H9CS: Cloud Security

Module Code:	H9CS
Long Title	Cloud Security AWAITING MODULE COORDINATOR
Title	Cloud Security
Module Level:	LEVEL 9
EQF Level:	7
EHEA Level:	Second Cycle
Credits:	10
Module Coordinator:	Mikhail Timofeev
Module Author:	MICHAEL BRADFORD
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	Critically review computing systems security principles in order to assess how these principles relate to cloud computing environments.
LO2	Investigate and analyse in-depth the security challenges associated with cloud deployment models and cloud delivery models in order to evaluate and devise strategies for securing cloud-based systems.
LO3	Recommend and evaluate solutions to detect, mitigate and prevent security breaches to cloud-based systems.
LO4	Evaluate and assess security management models in order to develop security policies and processes that can be utilised to protect the integrity of cloud-based systems.

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

Entry requirements	

H9CS: Cloud Security

Module Content & Assessment

Indicative Content

Cloud Computing Concepts
• Explore cloud computing architecture: cloud computing definition, essential characteristics, service models, deployment models, cloud foundational elements/enablers • Investigate and critically assess the concept of Multi-tenancy • Analyse and assess the levels of Security Control for SPI Model • Evaluate the security benefits of cloud computing

Cloud Security Concepts
• Investigate the Security Fundamentals (i.e. CIA Security Triad, Defence in Depth, AAAs of Security, Non-repudiation, Least Privilege, Separation of Duties, Due Diligence, etc.) • Identify and investigate Top Security Risks (i.e. Loss of Governance, Lock-In, Isolation Failure, Compliance Risks, Management Interface Compromise, Data Protection, Insecure or Incomplete Data Deletion, Malicious insider, etc.) • Explore various security architectures (i.e. TOGAF, SSE-CMM, etc.) and reference models (i.e. CSA TCI, Cloud Cube Model, etc.) • Compare and contrast various threat models (i.e. STRIDE, DREAD, etc.) • Investigate security assurance (i.e. CSA STAR initiative, ENISA Information Assurance Framework, etc.)

IaaS Security
• Assess IaaS Security Concerns • Explore the concept of Virtualisation • Analyse and assess Hypervisor architecture concerns • Assess the challenges associated with protecting data in IaaS (i.e. Information Architectures for IaaS, IaaS Encryption) • Investigate portability and interoperability in IaaS (i.e. Lock-In) • Appraise security in cloud environments with multi-tenancy at an Infrastructure level and testing in IaaS • Assess the challenges associated with protecting applications in IaaS • Explore how applications can be monitored in IaaS

PaaS Security
• Assess the challenges associated with protecting data in PaaS (i.e. Information Architectures for PaaS, PaaS Encryption) • Investigate portability and Interoperability in PaaS (i.e. Lock-in) • Appraise security in cloud environments with multi-tenancy at a platform level and testing in PaaS • Assess the challenges associated with protecting applications in PaaS • Explore how applications can be monitored in PaaS

SaaS Security
• Assess the challenges associated with protecting data in SaaS (i.e. Information Architectures for PaaS, PaaS Encryption) • Investigate portability and Interoperability in SaaS • Appraise security in cloud environments with multi-tenancy at a software level and testing in SaaS • Assess the challenges associated with protecting applications in SaaS • Explore how applications can be monitored in SaaS • Investigate and assess the impact of client-side vulnerabilities and mobile devices on cloud application security (XSS and CSRF) • Secure coding principles

Identity and Access Management (IAM)
• Assess identity federation and claims-based security services with respect to cloud based systems (e.g., SAML, OpenID and OAuth) • Evaluation of IAM provider types (e.g., Silo-based Identity Providers, Replicated Identity Providers) • Investigate risk-based authentication strategies for cloud applications (e.g., authentication based on geo-location, device identifier etc.)

Intrusion Detection and Incident Response
• Assess the challenges associated with establishing security perimeters within cloud computing environments (e.g. the impact of mobile devices on extending the attack surface of cloud based systems) • Investigate and assess a range of attack vectors that may be encountered on cloud based environments (e.g. Cryptanalysis, Impersonation, Social Engineering, DNS Mis-directions, DDoS, Brute Force) • Assess the challenges associated with monitoring and logging within cloud computing systems • Determine how to identify security breaches, detect intrusions (e.g. honey pots) and recommend responses to such incidents (e.g. containment)

Information Management and Data Security
• Analyse and assess data dispersion in cloud environments • Compare and contrast the Data Security Lifecycle and Information Lifecycle Management • Analyse and assess information security governance processes • Assess the challenges associated with protecting data in a cloud (i.e. Detecting and Preventing Data Migrations to the Cloud, Protecting Data Moving To and within the Cloud, Content Discovery, Data Loss Prevention, Database and File Activity Monitoring, Privacy Preserving Storage, Digital Rights Management)

Encryption and Key Management
• Evaluate and assess means of cryptographic protection of data in storage, data in transmission and data in an application environment • Appraise data security in multi-tenancy environments • Compare and contrast symmetric and asymmetric cryptosystems and analyse how these cryptosystems can be implemented to provide data security in the cloud • Evaluate and recommend strategies for implementing key management infrastructure solutions. • Investigate network encryption techniques

