career pathways. Through this blended approach, students would develop both theoretical knowledge and practical skills essential for security engineering in online environments. This module includes regular live synchronous sessions, such as supervised practical workshops, tutor-led demonstrations, live problem-solving sessions, and scheduled progress reviews. These activities form part of the module's contact hours and supervised placement and practice (non-WBL) hours and are delivered via video-conferencing tools integrated into the Virtual Learning Environment (VLE).

Assessment Weightings:

- Written assignments (40%) (It should not be more than 1250-word count)
- Programming Mini Project (30%)
- Final Examination (30%)

Learners must achieve a minimum of 50% overall and 50% in each assessment component; authenticity is verified through Turnitin (similarity and AI-writing indicators), VLE audit trails, and a recorded online viva and/or timed proctored task where appropriate, in accordance with institutional assessment regulations.

Digital learning tools like online submission platforms, code repositories, and video conferencing software will facilitate assessment.

Reading List

- Williams, S. (2023). Cybersecurity for Executives: A Practical Guide. Apress.
- Johnson, J. (2023). Web Application Security: A Beginner's Guide. McGraw-Hill.
- Smith, R. (2023). Digital Forensics and Cyber Crime: 14th International Conference, ICDF2C 2023. Springer.
- Goutam, R. K. (2021). Cybersecurity Fundamentals: Understand the Role of Cybersecurity, Its Importance and Modern Techniques Used by Cybersecurity Professionals (English Edition). BPB Publications.
- Moore, R. (2014). Cybercrime: Investigating high-technology computer crime. Routledge.
- Perlman, R., Kaufman, C., & Speciner, M. (2016). Network security: private communication in a public world. Pearson Education India.

Suggested Research Oriented reading:

- McDonald, P. (2023). Cybersecurity Essentials: Protecting Your Digital Life. Wiley.
- Dash, S. (2023). Data Privacy and Security: A Practical Guide for IT Professionals. Springer.
- Mitnick, K. D., & Simon, W. L. (2021). The Art of Deception: Controlling the Human Element of Security. Wiley.
- Ransbotham, S., & Mitra, S. (2021). The Impact of Cybersecurity Awareness on Employees. Cambridge University Press.

MCS711

Internet of Things and Cryptography

Module Description

This extensive module provides definitions of important terminologies about Internet of Things (IoT) and Cryptography. Students will explore the intricate relationship between the IoT and cryptography, gaining a profound understanding of how cryptography plays a pivotal role in securing the expansive network of interconnected devices that constitute the IoT ecosystem. This module will provide you with a comprehensive theoretical foundation on how cryptographic techniques are applied to IoT environments, ensuring their security and privacy. The module incorporates engagement with current research on IoT architectures and applied cryptography, including secure communication protocols, lightweight cryptographic schemes, and privacy-preserving IoT systems. Students analyse emerging research challenges through academic journals and standards-based publications.

Learning Outcomes

Competences:

At the end of the Module the learner will have acquired the responsibility and autonomy to:

- **Manage and take responsibility for complex IoT security initiatives,** making informed technical, ethical, and strategic decisions in unpredictable technological and organisational contexts.
- **Exercise leadership and professional accountability in IoT and cryptography projects,** guiding teams in the adoption of secure design principles, ethical practices, and industry standards.
- **Integrate interdisciplinary knowledge and professional judgement** to develop innovative, resilient, and ethically responsible IoT security solutions where requirements, risks, or technologies are evolving or contested.
- **Advise stakeholders on strategic IoT and security decisions,** balancing technical effectiveness, regulatory compliance, privacy considerations, and long-term sustainability.

Knowledge:

At the end of the Module the learner will have been exposed to the following:

- **Demonstrate highly specialised and critical understanding of Internet of Things (IoT) architectures and ecosystems,** synthesising knowledge of sensing, communication, computation, and data management as a basis for original analysis of IoT-enabled systems.
- **Critically evaluate the technical, architectural, and operational challenges of IoT systems,** including security, scalability, interoperability, and resilience, assessing their implications across diverse application domains such as smart cities, healthcare, and industrial environments.
- **Integrate advanced theoretical knowledge of cryptography** to critically assess its role in securing IoT systems, including mechanisms for confidentiality, integrity, authentication, and trust management in constrained and distributed environments.
- **Analyse and critique IoT authentication and key-management approaches,** including certificate-based and lightweight cryptographic schemes, evaluating their effectiveness, limitations, and suitability for heterogeneous IoT deployments.
- **Demonstrate critical awareness of ethical, legal, and societal considerations** associated with IoT and cryptography, including privacy, data protection, informed consent, accountability, and responsible data governance.

Skills:

At the end of the Module the learner will have acquired the following skills:

- **Design, implement, and critically evaluate secure IoT communication and data-protection solutions**, integrating cryptographic techniques and protocol design to address complex or unfamiliar security challenges using research-informed judgement.
- **Apply and assess advanced cryptographic mechanisms** for device authentication, key exchange, and secure data transmission, making defensible technical decisions under conditions of uncertainty or incomplete information.
- **Configure, optimise, and validate secure communication protocols** (e.g. MQTT, CoAP, TLS/SSL) for IoT environments, critically evaluating trade-offs in performance, scalability, and security.

- **Conduct systematic security analyses of IoT systems and case studies,** synthesising evidence to identify vulnerabilities, evaluate risks, and propose innovative cryptographic and architectural countermeasures.
- **Communicate complex IoT security designs, risk assessments, and recommendations** clearly and unambiguously to specialist and non-specialist audiences, justifying solutions through structured, evidence-based reasoning.
- **Demonstrate advanced learning skills by independently identifying** emerging IoT technologies, cryptographic methods, standards, and regulatory developments, critically evaluating their relevance to professional practice, and undertaking self-directed learning to maintain and enhance specialised competence.

Module-Specific Learner Skills

Upon completion of the module, learners will demonstrate enhanced abilities in

- Proficiency in implementing cryptographic techniques to secure IoT devices and communications.
- Ability to identify and mitigate security risks associated with IoT deployments using cryptographic solutions.
- Skill in articulating complex cryptographic concepts and IoT security issues to stakeholders with varying levels of technical expertise.
- Capacity to stay abreast of evolving IoT security trends and adjust cryptographic strategies accordingly for enhanced protection

Module-Specific Digital Skills and Competences

Learners will develop digital skills and competencies including

- Proficiency in using cryptographic software for securing IoT environments.
- Ability to analyse network traffic data for detecting security threats.
- Competence in Python programming for enhancing IoT device security.
- Skill in configuring firewall rules to protect IoT devices from unauthorised access.

