H9IACS: Information Assurance and Cybersecurity

Module Code:	H9IACS
Long Title	Information Assurance and Cybersecurity APPROVED
Title	Information Assurance and Cybersecurity
Module Level:	LEVEL 9
EQF Level:	7
EHEA Level:	Second Cycle
Credits:	5
Module Coordinator:	Simon Caton
Module Author:	Simon Caton
Departments:	School of Computing
Specifications of the qualifications and experience required of staff	

Learning Outcomes	
On successful completion of this module the learner will be able to:	
#	**Learning Outcome Description**
LO1	Investigate the requirements to ensure confidentiality, integrity and availability of information and systems
LO2	Critically assess and evaluate the key data lifecycle stages and reliance on these for effective information governance in real-world settings
LO3	Critically appraise, and instrument key concepts of risk management and information technology resilience
LO4	Identify, assess, and combat key threats to information systems and data processing services
LO5	Review and discuss the research literature in the context of real-world information assurance and cybersecurity issues

Dependencies
Module Recommendations
No recommendations listed
Co-requisite Modules
No Co-requisite modules listed

Entry requirements	

H9IACS: Information Assurance and Cybersecurity

Module Content & Assessment

Indicative Content
Key Cybersecurity Concepts • Protection key assets including prioritization of people, processes and technology • Implementing and validating preventative, detective & corrective controls • Overview & applying security in Cloud Computing environments • Key components of a cyber security programme
Data Lifecycle Management • Key stages and components of Data Lifecycle Management • Regulatory & Privacy Components (including Data Protection Act) • Policies & Enforcement • Data Classification • Information Governance Reporting
Risk Assessment & Risk Management • Key Risks Management Components (e.g., ability to assess and measure risks) • Risk Mitigation Techniques (e.g., reduce / mitigate, transfer, accept, etc.) • Cost Benefit Analysis
Threats to Information & Data Processing Services • Understand the threat landscape • Typical Attack Methods and Threat Actors / Vectors • Impact of cyber-attacks and data breaches • Executive interactions and reporting

Assessment Breakdown	%
Coursework	60.00%
End of Module Assessment	40.00%

Assessments

Full Time

Coursework

Assessment Type:	Continuous Assessment	**% of total:**	60
Assessment Date:	n/a	**Outcome addressed:**	2,3,4,5
Non-Marked:	No		

Assessment Description:
Learners will undertake a series (2-4) of literature-based as well as practically focused (project work) case studies.

End of Module Assessment

Assessment Type:	Terminal Exam	**% of total:**	40
Assessment Date:	End-of-Semester	**Outcome addressed:**	1,2,3,4
Non-Marked:	No		

Assessment Description:
The examination will be a minimum of two hours in duration and may include a mix of: short answer questions, vignettes, essay based questions and case study based questions. Marks will be awarded based on clarity, appropriate structure, relevant examples, depth of topic knowledge, and evidence of outside core text reading.

No Workplace Assessment

Reassessment Requirement

Repeat examination
Reassessment of this module will consist of a repeat examination. It is possible that there will also be a requirement to be reassessed in a coursework element.

H9IACS: Information Assurance and Cybersecurity

Module Workload

Module Target Workload Hours 0 Hours

Workload: Full Time

Workload Type	*Workload Description*	*Hours*	*Frequency*	*Average Weekly Learner Workload*
Lecture	No Description	24	Every Week	24.00
Tutorial	No Description	12	Every Week	12.00
Independent Learning Time	No Description	89	Every Week	89.00
			Total Weekly Contact Hours	36.00

Workload: Part Time

Workload Type	*Workload Description*	*Hours*	*Frequency*	*Average Weekly Learner Workload*
Lecture	No Description	24	Every Week	24.00
Tutorial	No Description	12	Every Week	12.00
Independent Learning Time	No Description	89	Every Week	89.00
			Total Weekly Contact Hours	36.00

Module Resources

Recommended Book Resources

Jason Andress. The Basics of Information Security, 2. Syngress, p.208, [ISBN: 9781597496537].

Corey Schou, Steven Hernandez ; technical editors, Flemming Faber, Jill Slay.. Information assurance handbook, 1. ; McGraw-Hill Education, [ISBN: 9780071821650].

Carstensen, Jared, Bernard Golden and JP Morgenthal. (2012), Cloud Computing - Assessing the Risks., IT Governance Publishing, [ISBN: 9781849283595].

This module does not have any article/paper resources

This module does not have any other resources

Discussion Note:	