Disaster Recovery and Business Continuity
• Assess Cloud Service Provider capabilities and responsibilities with respect to business continuity and disaster recovery • Investigation of the opportunities afforded by cloud storage for backup and disaster recovery • Devise strategies for testing disaster recovery and business continuity processes and activities within cloud based environments

Security Management
• Cloud Governance, Risk and Compliance • Analyse and assess information security governance processes • Evaluate pertinent control frameworks and standards (e.g., ISO/IEC 27001-2) • Investigate and analyse Risk Assessment and Threat Models • Assess Information Assurance Frameworks in relation to meeting requirements for implementing secure cloud based computing environments • Analyse and recommend enterprise risk management approaches and techniques • Investigate the impact and importance of Service Level Agreements (SLAs) with respect to implementing cloud solutions

Legal and Compliance
Legal and regulatory requirements and challenges unique to cloud environment • Cloud Outsourcing • Analyse the legal and compliance challenges of migration, outsourcing management and exit strategies

Cloud Forensics
• Cloud Crime • Cloud Forensics dimensions and technical challenges • Cloud forensics tools and process • Analyse cloud forensics challenges and opportunities

Assessments

Full Time

Coursework

Assessment Type:	Project	**% of total:**	40
Assessment Date:	n/a	**Outcome addressed:**	2,3
Non-Marked:	No		

Assessment Description:
Learners are required to do a project where they would devise policies, strategies and recommendations for securing cloud based service offerings (e.g., an IaaS, PaaS or SaaS service). Learners may also be required to implement a security test plan to evaluate the effectiveness of security recommendations for cloud services in given contextual scenarios. The project may be team-based and use cross-module assessment, depending on learner's specialisation.

End of Module Assessment

Assessment Type:	Terminal Exam	**% of total:**	60
Assessment Date:	End-of-Semester	**Outcome addressed:**	1,4
Non-Marked:	No		

Assessment Description:
End-of-Semester final examination

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.

H9CS: Cloud Security

Module Workload

Module Target Workload Hours 0 Hours

Workload: Full Time

Workload Type	*Workload Description*	*Hours*	*Frequency*	*Average Weekly Learner Workload*
Lecture	No Description	2	Every Week	2.00
Practical	No Description	2	Every Week	2.00
Independent Learning Time	No Description	17	Once per semester	1.42
			Total Weekly Contact Hours	4.00

Workload: Part Time

Workload Type	*Workload Description*	*Hours*	*Frequency*	*Average Weekly Learner Workload*
Lecture	No Description	2	Every Week	2.00
Practical	No Description	2	Every Week	2.00
Independent Learning	No Description	17	Every Week	17.00
			Total Weekly Contact Hours	4.00

Module Resources

Recommended Book Resources

Malisow, B.. (2017), CCSP (ISC) 2 Certified Cloud Security Professional Official Study Guide, John Wiley & Sons.

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

Supplementary Book Resources

Rittinghouse, J.W. and Ransome, J.F.. (2016), Cloud computing: implementation, management, and security, CRC Press.

Anthony, A.. (2017), Mastering AWS Security: Create and maintain a secure cloud ecosystem, Packt Publishing.

Kunjal Trivedi and Keith Pasley. (2012), Cloud Computing Security,, Cisco Press.

Tim Mather, Subra Kumaraswamy, Shahed Latif. Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance, O'Reilly Media, Inc., [ISBN: 0596802765].

This module does not have any article/paper resources

Other Resources

[Website], Cloud Security Alliance. (2011), Cloud Security Alliance 2017, Security Guidance for Critical Areas of Focus in Cloud Computing V4.0, https://cloudsecurityalliance.org/artifa cts/security-guidance-v4/

[Website], OWASP Cloud – 10 Project, https://www.owasp.org/index.php/Category :OWASP_Cloud_%E2%80%90_10_Project

[Website], NIST Cloud Computing Program - NCCP, https://www.nist.gov/programs-projects/n ist-cloud-computing-program-nccp

[Website], Journal of Cloud Computing, https://journalofcloudcomputing.springer open.com/articles

[Website], International Journal of Cloud Computing,, http://www.inderscience.com/browse/index .php?journalCODE=ijcc

[Website], Future Generation Computer Systems,, http://www.journals.elsevier.com/future- generation-computer-systems/

[Website], Journal of Computer Security,, http://www.iospress.nl/journal/journal-o f-computer-security/

[Website], Computers and Security,, http://www.journals.elsevier.com/compute rs-and-security/

[Website], Computer Fraud and Security,, http://www.elsevier.com/journals/compute r-fraud-and-security/

[Website], Journal of Computer and System Sciences,, http://www.journals.elsevier.com/journal -of-computer-and-system-sciences/

[Website], Journal of Information Security and Applications,, http://www.journals.elsevier.com/journal -of-information-security-and-application s/

Discussion Note:	