

MODULE DIRECTORY

MSc CYBERSECURITY AND DIGITAL FORENSICS

LEVEL 7

ACADEMIC DISCIPLINE OF BIRMINGHAM AND LONDON CAMPUSES

INSTITUTE OF INNER CITY LEARNING

2026-2027

CONTENTS PAGE

Page No

INTRODUCTION.....	1
MODULES	2
ACCA7027	2
ACCA7028	5
ACCA7031	6
ACCA7032	10
ACCA7033	13
ACFA7003.....	16
ACFA7004.....	20

INTRODUCTION

This Module Directory includes all the modules for Level 7 within the Institute of Inner City Learning in the academic year 2026-2027.

This directory accompanies the Programme of Study Handbook, which will provide you with details of which modules you will be studying for your programme this year in the 'Programme of Study' section. This directory may include modules that are running on other programmes of study within your School/Faculty. If you require assistance in identifying the modules for your programme of study, please contact the Programme Manager (whose name and contact details are provided in the accompanying Programme of Study Handbook), or the relevant Faculty Office.

The University has made every effort to make the information as full and as accurate as possible, but you should note that minor changes in the organisation of modules between the planning stage and the actual teaching are inevitable. We shall try to keep any such changes to a minimum, and you will receive plenty of advance warning in the event of any alteration. We would also be grateful if you would let us know about any changes that you think might be helpful if introduced into future handbooks.

MODULES

Module Code	ACCA7027
Title	Cloud Engineering Principles and Practice
Date	31/07/2020
Level	7
Credits	20
Pre-Requisites	None

AIM(S)

- To enable students to critically evaluate cloud related systems, technologies, applications, software development process, administration techniques and principles
- To be able to implement, configure or work within a virtualised environment that can either be deployed to the cloud or implemented within the cloud computing providers platform

LEARNING OUTCOMES

Upon the successful completion of this module, the student should be able to:

- Critically evaluate the cloud computing related technologies and the applications of cloud services
- Implement virtual systems and/or applications that can be deployed to the cloud and demonstrate an understanding of the features of platforms provided by cloud computing providers

INDICATIVE CONTENT

- Containerization using Docker and Kubernetes, building and running images, Docker compose
- Big data. Principles of distributed file systems (Hadoop, AWS EFS), NoSQL e.g. Redis, AWS S3, MongoDB, AWS DynamoDB, Cassandra, CAP Theorem, etc.
- Infrastructure components of cloud computing provider platforms e.g. virtual networks, virtual machines (e.g. EC2 instances), containers (e.g. AWS ECS), gateways, etc.
- Availability and scalability e.g. Load balancing and scaling groups.
- Web service and microservice deployment, message and event queues e.g. RabbitMQ, Kafka, AWS Simple Queue Service
- Security of virtualized systems, authorization, firewalls, security groups, etc.
- Applications e.g. web servers, Node.js web services, IoT, etc.

Study Time Allocation

The study time for the module is divided as follows:

Activity type	Hours	Percentage
Scheduled learning	48	24%
Independent learning	152	76%
Placement learning		
TOTAL	200	100%

ASSESSMENT

Assessment Component 1

☐ Written exam ☒ Coursework ☐ Practical

Mode of assessment	Volume	Weighting
Portfolio	5,000 words equivalent Students will produce a portfolio of work appropriate to the nature of their area of study. Portfolio elements may include a selection of the following: • Written Report • Documented application of tools or processes • Administration of virtualized systems • Implementation of cloud computing related applications • Discussion or demonstration of cloud computing platform features or functionality • Demonstration of their work e.g. written or presentation	100%

Assessment Summary

Activity type	Percentage
Written exam	
Coursework	100%
Practical	
TOTAL	100%

INDICATIVE READING LIST

Module Code	ACCA7027	
Module Title	Cloud Engineering Principles and Practice	
Classification	Reading List entry	Electronic*