Hours of Total Learning for this Module

- **Total Contact Hours: 30**

Contact Hours are hours invested in learning new content under the Direction of a tutor/lecturer e.g. lectures participation in online forums

- **Supervised Placement and Practice Hours: 20**

  During these hours the learner is supervised, coached, or mentored.

- **Self-Study Hours: 80**

  Estimated workload of research and study

- **Assessment Hours: 20**

  Examinations/ presentations/ group work/ projects etc.

- **Total Number of ECTS of this Module/Unit: 6 ECTS**

Total Learning Hours of this Module: 150 Hours

Pedagogy for this Module

The module will be taught multifaceted approach, blending lectures, practical labs, and interactive discussions. Students will delve into theoretical concepts through lectures, while practical lab sessions will offer hands-on experience in applying cryptographic techniques to secure IoT environments. Case studies of real-world breaches will deepen understanding, and assignments will challenge students to implement secure solutions. Guest lectures and workshops by industry experts will provide practical insights. Throughout, the focus will be on active learning, practical application, and critical thinking, ensuring students grasp both the theory and practice of IoT security and cryptography

Assessment Weightings:

- Written assignments (40%) (It should not be more than 1250-word count)
- Formative Knowledge Checks (30%)
- Final Examination (30%)

Learners must achieve a minimum of 50% overall and 50% in each assessment component; authenticity is verified through Turnitin (similarity and AI-writing indicators), VLE audit trails, and a recorded online viva and/or timed proctored task where appropriate, in accordance with institutional assessment regulations

Digital learning tools like online submission platforms, code repositories, and video conferencing

software will facilitate assessment.

Reading List

- Zargar, S., & Marjani, A. (2023). Internet of Things (IoT) Security: Principles and Practices. Springer.
- Yang, Y., & Yu, H. (2023). Cryptography and Security in the Internet of Things: Advances and Applications. Wiley.
- Xu, L. D., & Liu, C. (2023). IoT Security and Privacy: Principles, Practices, and Challenges. Elsevier.
- Patel, S. K., & Kaur, A. (2022). Internet of Things: Security and Privacy Issues. CRC Press.
- Al-Muhtadi, J., & Cheng, Y. (2022). Cryptographic Techniques for Secure IoT Applications. IGI Global.

Suggested Research Oriented reading:

- Mavrommati, I., & Al-Khori, A. (2022). Secure Internet of Things: Architecture, Protocols, and Standards. Springer.
- Khan, M. K., & Khan, M. I. (2023). IoT Security: Current Trends and Future Directions. Academic Press.
- Gupta, R., & Singh, R. (2023). Cybersecurity for the Internet of Things: A Comprehensive Guide. CRC Press.

MCS712

Networking and Kali Linux

Module Description

The Networking and Kali Linux module provides students with a comprehensive understanding of networking fundamentals and hands-on experience with Kali Linux, a powerful platform for penetration testing and cybersecurity. Students will learn about network protocols, IP addressing, subnetting, routing, and switching, as well as how to configure and secure networks. The module will also cover the use of Kali Linux tools for ethical hacking, including information gathering, vulnerability scanning, and exploitation techniques. Through practical exercises, students will develop the skills necessary to assess and secure networks in real-world environments. Students engage with contemporary research in network security and penetration testing, including emerging attack vectors, defensive strategies, and ethical hacking methodologies. Research literature and professional security reports are used to contextualise practical activities and tools.

Learning Outcomes

Competences:

At the end of the Module the learner will have acquired the responsibility and autonomy to:

- **Manage and take responsibility for complex network security and penetration-testing activities,** making informed technical and ethical decisions in unpredictable organisational or threat environments.
- **Exercise leadership and professional accountability in cybersecurity operations,** supervising teams and guiding the application of best practices in ethical hacking, vulnerability assessment, and incident prevention.
- **Advise stakeholders on strategic network security decisions**, integrating technical risk analysis with business priorities, regulatory obligations, and long-term resilience considerations.
- **Integrate interdisciplinary knowledge and professional judgement** to develop innovative and responsible security solutions where network environments, threats, or organisational requirements are evolving or contested.

Knowledge:

At the end of the Module the learner will have been exposed to the following:

- **Demonstrate highly specialised and critical understanding of advanced networking principles**, synthesising knowledge of IP addressing, routing, switching, and network architectures as a foundation for analysing and securing complex networked systems.
- **Critically evaluate network security architectures and threat models**, assessing how vulnerabilities arise across layered network environments and how defensive strategies mitigate risks in organisational contexts.
- **Analyse and critique penetration testing methodologies and frameworks**, including ethical hacking standards and regulatory constraints, evaluating their role in proactive security assurance.
- **Integrate advanced theoretical knowledge of offensive and defensive security tools,** including Kali Linux–based ecosystems, to assess their capabilities, limitations, and appropriateness for different security objectives.
- **Demonstrate critical awareness of ethical, legal, and professional responsibilities** associated with penetration testing and network security, including responsible disclosure, compliance, and risk governance.

Skills:

At the end of the Module the learner will have acquired the following skills:

- **Design, execute, and critically evaluate penetration testing and vulnerability-assessment workflows,** integrating networking knowledge and Kali Linux tools to address complex or unfamiliar security challenges using research-informed judgement.
- **Critically assess network configurations and traffic behaviour**, applying advanced diagnostic and analytical techniques to identify vulnerabilities, misconfigurations, and attack vectors.
- **Apply and evaluate a range of penetration testing and security analysis tools** (e.g. scanning, exploitation, and traffic-analysis utilities), making defensible technical decisions under conditions of uncertainty or incomplete information.
- **Develop and justify network hardening and remediation strategies**, balancing technical effectiveness, organisational constraints, and ethical considerations.

- **Communicate penetration testing findings, risk assessments, and security recommendations** clearly and unambiguously to specialist and non-specialist audiences through structured reports and briefings.
- **Demonstrate advanced learning skills by independently** identifying emerging networking threats, penetration-testing techniques, and security standards, critically evaluating their relevance to professional practice, and undertaking self-directed learning to maintain and enhance specialised competence.

Module-Specific Learner Skills

Upon completion of the module, learners will demonstrate enhanced abilities in

- Ability to configure and manage network devices, troubleshoot issues, and implement advanced network protocols to ensure secure and efficient network operation.
- Skill in using Kali Linux tools to perform comprehensive penetration testing, including vulnerability scanning, exploitation, and post-exploitation activities in a secure and ethical manner.
- Ability to analyse network traffic, detect anomalies, and monitor network performance to ensure security and optimise the functionality of network systems.
- Capability to conduct thorough security assessments, identify potential threats, and recommend mitigation strategies to safeguard networks from attacks.
- Proficiency in documenting penetration testing results, security assessments, and network configurations in detailed, professional reports that include technical findings and recommendations.