Essential	Kane, S.P., Matthias, K., (2018) Docker: Up & Running: Shipping Reliable Containers in Production, O'Reilly Media	☒
Essential	Laszewski, T., Arora, K., Farr, E., Zonooz, P., (2018) Cloud Native Architectures: Design high-availability and cost-effective applications for the cloud. Packt Publishing	☒
Essential	Perkins, L., Redmond, E., Wilson, J., (2018) Seven Databases in Seven Weeks: A Guide to Modern Databases and the NoSQL Movement, Second Edition. Pragmatic Bookshelf	☒
Further	Burns, B., Beda, J., Hightower, K., (2019) Kubernetes: Up and Running: Dive into the Future of Infrastructure, O'Reilly Media	☒
Further	Bradshaw, S., Brazil, E., Chodorow, K., (2019) MongoDB: The Definitive Guide: Powerful and Scalable Data Storage, O'Reilly Media	☒
Further	Sarkar, A., Shah, A., (2018) Learning AWS, Second Edition. Packt Publishing	☒
Further	Ganesan, K., Skaria, R., Vos, F., (2020) Hands-On Linux Administration on Azure: Develop, maintain, and automate applications on the Azure cloud platform. Packt Publishing	☒
Further	Morris, K., (2016) Infrastructure as Code: Managing Servers in the Cloud. O'Reilly Media	☒

Module Code	ACCA7028
Title	Data Security, Governance and Compliance
Date	31/07/2020
Level	7
Credits	20
Pre-Requisites	

AIM(S)

- To provide students with sound principles of information systems security, governance and compliance for organisation goals and objectives. They must learn how to support, manage and make effective use of Information Technology (IT) frameworks, models, new regulations and standards of good practice for security management. Student must be able to assess and recognises emerging threats and vulnerability present in existing systems.

LEARNING OUTCOMES

Upon the successful completion of this module, the student should be able to:

- Demonstrate a systematic understanding of a wide range of current research and technological advances in data security, governance and compliance.
- Consistently apply the principles and practices of data security with skills and experiences to administer and manage the more secure information and communications technology environment that organisations need.

INDICATIVE CONTENT

- Introduction to Management of Information Security.
- The need for Security.
- Compliance: Law and Ethics.
- Governance and Strategic Planning for Security.
- Security Management Models.
- Security Management Practices.
- Planning for Contingencies.
- Information Security Policy.
- Developing the Security Program.
- Risk Management: Identifying and Assessing Risk.
- Risk Management: Controlling Risk.
- Security Maintenance and the Management of Digital Forensics.
- Protection Mechanisms.
- Cryptography.
- Physical Security.
- Implementing Information Security.
- Security and Personnel.
- Information Security Maintenance.
- Intrusion Detection, Prevention Systems and Other Security Technology.
- Access Controls, Firewalls and VPNs.

Study Time Allocation

The study time for the module is divided as follows:

Activity type	Hours	Percentage
Scheduled learning	48	24%

Independent learning	152	76%
Placement learning	0	0%
TOTAL	200	100%

ASSESSMENT

Assessment Component 1

☒ **Written exam** ☐ **Coursework** ☐ **Practical**

Mode of assessment	Volume	Weighting
Exam	2 hours	50%

Assessment Component 2

☐ **Written exam** ☒ **Coursework** ☐ **Practical**

Mode of assessment	Volume	Weighting
Written Report	3,000 words	50%

Assessment Summary

Activity type	Percentage
Written exam	50%
Coursework	50%
Practical	
TOTAL	100%

INDICATIVE READING LIST

Module Code	ACCA7028	
Module Title	Data Security, Governance and Compliance	
Classification	Reading List entry	Electronic*
Essential	Management of Information Security 6th Ed by Michael E Whitman, Herbert	☒
Essential	Principles of Information Security 6th Ed by Michael E. Whitman	☒
Further	The Management of Network Security, Technology, Design and Management Control, by Houston, H. Carr, Charles A. SNYDER and Bliss N. Bailey	☐
Further	Cryptography and Network Security: Principles and Practice, Global Edition, 7/E William Stallings	☐
Further	Network Security Essentials: Applications and Standards, Global Edition, 6/E William Stallings	☐
Further	Fundamentals of Information Systems Security, by David Kim and Michael G. Solomon	☐
Further	IEEE/ACM, IEEE/ACM Transactions on Networking	☒
Further	IEEE, IEEE Network Magazine	☒
Further	Science Direct	☒
Module Code	ACCA7031	

Title	Digital Forensics Analysis
Date	25/04/2023
Level	7
Credits	20
Pre-Requisites	None

AIM(S)

- To establish concepts relating to essential procedures and corresponding techniques involved in computer forensics process, in correlation to real-world scenarios.
- Students will gain understanding of the process of finding evidence related to a digital crime to find the culprits and initiate legal action against them. They will understand the methodological procedures and techniques using up-to-date tools that will allow them to facilitate assessments and technical approaches that are necessary to analyse and mitigate risks, threats, vulnerabilities and attacks relating to cyber incidents which could occur across various industries.