Module-Specific Digital Skills and Competences

Learners will develop digital skills and competencies including

- Proficiency in using digital tools to configure network devices and simulate network environments, including routers, switches, and firewalls, to ensure secure connectivity.
- Competence in using Kali Linux-based tools like Nmap, Metasploit, Wireshark, and Burp Suite for network vulnerability scanning, exploitation, and security auditing.
- Ability to analyse network traffic using packet sniffers (such as Wireshark) to detect vulnerabilities, monitor traffic patterns, and identify potential threats in real-time.
- Skilled use of security auditing and risk analysis software to assess network configurations,

identify weaknesses, and propose security improvements.

- Experience in using virtual machines and simulators (e.g., VMware, VirtualBox) to create isolated environments for ethical hacking, penetration testing, and network troubleshooting.

Hours of Total Learning for this Module

- **Total Contact Hours: 30**

  Contact Hours are hours invested in learning new content under the Direction of a tutor/lecturer e.g. lectures participation in online forums

- **Supervised Placement and Practice Hours: 20**

  During these hours the learner is supervised, coached, or mentored.

- **Self-Study Hours: 80**

  Estimated workload of research and study

- **Assessment Hours: 20**

  Examinations/ presentations/ group work/ projects etc.

- **Total Number of ECTS of this Module/Unit: 6 ECTS**

Total Learning Hours of this Module: 150 Hours

Pedagogy for this Module

The Networking and Kali Linux module will be taught through a combination of theoretical lectures, practical demonstrations, and hands-on lab sessions. Students will engage with Kali Linux and related penetration testing tools such as Nmap, Wireshark, and Metasploit in a controlled virtual environment. Learning will be supported by online resources, including video tutorials, lab exercises, and interactive forums for collaboration. Virtualization platforms like VMware or VirtualBox will be used to simulate network environments for penetration testing and network analysis. Assessment will involve both practical exercises and written reports to demonstrate applied skills in network security. This module includes regular live synchronous sessions, such as supervised practical workshops, tutor-led demonstrations, live problem-solving sessions, and scheduled progress reviews. These activities form part of the module's contact hours and supervised placement and practice (non-WBL) hours and are delivered via video-

conferencing tools integrated into the Virtual Learning Environment (VLE).

Assessment Weightings:

- Written assignments (40%) (It should not be more than 1250-word count)
- Formative Knowledge Checks (30%)
- Final Examination (30%)

Learners must achieve a minimum of 50% overall and 50% in each assessment component; authenticity is verified through Turnitin (similarity and AI-writing indicators), VLE audit trails, and a recorded online viva and/or timed proctored task where appropriate, in accordance with institutional assessment regulations.

Digital learning tools like online submission platforms, code repositories, and video conferencing software will facilitate assessment.

Reading List

- William Stallings (2021). Data and Computer Communications (11th ed.). Pearson.
- Kali Linux Revealed (2020). Mastering the Penetration Testing Distribution (2nd ed.). Kali Linux Documentation.
- Geoffrey K. B. and Andrew Whitaker (2021). The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws. Wiley.
- Chris Sanders (2020). Practical Packet Analysis: Using Wireshark to Solve Real-World Network Problems (3rd ed.). No Starch Press.

Suggested Research Oriented reading:

- Mavrommati, I., & Al-Khori, A. (2022). Secure Internet of Things: Architecture, Protocols, and Standards. Springer.
- Khan, M. K., & Khan, M. I. (2023). IoT Security: Current Trends and Future Directions. Academic Press.
- Gupta, R., & Singh, R. (2023). Cybersecurity for the Internet of Things: A Comprehensive Guide. CRC Press.

Additional reading:

- Tomer L. and Doug Beattie (2022). Metasploit: The Penetration Tester's Guide. McGraw-Hill Education.

- Michael Gregg (2021). Kali Linux 2021: Assuring Security by Penetration Testing. Wiley.
- Kali Linux Cookbook (2021). Packt Publishing.
- Michael T. (2021). The Hacker Playbook 3: Practical Guide to Penetration Testing. CreateSpace Independent Publishing Platform.
- Thomas Wilhelm (2020). Mastering Kali Linux for Advanced Penetration Testing (3rd ed.). Syngress.

MCS713

Engineering of Hacking

Module Description

The Engineering of Hacking module focuses on the techniques, tools, and methodologies used in ethical hacking and penetration testing. Students will learn how to identify, exploit, and defend against vulnerabilities in various systems, including networks, web applications, and devices. The module emphasises hands-on practice with tools like Kali Linux to perform real-world hacking simulations and understand cybersecurity concepts. By the end, students will be able to apply ethical hacking principles to assess and improve system security. The module draws on current research in ethical hacking and offensive security, including studies on vulnerability discovery, exploit development, and responsible disclosure. Students engage with peer-reviewed research and professional security publications to inform analytical and practical work.

Learning Outcomes

Competences:

At the end of the Module the learner will have acquired the responsibility and autonomy to:

- **Manage and take responsibility for complex ethical hacking and penetration-testing projects,** independently planning, executing, and evaluating security assessments in unpredictable technical and organisational environments.
- **Exercise leadership and professional accountability in offensive security contexts**, guiding teams in the application of ethical hacking standards, best practices, and responsible decision-making.
- **Advise organisations strategically on security posture and resilience**, integrating penetration-testing evidence with business priorities, regulatory obligations, and risk management considerations.
- **Integrate interdisciplinary knowledge and professional judgement** to develop innovative and responsible security solutions where threat landscapes, technologies, or organisational requirements are evolving or contested.

Knowledge:

At the end of the Module the learner will have been exposed to the following:

- **Demonstrate highly specialised and critical understanding of ethical hacking and penetration-testing paradigms,** synthesising contemporary attack methodologies, threat models, and defensive strategies as a basis for original security analysis.
- **Critically evaluate vulnerability discovery and exploitation techniques** across networked systems, operating systems, and web applications, assessing their limitations, risks, and applicability in complex and evolving threat environments.
- **Analyse and critique ethical hacking frameworks, standards, and legal boundaries**, evaluating how professional codes, regulatory requirements, and governance structures shape responsible penetration-testing practice.
- **Integrate advanced theoretical knowledge of offensive and defensive security mechanisms,** critically assessing how security controls, protocols, and architectures respond to sophisticated attack techniques.
- **Demonstrate critical awareness of ethical, legal, and societal implications** of hacking activities, including responsible disclosure, proportionality, accountability, and the impact of security decisions on organisations and society.