LEARNING OUTCOMES

Upon the successful completion of this module, the student should be able to:

- provide a systematic understanding of a wide range of current research and technological advances in digital and cyber security incidents and defensive techniques;
- perform computer forensics, to assess, investigate and analyse digital and cyber security crimes of an organisation with effective usage of security tools and methodologies.

INDICATIVE CONTENT

- Incident Response and Handling Process including but not limited to:
 - Cyber Kill Chain & Threat Intelligence.
 - Security Auditing & Policies.
 - Role of SOC in Incident Response.
- Forensic Science – Procedures and Methodology.
- Computer and digital Forensics Investigation Process.
- The investigation process includes but not limited to:
 - Searching and Seizing Computers.
 - Presenting Digital Evidence.
 - First Responder Procedures.
 - Understanding Hard Disks and File Systems.
 - Data Acquisition and Duplication.
 - Defeating Anti-Forensics Techniques.
 - Recovering Deleted Files and Deleted Partitions.
 - Operating System Forensics.
 - Network Forensics.
 - Investigating web attacks.
 - Database Forensics.
 - Cloud Forensics.
 - Malware Forensics.
 - Investigating Email Crimes.
 - Mobile Forensics.
 - Information Security and Forensic Tools.
- Forensics Report Writing and Presentation.

Study Time Allocation

The study time for the module is divided as follows:

Activity type	Hours	Percentage
Scheduled learning	48	24%
Independent learning	152	76%
Placement learning	0	0%
TOTAL	200	100%

ASSESSMENT

Assessment Component 1

(Tick one)

☐ Written exam ☒ Coursework ☐ Practical

Mode of assessment	Volume	Weighting
Report	5000 words	100%

Assessment Summary

Activity type	Percentage
Written exam	0%
Coursework	100%
Practical	0%
TOTAL	100%

INDICATIVE READING LIST

Module Code	ACCA7031	
Module Title	Digital Forensics Analysis	
Classification	Reading List entry	Electronic*
Essential	Essential Sachowski, J. (2021). <i>Digital Forensics and Investigations</i> . 2nd Edition. CRC Press.	☒
Essential	Chuck, W. (2021). <i>Penetration Testing Fundamentals</i> . 2nd Edition. Pearson IT Certification.	☒
Further	Blunden, B. (2014). <i>The Rootkit arsenal: escape and evasion in the dark corners of the system</i> . 2nd Edition. Burlington, Ma Jones & Bartlett Learning.	☒
Further	Pfleeger, C. P., Pfleeger, S. L., & Margulies, J. (2015). <i>Analyzing computer security: a threat / vulnerability / countermeasure approach</i> . 3rd Edition. Prentice Hall.	☒
Further	Johansen, G. (2021). <i>Digital Forensics and Incident Response: An intelligent way to respond to attacks</i> . 2nd Edition. Packt Publishing Limited.	☐
Further	Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2019). <i>Cybercrime and Digital Forensics: An Introduction</i> . 3rd Edition. Routledge.	☒
Further	Gogolin, G., Ciaramitaro, B. L., Emerick, G., Otting, J., & Pavlov, V. (2017). <i>Digital forensics explained</i> . 2nd Edition. Boca Raton, FL: CRC Press.	☒

Further	IEEE Transactions on Computers. (2021). IEEE Security & Privacy, 19(1)	☒
Online	OWASP Foundation. (n.d.). Open Web Application Security Project (OWASP). [online] Available at: https://owasp.org/ .	☒
Online	EC-Council. (n.d.). Computer Hacking Forensic Investigator (CHFI). Retrieved from https://www.eccouncil.org/programs/computer-hacking-forensic-investigator/	
Online	Online IEEE Transactions on Information Forensics and Security. (2023). IEEE Xplore. [online] Available at: https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=10206 [Accessed 22 Mar. 2023].	☒
Online	Online ACM Digital Library. (n.d.). [online] Available at: https://dl.acm.org/ .	☒
Online	Elsevier. (2023). ScienceDirect.com Science, Health and Medical journals, Full Text Articles and books. [online] Available at: https://www.sciencedirect.com/ .	☒
Online	TryHackMe.com https://www.eccouncil.org/ https://aspen.eccouncil.org/ https://codered.eccouncil.org/?utm_source=aspen&utm_medium=header&utm_campaign=navigation&logged=false	☒