Skills:

At the end of the Module the learner will have acquired the following skills:

- **Design, execute, and critically evaluate penetration-testing engagements**, integrating ethical hacking methodologies, tooling, and reporting practices to address complex or unfamiliar security challenges using research-informed judgement.
- **Apply and critically assess offensive security tools and techniques** (e.g. reconnaissance, scanning, exploitation, post-exploitation), making defensible decisions under conditions of uncertainty or incomplete technical information.
- **Analyse penetration-testing findings to prioritise security risks**, evaluating likelihood, impact, and organisational context to inform effective remediation strategies.
- **Develop and justify security improvement recommendations**, balancing technical effectiveness, operational constraints, legal compliance, and ethical responsibility.
- **Communicate penetration-testing methodologies, findings, and strategic recommendations** clearly and unambiguously to specialist and non-specialist audiences

through professional reports and briefings.

- **Demonstrate advanced learning skills by independently identifying** emerging networking threats, penetration-testing techniques, defensive technologies, and relevant security standards, critically evaluating their relevance to professional practice, and undertaking self-directed learning to maintain and enhance specialised competence.

Module-Specific Learner Skills

Upon completion of the module, learners will demonstrate enhanced abilities in

- Develop the ability to analyse and assess vulnerabilities in systems, networks, and applications using penetration testing techniques.
- Demonstrate problem-solving skills by identifying security flaws and applying appropriate tools and techniques to exploit and fix them.
- Gain proficiency in using penetration testing tools such as Kali Linux, Metasploit, and Wireshark for real-world hacking simulations.
- Apply ethical guidelines and standards when conducting hacking activities, ensuring all actions comply with legal and professional codes of conduct.
- Effectively document findings, prepare comprehensive penetration testing reports, and communicate recommendations to stakeholders and non-technical audiences.

Module-Specific Digital Skills and Competences

Learners will develop digital skills and competencies including

- Demonstrate proficiency in using digital tools such as Kali Linux, Metasploit, Burp Suite, and Wireshark for ethical hacking and vulnerability assessment.
- Perform network scans, traffic analysis, and vulnerability assessments using digital tools to identify weaknesses and potential entry points.
- Apply advanced digital techniques to exploit security vulnerabilities in web applications, networks, and other digital infrastructures.
- Conduct digital security audits and create actionable reports, using tools and software to document findings and provide recommendations for system hardening.
- Utilise digital forensics tools to analyse compromised systems, recover evidence, and trace cyber-attacks during penetration testing.

Hours of Total Learning for this Module

- **Total Contact Hours: 30**

  Contact Hours are hours invested in learning new content under the Direction of a tutor/lecturer e.g. lectures participation in online forums

- **Supervised Placement and Practice Hours: 20**

  During these hours the learner is supervised, coached, or mentored.

- **Self-Study Hours: 80**

  Estimated workload of research and study

- **Assessment Hours: 20**

  Examinations/ presentations/ group work/ projects etc.

- **Total Number of ECTS of this Module/Unit: 6 ECTS**

Total Learning Hours of this Module: 150 Hours

Pedagogy for this Module

The Engineering of Hacking module will be taught using a blend of theoretical instruction and hands-on practical sessions. Lectures will cover ethical hacking concepts, methodologies, and legal considerations, while lab sessions will provide students with real-world scenarios for penetration testing and vulnerability assessment. Students will use industry-standard tools like Kali Linux, Metasploit, and Wireshark to conduct simulated hacking exercises. Digital learning tools will include virtual labs for safe, controlled testing environments and learning management systems (LMS) for accessing resources and submitting assignments. Assessment will combine practical demonstrations of skills and theoretical knowledge tests. Collaborative learning will be encouraged through group projects and peer assessments. This module includes regular live synchronous sessions, such as supervised practical workshops, tutor-led demonstrations, live problem-solving sessions, and scheduled progress reviews. These activities form part of the module's contact hours and supervised placement and practice (Non-WBL) hours and are delivered via video-conferencing tools integrated into the Virtual Learning Environment (VLE).

Assessment Weightings:

- Written assignments (40%) (It should not be more than 1250-word count)
- Formative Knowledge Checks (30%)
- Final Examination (30%)

Learners must achieve a minimum of 50% overall and 50% in each assessment component; authenticity is verified through Turnitin (similarity and AI-writing indicators), VLE audit trails, and a recorded online viva and/or timed proctored task where appropriate, in accordance with institutional assessment regulations.

Digital learning tools like online submission platforms, code repositories, and video conferencing software will facilitate assessment.

Reading List

- Hertzog, R., O'Gorman, J., & Aharoni, M. (2020). Kali Linux Revealed: Mastering the Penetration Testing Distribution. Kali Linux.
- Stuttard, D., & Pinto, M. (2020). The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws. Wiley.
- Weidman, G. (2020). Penetration Testing: A Hands-On Introduction to Hacking. No Starch Press.
- Dowd, M., McDonald, J., & Schuh, J. (2020). The Art of Software Security Assessment: Identifying and Preventing Software Vulnerabilities. Addison-Wesley Professional.
- Kennedy, D., O'Gorman, J., Kearns, D., & Aharoni, M. (2020). Metasploit: The Penetration Tester's Guide. No Starch Press.

Suggested Research Oriented reading:

- Lloyd, S. (2021). Mastering Modern Web Penetration Testing. Packt Publishing.
- Bishop, M. (2020). Computer Security: Art and Science. Addison-Wesley.
- Shostack, A. (2021). Threat Modelling: Designing for Security. Wiley.
- Forrest, S., & Soni, A. (2021). The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy. Elsevier.

MCS714

Forensic Computing

Module Description

The Forensic Computing module provides students with the knowledge and skills required to investigate and analyse digital evidence from a variety of sources. It covers topics such as data acquisition, evidence preservation, cybercrime investigation, and legal considerations in digital forensics. The module focuses on the application of forensic tools and techniques to solve real-world cybercrime cases, ensuring students understand both technical and ethical aspects of forensic computing. Students engage with contemporary research in digital forensics, including evidence acquisition, forensic analysis techniques, and legal admissibility of digital evidence. Academic research and professional guidelines are used to analyse evolving forensic challenges.

Learning Outcomes

Competences:

At the end of the Module the learner will have acquired the responsibility and autonomy to:

- **Manage and take responsibility for complex digital forensic investigations,** making informed technical, legal, and ethical decisions in unpredictable investigative or organisational environments.
- **Exercise professional accountability and leadership in forensic practice**, supervising others in evidence handling, analysis, and adherence to legal, procedural, and ethical standards.
- **Advise organisational and legal stakeholders on forensic risk and response strategies,** integrating investigative findings with regulatory obligations, evidentiary requirements, and organisational priorities.
- **Assume responsibility for the integrity and admissibility of digital evidence**, ensuring that investigative processes comply with professional standards and withstand legal and regulatory scrutiny.