Module Code	ACCA7032
Title	Enterprise Network Security
Date	25/04/2023
Level	7
Credits	20
Pre-Requisites	None

AIM(S)

- To provide students with an appreciation of information security concepts and a deep understanding of how they are applied using Internet technologies. Students will gain a thorough understanding of up-to-date security threats posed to networks and an understanding of the legal, policy and technical approaches that are necessary to mitigate such risks.

LEARNING OUTCOMES

Upon the successful completion of this module, the student should be able to:

- demonstrate a systematic understanding of a wide range of current research and technological advances in network security underpinning the key elements of unified security management architecture in managing and monitoring network traffic;
- apply the principles and practices of network security for mitigating the key technical security vulnerabilities that organisations face and gain insight on how security features are enabled, and policies applied.

INDICATIVE CONTENT

- Current and emerging security related web-based technologies e.g. Intranet, ecommerce.
- Use of the Security Policy and Security Management in an organisation eg roles and responsibilities, security policies.
- Cryptography and Digital Identification: PKI, Signatures, Certificates.
- Security: Web Server, Operating System, Wireless, Mobile.
- Firewalls and their architectures:
 - Policy Layers.
 - Application Control & URL Filtering.
 - Managing User Access.
 - Network Address Translation.
 - Traffic Visibility.
 - Monitoring System States.
 - Threat Prevention.
- Virtual Private Networks (VPNs) concepts.
- Implementing Defence-in-Depth strategies: eg tools for scanning system weaknesses.
- The future of Information Security eg m-commerce, ID theft, biometrics, blockchain.

Study Time Allocation

The study time for the module is divided as follows:

Activity type	Hours	Percentage
Scheduled learning	48	24%
Independent learning	152	76%

Placement learning	0	0%
TOTAL	200	100%

ASSESSMENT

Assessment Component 1

(Tick one)

☐ Written exam ☒ Coursework ☐ Practical

Mode of assessment	Volume	Weighting
Portfolio (eg CBT, Written Report, Implementation and/or Presentation)	3 elements or equivalent. Students will produce a portfolio of work. Portfolio elements may include a selection of the following: ○ Computer Based Test ○ Written Report ○ Implementation ○ Demonstration of their work e.g. written or presentation	100%

Assessment Summary

Activity type	Percentage
Written exam	0%
Coursework	100%
Practical	0%
TOTAL	100%

INDICATIVE READING LIST

Module Code	ACCA7032	
Module Title	Enterprise Network Security	
Classification	Reading List entry	Electronic*
Essential	Stallings, W. (2022). <i>Cryptography and network security 8th Edition</i> . Pearson	☒
Essential	Yakovlev, V. and Welch, D.D. (2022). <i>Check Point Firewall Administration R81.10+</i> . Packt Publishing Ltd.	☒
Further	Stallings, W. (2016). <i>Network Security Essentials: Applications and Standards</i> . Boston: Pearson Education, Inc.	☒
Further	Brotherston, L. and Berlin, A. (2017). <i>Defensive Security Handbook</i> . O'Reilly Media, Inc.'	☒
Further	Sanders, C. and Smith, J. (2014). <i>Applied network security monitoring: collection, detection, and analysis</i> . Amsterdam; Boston: Syngress, An Imprint of Elsevier.	☒
Further	Manuj Aggarwal (2018). <i>Network security with pfSense: architect, deploy, and operate enterprise-grade firewalls</i> . Birmingham, Uk: Packt Publishing.	☒
Further	Hooper, H. (2012). <i>CCNP Security VPN 642-648 Official Cert Guide</i> . Cisco Press.	☒
Further	Gilman, E. and Barth, D. (2017). <i>Zero trust networks: building secure systems in untrusted networks</i> . Sebastopol, CA: O'Reilly Media.	☒