Knowledge:

At the end of the Module the learner will have been exposed to the following:

- **Demonstrate highly specialised and critical understanding of digital forensic**

principles and investigative models, synthesising knowledge of evidence acquisition, preservation, analysis, and reporting as a basis for original forensic reasoning.

- **Critically evaluate forensic tools, techniques, and methodologies** used in the examination of digital evidence from computers, mobile devices, networks, and cloud environments, assessing their reliability, limitations, and evidential value.
- **Analyse and critique legal and regulatory frameworks governing digital forensic practice,** including evidentiary admissibility, chain of custody requirements, data protection legislation, and courtroom procedures.
- **Integrate interdisciplinary knowledge** from cybersecurity, information systems, and law to assess the nature, scope, and impact of cybercrime, fraud, and digital misconduct in complex organisational and societal contexts.
- **Demonstrate critical awareness of ethical and societal responsibilities** inherent in forensic investigations, including privacy, proportionality, accountability, and responsible handling of sensitive digital evidence.

Skills:

At the end of the Module the learner will have acquired the following skills:

- **Design, conduct, and critically evaluate digital forensic investigations,** applying appropriate methodologies and tools to address complex or unfamiliar incidents using research-informed judgement.
- **Apply advanced forensic acquisition and analysis techniques**, critically assessing data integrity, authenticity, and evidential relevance when working with incomplete, corrupted, or contested digital evidence.
- **Critically interpret and evaluate forensic findings,** exercising judgement in assessing their significance, limitations, and implications for legal proceedings, organisational risk, or further investigation.
- **Employ forensic technologies and platforms** to examine diverse digital artefacts, making defensible technical decisions under conditions of uncertainty, legal constraint, or limited information.
- **Communicate forensic methodologies, findings, and expert conclusions** clearly and unambiguously to specialist and non-specialist audiences through structured reports, briefings, and evidentiary documentation.

Module-Specific Learner Skills

Upon completion of the module, learners will demonstrate enhanced abilities in

- Develop the ability to carefully collect, preserve, and transport digital evidence while maintaining chain of custody.
- Gain hands-on experience with industry-standard forensic tools (e.g., FTK, EnCase, X1) to conduct data recovery and analysis.
- Enhance skills in analyzing digital evidence, identifying anomalies, and preparing detailed forensic reports for legal or corporate investigations.
- Cultivate problem-solving abilities to address challenges in digital forensic investigations, such as damaged or encrypted files.
- Develop an understanding of legal frameworks and ethical guidelines for conducting forensic investigations, ensuring compliance with laws and regulations.

Module-Specific Digital Skills and Competences

Learners will develop digital skills and competencies including

- Proficiency in using forensic software tools such as EnCase, FTK, X1, and Autopsy to extract, analyze, and present digital evidence from various devices (computers, smartphones, and servers).
- Data Recovery and Analysis:
- Ability to recover and analyse deleted, encrypted, or corrupted data from hard drives, mobile devices, and cloud storage systems using industry-standard techniques.
- Competence in ensuring the integrity of digital evidence, maintaining accurate documentation of the chain of custody, and utilising hashing algorithms to verify the authenticity of the data.
- Skills in analysing network traffic to identify malicious activity, unauthorised access, or data breaches, using network forensic tools such as Wireshark and NetFlow analyzers.
- Ability to compile and present forensic findings in clear, concise reports, including legal documentation, screenshots, and technical details, suitable for courtrooms or corporate investigations.

Hours of Total Learning for this Module

- **Total Contact Hours: 30**

  Contact Hours are hours invested in learning new content under the Direction of a tutor/lecturer e.g. lectures participation in online forums

- **Supervised Placement and Practice Hours: 20**

  During these hours the learner is supervised, coached, or mentored.

- **Self-Study Hours: 80**

  Estimated workload of research and study

- **Assessment Hours: 20**

  Examinations/ presentations/ group work/ projects etc.

- **Total Number of ECTS of this Module/Unit: 6 ECTS**

Total Learning Hours of this Module: 150 Hours

Pedagogy for this Module

The Forensic Computing module will be taught through a combination of theoretical lectures, practical labs, and case study analysis. Students will gain hands-on experience using industry-standard forensic tools such as EnCase, FTK, and Autopsy to analyse and recover digital evidence. Digital learning tools, including virtual labs and simulation software, will be used to provide real-world scenarios for analysis and reporting. Additionally, online resources such as instructional videos, digital forensic case databases, and forums will support learning. Regular assessments will ensure students are equipped to handle digital investigations effectively, adhering to legal standards.

Assessment Weightings:

- Written assignments (40%) (It should not be more than 1250-word count)
- Peer Review (30%)
- Final Examination (30%)

Learners must achieve a minimum of 50% overall and 50% in each assessment component; authenticity is verified through Turnitin (similarity and AI-writing indicators), VLE audit trails, and a recorded online viva and/or timed proctored task where appropriate, in accordance with

institutional assessment regulations

Digital learning tools like online submission platforms, code repositories, and video conferencing software will facilitate assessment.

Reading List

- Casey, E. (2011). Handbook of Digital Forensics and Investigation. Elsevier.
- Nelson, B., Phillips, A., & Steuart, C. (2019). Guide to Computer Forensics and Investigations (6th ed.). Cengage Learning.
- Bunting, M. (2019). Digital Forensics: Digital Evidence in Criminal Investigations. Wiley.
- Shinder, D., & Cross, M. (2017). Scene of the Cybercrime: Computer Forensics Handbook. Syngress.

Suggested Research Oriented reading:

- Kennesaw, A. (2020). Digital Forensics for Legal Professionals: Understanding Digital Evidence from the Warrant to the Courtroom. Syngress.
- Easttom, C. (2020). Computer Security and Digital Forensics. Pearson.
- Baggili, I. (2017). Digital Forensics and Cyber Crime: 9th International Conference, ICDF2C 2017. Springer.
- Brous, P., & Boulanger, C. (2020). Practical Guide to Computer Forensics Investigations. CRC Press.
- Maras, M. H. (2016). Computer Forensics: Cybercriminals, Laws, and Evidence. Jones & Bartlett Learning.

MCS715

Application and Device Audit

Module Description

The Application and Device Audit module focuses on the methodologies and techniques for auditing software applications and devices within organisational environments. Students will learn how to assess security, compliance, and performance of various applications and devices, identifying vulnerabilities and potential risks. The module emphasises practical tools and real-world scenarios for conducting effective audits, ensuring the integrity and security of IT systems. The module integrates current research on application security, device auditing, and compliance frameworks. Students engage with academic and professional research on audit methodologies, risk assessment, and emerging regulatory and technological challenges.