Further	Karame, G. and Androulaki, E. (2016). <i>Bitcoin and blockchain security</i> . Norwood, MA: Artech House.	☒
Further	Elad Elrom and Springerlink (Online Service (2019). <i>The Blockchain Developer: A Practical Guide for Designing, Implementing, Publishing, Testing, and Securing Distributed Blockchain-based Projects</i> . Berkeley, Ca: Apress.	☒

Module Code	ACCA7033
Title	Ethical Hacking
Date	25/04/2023
Level	7
Credits	20
Pre-Requisites	None

AIM(S)

- To establish concepts relating to the understanding of how malicious hackers attack and exploit systems. This includes essential procedures and corresponding techniques involved in ethical hacking activities, in correlation to real-world scenarios. Students will gain understanding of security threats, information security, vulnerability, penetration testing procedures and methodologies using up-to-date tools that will allow them to facilitate assessments and technical approaches that are necessary to analyse and mitigate risks, threats, vulnerabilities and attacks across various industries.

LEARNING OUTCOMES

Upon the successful completion of this module, the student should be able to:

- provide a systematic understanding of a wide range of current research and technological advances in cyber security incidents;
- perform information security assessments, investigate, analyse, and support cyber security activities of an organisation with effective usage of security tools and methodologies.

INDICATIVE CONTENT

- Security Threats, Attack Vectors and Defense Technologies included but not limited to:
 - Elements of Information Security (CIA Triad, Defense in Depth, IDS, etc.).
 - Cryptography.
 - Malware Threats.
 - Threats to Hosts, Networks and Web Applications.
 - Mobile platform.
 - Internet of Things (IoT).
- Security Assessment – Processes and Methodologies included but not limited to:
 - Open-Source Intelligence (OSINT).
 - Social Engineering Campaigns.
 - Network Penetration Testing.
 - Web Application Penetration Testing.
 - Mobile Penetration Testing.
 - Wireless Penetration Testing.

Study Time Allocation

The study time for the module is divided as follows:

Activity type	Hours	Percentage
Scheduled learning	48	24%
Independent learning	152	76%
Placement learning	0	0%
TOTAL	200	100%

ASSESSMENT

Assessment Component 1

(Tick one)

☐ Written exam ☒ Coursework ☐ Practical

Mode of assessment	Volume	Weighting
Report	5000 words	100%

Assessment Summary

Activity type	Percentage
Written exam	0%
Coursework	100%
Practical	0%
TOTAL	100%

INDICATIVE READING LIST

Module Code	ACCA7033	
Module Title	Ethical Hacking	
Classification	Reading List entry	Electronic*
Essential	Diogenes, Y. and Erdal Ozkaya (2019). <i>Cybersecurity - Attack and Defense Strategies; Counter Modern Threats and Employ State-Of-The-Art Tools and Techniques To Protect your Organization against cybercriminals</i> . Packt Publishing	☒
Essential	Whitman, M.E. and Mattord, H.J. (2022). <i>Principles of information security</i> . Boston, Ma: Cengage.	☒
Essential	Rafay Baloch (2017). <i>Ethical hacking and penetration testing guide</i> . Boca Raton: Auerbach Publications.	☒
Further	Blunden, B. (2016). <i>The Rootkit arsenal: escape and evasion in the dark corners of the system</i> . Burlington, Ma Jones & Bartlett Learning.	☒
Further	McClure, S., Scambray, J. and Kurtz, G. (2012). <i>Hacking exposed: network security secrets and solutions</i> . Emeryville, Calif.: McGraw-Hill/Osborne; London.	☒
Further	Charles Paul Pfleeger and Shari Lawrence Pfleeger (2012). <i>Analyzing computer security: a threat/vulnerability/countermeasure approach</i> . Upper Saddle River, New Jersey; Toronto: Prentice Hall.	☒
Further	Tadayoshi Kohno, Niels Ferguson and Schneier, B. (2010). <i>Cryptography engineering: design principles and practical applications</i> . Indianapolis, In: Wiley Pub., Inc.	☒
Further	Niels Provos and Holz, T. (2007). <i>Virtual Honeypots</i> . Pearson Education.	☒
Further	Bejtlich, R. (2010). <i>The Tao of network security monitoring: beyond intrusion detection</i> . Boston: Addison-Wesley.	☒