Learning Outcomes

Competences:

At the end of the Module the learner will have acquired the responsibility and autonomy to:

- **Manage and take responsibility for complex application and device audit activities**, making independent and informed decisions on audit scope, risk prioritisation, and execution in unpredictable organisational contexts.
- **Exercise professional accountability and leadership during audit processes,** supervising the application of security controls and ensuring adherence to recognised industry standards and ethical requirements.
- **Advise organisational stakeholders on audit outcomes and risk mitigation strategies**, integrating technical findings with business objectives, regulatory obligations, and organisational risk appetite.
- **Assume responsibility for the integrity, credibility, and impact of audit conclusions**, ensuring that audit processes and outputs withstand professional, regulatory, and managerial scrutiny.

Knowledge:

At the end of the Module the learner will have been exposed to the following:

- **Demonstrate highly specialised and critical understanding of application and device audit frameworks**, synthesising principles of security assurance, compliance, and risk management as a basis for original audit planning and evaluation.
- **Critically evaluate auditing methodologies and standards** applicable to software applications and hardware devices, assessing their effectiveness in identifying vulnerabilities, misconfigurations, and compliance gaps in complex organisational environments.
- **Analyse and critique the role of application and device auditing** in protecting organisational data integrity, resilience, and trust, particularly in the context of evolving cyber threats and regulatory requirements.
- **Integrate advanced theoretical knowledge of secure software and device configurations**, critically assessing how source code analysis, configuration review, and system hardening contribute to effective audit outcomes.
- **Demonstrate critical awareness of ethical, legal, and professional considerations** in audit practice, including confidentiality, proportionality, accountability, and responsible disclosure of audit findings.

Skills:

At the end of the Module the learner will have acquired the following skills:

- **Design, conduct, and critically evaluate application and device audit engagements,** applying appropriate tools and methodologies to address complex or unfamiliar security and compliance challenges using research-informed judgement.
- **Apply and critically assess digital auditing and security-scanning tools** (e.g. vulnerability scanners, traffic analysers, configuration assessment tools), making defensible decisions under conditions of uncertainty or incomplete technical information.
- **Analyse audit findings to prioritise risks and vulnerabilities**, exercising judgement in balancing technical severity, business impact, regulatory exposure, and remediation feasibility.

- **Develop and communicate comprehensive audit reports**, clearly articulating vulnerabilities, compliance gaps, assumptions, and recommendations to specialist and non-specialist stakeholders.
- **Demonstrate learning skills through self-directed engagement with emerging audit tools, standards, and threat landscapes**, adapting audit approaches in response to technological change, new regulations, and evolving security practices.

Module-Specific Learner Skills

Upon completion of the module, learners will demonstrate enhanced abilities in

- Construct secure device configurations and analyse them through device management systems and mobile device management (MDM) tools.
- Use real-time monitoring systems to track and analyze device behaviour during the audit process, ensuring compliance with security policies.
- Plan and demonstrate the application of real-world security assessments and audits for networked applications, using a variety of digital forensic tools to gather evidence and support findings.

Module-Specific Digital Skills and Competences

Learners will develop digital skills and competencies including

- Students will gain expertise in using advanced digital forensics tools such as FTK Imager, EnCase, or Autopsy for extracting and analysing data from applications and devices during audits.
- Apply and configure security audit tools to assess and monitor the implementation of security policies across applications, operating systems, and networked devices.
- Learn to configure and operate endpoint security software (e.g., antivirus, EDR) to assess the effectiveness of security measures on applications and devices during audits.
- Use automated vulnerability scanning tools (such as OpenVAS, Nessus, or Qualys) to scan applications and devices for vulnerabilities and generate detailed security reports.
- Apply network analysis tools (e.g., Wireshark, tcpdump) to monitor and assess network traffic originating from applications and devices, identifying potential security threats and anomalies.
- Use log analysis tools (e.g., Splunk, ELK Stack) to analyse logs from devices and

applications, identifying any security breaches, access patterns, or compliance issues.

- Learn to integrate device management tools (e.g., MDM solutions) with auditing systems for a comprehensive security review of mobile and endpoint devices.

Hours of Total Learning for this Module

- **Total Contact Hours: 30**

  Contact Hours are hours invested in learning new content under the Direction of a tutor/lecturer e.g. lectures participation in online forums

- **Supervised Placement and Practice Hours: 20**

  During these hours the learner is supervised, coached, or mentored.

- **Self-Study Hours: 80**

  Estimated workload of research and study

- **Assessment Hours: 20**

  Examinations/ presentations/ group work/ projects etc.

- **Total Number of ECTS of this Module/Unit: 6 ECTS**

Total Learning Hours of this Module: 150 Hours

Pedagogy for this Module

This Application and Device Audit module will be taught through a combination of theoretical lectures, hands-on practical sessions, and real-world case studies. Students will utilise digital tools such as FTK Imager, Wireshark, and OpenVAS for conducting device and application audits. The course will include guided lab work, interactive tutorials, and group discussions to ensure students can effectively use these tools to analyse, audit, and secure applications and devices. Additionally, students will be encouraged to work on real-time scenarios to apply their knowledge in a practical setting.

Assessment Weightings:

- Written assignments (40%) (It should not be more than 1250-word count)
- Peer Review (30%)
- Final Examination (30%)

Learners must achieve a minimum of 50% overall and 50% in each assessment component; authenticity is verified through Turnitin (similarity and AI-writing indicators), VLE audit trails, and a recorded online viva and/or timed proctored task where appropriate, in accordance with institutional assessment regulations.

Digital learning tools like online submission platforms, code repositories, and video conferencing software will facilitate assessment.

Reading List

- Stallings, W. (2021). Network Security Essentials. Pearson Education.
- Sikorski, M., & Honig, A. (2020). Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software. No Starch Press.
- Stuttard, D., & Pinto, M. (2020). The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws. Wiley.
- Schneier, B. (2021). Applied Cryptography: Protocols, Algorithms, and Source Code in C. Wiley.
- Ligh, M. H., Adair, S., Hartstein, B., & Richard, M. (2020). The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory. Wiley.

Suggested Research Oriented reading:

- Kurtz, M., & Duna, J. (2022). Practical Guide to Digital Forensics Investigations. CRC Press.
- Vacca, J. R. (2020). Computer and Information Security Handbook. Elsevier.
- Kurose, J. F., & Ross, K. W. (2021). Computer Networking: A Top-Down Approach. Pearson.