Further	IEEE Transactions on Computers. (2020). <i>IEEE Security & Privacy</i> , 18(1), pp.7–7.	
Online	owasp.org. (n.d.). <i>OWASP Foundation Open-Source Foundation for Application Security</i> . [online] Available at: http://owasp.org .	☒
Online	EC-Council. (n.d.). Certified Ethical Hacker (CEH). Retrieved from https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/	
Online	www.acm.org. (n.d.). <i>ACM Digital Library</i> . [online] Available at: https://www.acm.org/publications/digital-library	☒
Online	Elsevier (2022). <i>ScienceDirect.com Science, Health and Medical journals, Full Text Articles and books</i> . [online] Sciencedirect.com. Available at: https://www.sciencedirect.com/ .	☒

Module Code	ACFA7003
Title	Masters Project
Date	11/04/2019
Level	7
Credits	60
Pre-Requisites	None

AIM(S)

- To allow the student to advance their knowledge and understanding by undertaking and managing a significant project of their own choice, related to the major themes of their MSc programme.

LEARNING OUTCOMES

Upon the successful completion of this module, the student should be able to:

- critically identify and develop an advanced research topic
- review appropriate literature by contextualising and integrating the study into the continuing development of knowledge and understanding of chosen research topic
- critically formulate a series of research objectives and devise strategies to support these
- demonstrate and display advanced critical, analytic and creative thinking
- demonstrate advanced professional skills to present information both orally and in a written form

INDICATIVE CONTENT

The Masters Project is an essential part of the degree; it is the culmination of the Masters programme. As such, it has been designed and conceived as an integral part of the programme. Preparation for the Masters Project begins early in the programme, and students acquire analytical and other research skills throughout part 1. This underpins and enhances the student's ability to undertake research.

- Formulation and rationale for suitable post-graduate research objectives
- Application of an appropriate methodology for the investigation.
- Collation and communication - recording and organising information, analysis of results, communicating the results, referencing, plagiarism.
- Critical review of appropriate literature within a conceptual/theoretical framework.
- Determination of research results.
- Critical appraisal of the results/solutions of the investigation.
- Project planning - project time scale control
- Oral/visual critique and presentation of the results of the investigation.
- Written and verbal critique of the research
- Intellectual property - copyright, trademarks, patents.
- Social and cultural context, and ethical issues
- Intellectual property - copyright, trademarks, patents.
- Social and cultural context, and ethical issues

Study Time Allocation

The study time for the module is divided as follows:

Activity type	Hours	Percentage
----------------------	--------------	-------------------

Scheduled learning	15	2.5%
Independent learning	585	97.5%
Placement learning	0	0%
TOTAL	600	100%

ASSESSMENT

Assessment Component 1

☐	Written exam	☒	Coursework	☐	Practical
--------------------------	---------------------	-------------------------------------	-------------------	--------------------------	------------------

Mode of assessment	Volume	Weighting
Masters Project	15,000 words equivalent Students will produce a research portfolio of work appropriate to the nature of their project. This will vary slightly according to the nature of the project undertaken. Portfolio elements may include a selection of the following, to be agreed with the external examiner: • Written Report (all students) • Exhibition Board (all students) • Presentation slides • Hardware and/or software implementation	80%

Assessment Component 2

☐	Written exam	☐	Coursework	☒	Practical
--------------------------	---------------------	--------------------------	-------------------	-------------------------------------	------------------

Mode of assessment	Volume	Weighting
Viva voce	15 mins (before questions)	20%

Assessment Summary

Activity type	Percentage
Written exam	0%
Coursework	80%
Practical	20%
TOTAL	100%

INDICATIVE READING LIST

Module Code	ACFA7003	
Module Title	Masters Project	
Classification	Reading List entry	Electronic *
Essential	McCormac, C. and Davis, J. (2015) <i>Research Project Success: The Essential Guide for Science</i>	☒