MCS716

Capstone Project

Module Description

The aim of this module is to provide students with an opportunity to apply their knowledge and skills to solve a real-world computing problem. Common objectives include applying knowledge, conducting in-depth research, showcasing problem-solving skills, demonstrating effective project management, communicating findings clearly, exhibiting technical proficiency, applying critical thinking, considering ethical considerations, and promoting collaboration. The specific requirements may vary, so it's essential to refer to your institution's guidelines for precise information. The Capstone Project requires sustained engagement with current research literature relevant to the chosen project domain. Students critically analyse academic research, industry reports, and professional standards to inform problem formulation, solution design, and evaluation.

The Dissertation / Capstone Project constitutes the culminating academic component of the Master of Computer Science and enables learners to demonstrate advanced theoretical understanding, applied technical competence, and independent scholarly judgement consistent with MQF Level 7 descriptors.

Through an individual, research-informed project, learners design, implement, and critically evaluate an advanced computing system or research study addressing complex and unpredictable technical challenges. The module emphasises autonomy, responsibility, and critical decision-making in both technical and research contexts.

Learning Outcomes

Competences:

At the end of the Module the learner will have acquired the responsibility and autonomy to:

- **Manage and take full responsibility for a complex, extended computing project,** independently planning, executing, and controlling all phases from problem definition to final delivery in unpredictable technical or organisational contexts.
- **Exercise professional accountability and leadership in project execution**, including managing time, resources, and, where relevant, collaboration with others to achieve defined objectives.

- **Make informed and responsible decisions regarding technical direction, methodological choices, and ethical implications**, ensuring that project outcomes meet professional, academic, and societal expectations.
- **Assume responsibility for the originality, quality, and integrity of project outcomes,** ensuring that the work contributes meaningfully to professional practice or applied research within the chosen domain.

Knowledge:

At the end of the Module the learner will have been exposed to the following:

- **Demonstrate highly specialised and critical understanding of advanced theories, principles, and practices in computer science**, synthesising knowledge from contemporary and emerging technological domains as a foundation for original project work.
- **Integrate specialised knowledge within a chosen area of computer science** (e.g. artificial intelligence, machine learning, cybersecurity, software engineering), critically linking theory, practice, and research to address complex real-world problems.
- **Critically analyse and contextualise current research and professional practice**, evaluating how methodological, technological, and interdisciplinary considerations influence problem formulation and solution design.
- **Demonstrate critical awareness of ethical, societal, and professional considerations** associated with advanced computing projects, including responsible innovation, sustainability, and the impact of technology on individuals and organisations.

Skills:

At the end of the Module the learner will have acquired the following skills:

- **Design, implement, and critically evaluate a substantial computing project,** applying advanced technical knowledge, research methods, and problem-solving strategies to address complex or unfamiliar challenges using research-informed judgement.
- **Apply advanced analytical and computational techniques**, including algorithm design, software development frameworks, and system evaluation methods, to produce robust, innovative, and ethically responsible solutions.
- **Perform critical evaluations and make defensible judgements under conditions of uncertainty**, incomplete information, or evolving requirements, optimising project

outcomes through iterative analysis and refinement.

- **Communicate project objectives, methodologies, findings, and limitations** clearly and unambiguously to specialist and non-specialist audiences through professional reports, presentations, and demonstrations.
- **Demonstrate learning skills through self-directed acquisition and application of new knowledge, tools, and methodologies**, adapting project scope and approach in response to emerging technologies, feedback, and research insights.
- **Select, justify, and apply appropriate programming languages, frameworks, and tools relevant to the project domain,** demonstrating informed technical judgement in choosing solutions that best address the defined problem.

Module-Specific Learner Skills

Upon completion of the module, learners will demonstrate enhanced abilities in

- Enhanced problem-solving skills to address complex challenges in computer science.
- Improved critical thinking abilities for analysing and evaluating technical solutions.
- Advanced communication skills for effectively conveying complex ideas to diverse audiences.
- Heightened creativity and innovation in proposing novel approaches to technical problems.

Module-Specific Digital Skills and Competences

Learners will develop digital skills and competencies including

- Proficient use of cutting-edge software development tools and technologies.
- Competent utilisation of data analytics platforms for extracting valuable insights from extensive datasets.
- Skilled implementation of cybersecurity measures to safeguard digital assets and mitigate potential risks.
- Adept navigation and utilisation of cloud computing platforms for scalable and adaptable computing resources.
- Proficient application of emerging technologies like artificial intelligence and machine learning for pioneering solutions.

Hours of Total Learning for this Module

- **Total Contact Hours: 150**

  Contact Hours are hours invested in learning new content under the Direction of a tutor/lecturer e.g. lectures participation in online forums

- **Supervised Placement and Practice Hours: 150**

  During these hours the learner is supervised, coached, or mentored.

- **Self-Study Hours: 330**

  Estimated workload of research and study

- **Assessment Hours: 120**

  Examinations/ presentations/ group work/ projects etc.

- **Total Number of ECTS of this Module/Unit: 30 ECTS**

Total Learning Hours of this Module: 750 Hours

Pedagogy for this Module

The capstone project for the Master of Computer Science programme will be facilitated through virtual platforms and online resources. The teaching approach will adapt to the digital environment while ensuring effective delivery of instruction and support to students.

- **Virtual Orientation Sessions:** Orientation sessions and workshops will be conducted virtually, where students will receive information about project requirements, timelines, and expectations. They will also be introduced to their faculty mentors and receive guidance on accessing online resources.
- **Remote Guidance and Mentorship:** Faculty mentors will provide remote guidance and mentorship to students through video conferencing, email, and online chat platforms. Regular virtual meetings will be scheduled to discuss project progress, address queries, and provide feedback on research and implementation strategies.
- **Online Research Resources:** Students will utilise online libraries, databases, and academic journals to conduct research and gather literature relevant to their project topics. Access to digital resources will enable students to explore a wide range of sources and stay updated with the latest developments in their field.

- **Virtual Collaboration Tools:** Online collaboration tools such as video conferencing platforms, discussion forums, and project management software will facilitate peer collaboration and communication. Students will have opportunities to engage in virtual group discussions, share resources, and collaborate on project tasks remotely.
- **Remote Project Implementation:** Students will implement their projects remotely using virtual development environments, cloud-based platforms, and collaboration tools. They will have access to online coding platforms, version control systems, and testing environments to develop and test their solutions.
- **Presentations and Reviews:** Reviews, presentations, and evaluations will be conducted online using video conferencing tools. Students will present their project progress, findings, and outcomes to faculty mentors and peers virtually. Feedback and discussions will be facilitated through online platforms to ensure effective communication and collaboration.
- **Digital Documentation and Reporting:** Project documentation, reports, and presentations will be created and shared digitally using online document editing tools, slide presentation software, and virtual whiteboards. Students will submit their project deliverables electronically, and evaluations will be conducted online.
- **Remote Reflection and Evaluation**: Students will reflect on their learning experiences and project outcomes through online reflection activities, discussion forums, and self-assessment tools. Evaluation of individual performance and project outcomes will be conducted remotely, with feedback provided digitally.