	<i>and Engineering Students</i> , Cambridge: Royal Society of Chemistry	
Essential	Greenfield, T. (2016) <i>Research Methods for Postgraduates</i> , London: Arnold	☒
Essential	Cottrell, S. (2011) <i>Critical Thinking Skills: Developing Effective Analysis and Argument - Palgrave Study Guides, 2nd Edition</i> , London: Palgrave Macmillan	☒
Essential	Cottrell, S. <i>Dissertations and Project Reports: A Step by Step Guide</i> (Palgrave Study Skills, 2014)	☒
Essential	O'Leary, Z. (2013) <i>Doing Your Research Project (2nd Edition)</i> , SAGE Publications Ltd	☒
Further	O'Leary, Z. (2015) <i>The Essential Guide to Doing Your Research Project</i> , Newcastle upon Tyne: Sage	☒
Further	Kranzler, J. H. (2017) <i>Statistics for the Terrified</i> , Upper Saddle River: Prentice Hall	☒
Further	Dawson, C. W. (2009) <i>Projects in Computing and Information Systems: a Student's Guide, 2nd Edition</i> , Boston: Addison-Wesley	☒
Further	Dipankar, D. (2019) <i>Engineering Research Methodology: A Practical Insight for Researchers</i> . Springer	☐
Further	Fellows, R. and Liu, A. <i>Research Methods for Construction</i> (Blackwell Oxford, 2015)	☐
Further	Few, S. (2012) <i>Show Me the Numbers</i> , Burlingame: Analytics Press	☒
Further	Hughes, B. and Cotterell, M. (2009) <i>5th Software Project Management</i> , New York: McGraw-Hill	☐
Further	Phillips, J. (2010) <i>IT Project Management: On Track from Start to Finish</i> , New York: McGraw-Hill	☐
Further	Gregoire, T.G. & Valentine, H.T. (2008) <i>Sampling strategies for natural resources and the environment</i> . Chapman, London	☐
Further	Baase, S. (2012) <i>A Gift of Fire: Social, Legal, and Ethical Issues for Computing and the Internet: International Edition, 4th Edition</i> , Boston: Pearson	☐
Further	Collis, J. and Hussey, R. (2009) <i>Business Research: a Practical Guide for Undergraduate and Postgraduate Students</i> , 3rd Edition, London: Palgrave Macmillan	☐
Further	Cottrell, S. (2011) <i>Critical Thinking Skills: Developing Effective Analysis and Argument - Palgrave Study Guides, 2nd Edition</i> , London: Palgrave Macmillan	☐
Further	Davies, M. B. (2007) <i>Doing a Successful Research Project</i> , London: Palgrave Macmillan	☐
Further	Dawson, C. W. (2009) <i>Projects in Computing and Information Systems: a Student's Guide</i> , 2nd Edition, Boston: Addison-Wesley	☐
Further	Hewson, C. , Vogel, C. & Laurent, D. (2015) <i>Internet research methods</i> . Sage: London.	☐

Further	Few, S. (2012) Show Me the Numbers: Designing Tables and Graphs to Enlighten, Burlingame: Analytics Press	☐
Further	Quinn, M. J. (2010) Ethics for the Information Age: International Edition - 4th Edition, Boston: Pearson	☐
Further	Yin, R. K. (2008) Case Study Research: Design and Methods, 4th Edition, Newcastle upon Tyne: Sage	☐
Further	Spence, R. (2014) <i>Information Visualization: an Introduction</i> , Boston: Addison-Wesley	☐
Further	Thiel, D.V. (2014) Research methods for engineers. Cambridge UP	☒
Further	Wheater, C.P. & Cook, P.A. (2015) Using statistics to understand the environment Routledge	☐
Further	Journals ACM Transactions on Information Systems Behaviour and Information Technology Communications on the ACM International Journal of Electronic Commerce Journal of Strategic Information Systems Journal of Systems Management	☒
Further	Websites http://www.acm.org http://www.bized.co.uk http://www.managers.org.uk http://www.cbronline.com http://www.eevl.ac.uk http://juno.emeraldinsight.com http://www.ft.chadwyck.co.uk http://www.itwales.com http://www3.gartner.com http://www.silicon.com http://www.mckinseyquarterly.com http://www.zdnetweek.co.uk http://projectmanagement.ittoolbox.com/ http://www.ics.ltsn.ac.uk/resources/projman/index.html http://www.niwotridge.com/Resources/PM-SWEResources/PMResources.htm http://www.tickit.org/international.htm http://www.bcs.org/ http://www.uml.org/ http://www.omg.org/	☒

Module Code	ACFA7004
Title	Research Methods and Professional Development
Date	11/04/2019
Level	7
Credits	20
Pre-Requisites	None

AIM(S)

- The aim of this module is for students to develop a problem solving approach to research to facilitate their production of a valid and reliable postgraduate dissertation.