The dissertation includes **350 hours of Supervised Placement and Practice Hours (Non-WBL),** delivered entirely within the institutional learning environment under academic supervision. This supervised practice supports learners in applying advanced knowledge through structured academic guidance and iterative feedback.

This module **does not constitute Work-Based Learning (WBL)** and does not involve external employers, workplace placements, or employment-based learning outcomes.

Supervised Placement and Practice Hours (Non-WBL) within the dissertation is delivered through:

- scheduled dissertation supervision meetings;
- supervised system design and implementation activities;
- guided technical reviews and code walkthroughs;
- formative feedback on research design, artefacts, and drafts;

- critical reflection on technical, methodological, and ethical decisions.

Supervision is provided by qualified academic staff and is documented through supervision logs, feedback records, and VLE engagement data. This supervised practice is **not classified as Work-Based Learning (WBL)** and does not involve external employers or workplace placements.

Supervision Model

- Each learner is allocated a named dissertation supervisor.
- Learners receive a minimum of 12–15 scheduled online supervision sessions.
- Supervisor-to-student ratio does not exceed 1:8.
- Supervision covers research design, advanced technical implementation, and academic writing.
- Supervision records, feedback, and progress monitoring are retained for audit purposes.
- Evidence retained: supervision logs, VLE records, annotated feedback, versioned artefacts.

Evaluation, Moderation, and Academic Integrity

Capstone Projects are subject to formal evaluation and quality assurance procedures. All written submissions are screened using plagiarism-detection software (e.g. Turnitin) in accordance with the institution's Academic Integrity Policy.

Assessment decisions are subject to **internal moderation**, whereby a second academic reviewer samples and reviews marking decisions to ensure consistency, fairness, and alignment with MQF Level 7 standards. Where applicable, external academic input may be used for benchmarking and

quality enhancement.

Assessment of the Capstone Project

The Capstone Project is assessed through a criterion-referenced approach, designed to evaluate the learner's ability to integrate advanced theoretical knowledge, applied technical skills, and research-informed judgement within a coherent and professionally executed computing project. Assessment focuses on both the process and outcomes of the project, ensuring that learners are evaluated on problem formulation, methodological rigor, technical implementation, critical analysis, and professional communication.

Each assessment component (project report, software or technical artefact, presentation and demonstration, and supporting documentation) is evaluated against the defined assessment criteria. These criteria collectively measure the learner's capacity to justify technical decisions, apply appropriate methodologies and tools, critically evaluate results, and communicate findings effectively. The assessment criteria are aligned with the learning outcomes of the Capstone

Project and reflect expectations of advanced postgraduate study in computer science.

Assessment judgements are based on the extent to which the project demonstrates academic rigor, technical competence, originality of approach where appropriate, and adherence to ethical and professional standards. The criteria are applied consistently across all projects to ensure transparency, fairness, and comparability of assessment outcomes.

1**. Project Assessment Components:**

Assessment of the Capstone Project is based on the following components:

- **Research Proposal and Methodology Design – 15%**

  Assessment of the clarity, coherence, and technical rigor of the proposed research problem, objectives, and methodology. This includes justification of the chosen technical approach, algorithms, system architecture, data sources, evaluation strategy, and ethical or professional considerations.

- **Implemented System / Technical Artefact – 25%**

  Evaluation of the developed software, system, model, or technical artefact. Assessment focuses on correctness, functionality, technical complexity, efficiency, robustness, and appropriateness of tools, programming languages, and frameworks used.

- **Technical Documentation and Validation Results – 20%**

  Assessment of supporting technical documentation and validation evidence, including system architecture descriptions, code documentation, configuration details, test cases, performance metrics, benchmarking, security testing, or experimental results. Documentation must support understanding, reproducibility, and critical evaluation of the solution.

- **Critical Analytical Dissertation (Project Report) – 25%**

  Evaluation of the written dissertation/report, which must critically integrate relevant literature, contextualise the project within current research and professional practice, analyse results rigorously, and reflect on limitations, trade-offs, and implications. The dissertation must demonstrate research-informed reasoning, academic rigor, and clear technical argumentation.

- **Online Oral Defence (Viva Voce) – 15%**

  Assessment of the learner's ability to present and defend the project in an online oral examination. This includes clarity of technical explanation, justification of design and methodological decisions, critical reflection, and the ability to respond accurately and professionally to questions and feedback.

Pass Mark:

Learners must achieve a minimum of 50% overall and 50% in each assessment component; authenticity is verified through Turnitin (similarity and AI-writing indicators), VLE audit trails, and the recorded Online Oral Defence (Viva Voce), in accordance with institutional assessment regulations.

2. Digital Learning Tools:

- **Learning Management System (LMS):** Often used for document submission, announcements, and tracking progress.
- **Plagiarism Detection Software:** Tools like Turnitin or SafeAssign to ensure academic integrity in dissertation submissions.
- **Research Databases:** Access to online libraries and databases for literature review and research data gathering**.**
- **Collaboration Tools:** Platforms like Google Workspace, Zoom, or Microsoft Teams for communication and collaborative work with supervisors and peers.

Assessment Weightings:

- Research Proposal and Methodology Design – 15%
- Implemented System / Technical Artefact – 25%
- Technical Documentation and Validation Results – 20%
- Critical Analytical Dissertation (Project Report) – 25%
- Online Oral Defence (Viva Voce) – 15%

Reading List

- Pahl, G., & Lee, J. (2021). Service-Oriented Architecture: Concepts, Technology, and Design. Springer.
- Dastjerdi, A. V., & Patel, A. (2021). Internet of Things: Principles and Paradigms. Morgan Kaufmann.
- Balaji, P., & Sundararajan, S. (2022). Machine Learning and Deep Learning in Real-Time Applications. Wiley.
- Gallo, J. (2022). Data Science for Business: A Beginner's Guide. Springer.
- Chen, J., & Zhao, Q. (2023). Cloud Computing: Principles and Practice (3rd ed.). Morgan Kaufmann.
- Allen, D. (2022). The Data Warehouse Toolkit: The Definitive Guide to Dimensional Modelling (4th ed.). Wiley.

Based on the practical subject.