LEARNING OUTCOMES

Upon the successful completion of this module, the student should be able to:

- Generate a project proposal that meets a given domain research requirements.
- Identify and visualise a complex research problem within a specific research domain, outline the investigative approach and comprehensively consider appropriate methods and solutions.
- Critically appraise the research process and its outcomes.

INDICATIVE CONTENT

- Core lectures on the principles of postgraduate research :
 - Research principles and approaches (e.g. the research process, purpose, sources of data including primary/secondary research, quantitative/qualitative data, objective/hypothesis formation, reliability, validity)
 - Research methodologies - historical, descriptive, correlational, comparative, experimental
 - Field data - survey design, questionnaires, sampling, statistical techniques, interviews, case studies, observation
 - Developing a proposal - research statement, research outline and design research schedule
 - Project planning - project time scale control
 - Intellectual property - copyright, trademarks, patents
 - Social and cultural context, and ethical considerations
- Writing up and publishing
- Domain specific research methods:
 - Research for engineering
 - Project planning for computing
 - Advanced Quantitative research methods
 - Advanced Qualitative research methods

Study Time Allocation

The study time for the module is divided as follows:

Activity type	Hours	Percentage
Scheduled learning	48	24%
Independent learning	152	76%
Placement learning	0	0%
TOTAL	200	100%

ASSESSMENT

Assessment Component 1

☐ Written exam ☒ Coursework ☐ Practical

Mode of assessment	Volume	Weighting
Research Proposal	4,000 words	70%

Assessment Component 2

☐ Written exam ☐ Coursework ☒ Practical

Mode of assessment	Volume	Weighting
Presentation	10 mins (plus questions)	30%

Assessment Summary

Activity type	Percentage
Written exam	0%
Coursework	70%
Practical	30%
TOTAL	100%

INDICATIVE READING LIST

Module Code	ACFA7004	
Module Title	Research Methods and Professional Development	
Classification	Reading List entry	Electronic*
Essential	Cottrell, S. (2011) Critical Thinking Skills: Developing Effective Analysis and Argument - Palgrave Study Guides, 2 nd Edition, London: Palgrave Macmillan	☒
Essential	Cottrell, S. (2014) Dissertations and Project Reports: A Step by Step Guide, Palgrave Study Skills	☒
Essential	O'Leary, Z. (2013) Doing Your Research Project (2 nd Edition), SAGE Publications Ltd	☒
Further	Dawson, C. W. (2009) Projects in Computing and Information Systems: a Student's Guide, 2 nd Edition, Boston: Addison-Wesley	☒
Further	Dipankar, D. (2019) Engineering Research Methodology: A Practical Insight for Researchers. Springer	☐
Further	Fellows, R. and Liu, A. (2015) Research Methods for Construction, Oxford: Blackwell	
Further	Few, S. (2012) Show Me the Numbers, Burlingame: Analytics Press	☐

Further	Gregoire, T.G. & Valentine, H.T. (2008) Sampling strategies for natural resources and the environment. London : Chapman	☐
Further	Hart, C. (1998) Doing a Literature Review, Sage	☒
Further	Hewson, C., Vogel, C. & Laurent, D. (2015) Internet research methods. London: Sage	☐
Further	Kranzler, J. H. (2011) Statistics for the Terrified, 5 th Edition, Upper Saddle River: Prentice Hall	☐
Further	Leedy. P. D. and Ormrod, J. E. (2012) Practical Research Planning and Design, 10 th Edition, Boston: Pearson Education	☒
Further	Maylor, H. (2010) Project Management, Boston: Pearson Education	☐
Further	Oppenheim, A. (1992) Questionnaire Design, Interviewing and Attitude Measurement, London: Continuum	☒
Further	Spence, R. (2014) Information Visualization: an Introduction, Boston: Addison-Wesley	
Further	Thiel, D.V. (2014) Research Methods for Engineers. Cambridge UP	☒
Further	Wheater, C.P. & Cook, P.A. (2015) Using Statistics to Understand the Environment, Routledge	☒

