H9CAS2: Cloud Architectures and Security

Module Code:	H9CAS2
Long Title	Cloud Architectures and Security APPROVED
Title	Cloud Architectures and Security
Module Level:	LEVEL 9
EQF Level:	7
EHEA Level:	Second Cycle
Credits:	10
Module Coordinator:	Arghir Moldovan
Module Author:	MICHAEL BRADFORD
Departments:	School of Computing
Specifications of the qualifications and experience required of staff	PhD/Master's degree in a computing or cognate discipline. May have industry experience also.

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	Critically analyse the security challenges associated with cloud-based systems in order to identify and evaluate candidate cloud security architectures and deployment strategies.
LO3	Recommend solutions to detect, mitigate and prevent security breaches to the cloud-based systems.
LO4	Appraise security management models in order to develop security policies and processes for protecting the integrity of cloud-based systems.

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

Entry requirements	Programme entry requirements must be satisfied.

H9CAS2: Cloud Architectures and Security

Module Content & Assessment

Indicative Content
Cloud Computing Concepts • Explore cloud computing architecture: cloud computing definition, essential characteristics, service models, deployment models. • Investigate and critically assess the concept of Multi-tenancy. • Analyse and assess the levels of Security Control for SPI Model. • Analyse and assess 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, Due Care). • Compare and contrast various threat models (STRIDE Threat model; OWASP Threat Risk modelling). • 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). • Evaluate the security benefits of cloud computing. • Investigate CSA STAR initiative, STAR Self-Assessment.
IaaS Security • Assess IaaS Security Concerns. • Explore the concept of Virtualization. • 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; IaaS 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; PaaS 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; SaaS Lock-in. • 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 (e.g., XSS and CSRF).
Identity and Access Management (IAM) • Assess identity federation and claims-based security services with respect to cloud based systems (e.g., Security Assertion Markup Language (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 vis-à-vis 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. • Investigate homomorphic encryption techniques • Quantum Computing and secure key distribution
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 • 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.
Cloud Security Architectural Patterns & Frameworks • What is cloud security architecture? • Analyse and assess: o Functional elements o cloud service model/deployment model considerations o architectural design patterns o Cloud Security Posture Management (CSPM) o reference security architectures and frameworks (e.g., AWS Security Reference Architecture, Google Cloud Architecture Framework, Microsoft Cloud Adoption Framework, IBM Security Architecture for Cloud Applications)

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

Assessments

Full Time

Coursework

Assessment Type:	Formative Assessment	**% of total:**	Non-Marked
Assessment Date:	n/a	**Outcome addressed:**	1,2,3,4
Non-Marked:	Yes		

Assessment Description:
Formative assessment will be provided on the in-class individual or group activities. Feedback will be provided in written or oral format, or on-line through Moodle. In addition, in class discussions will be undertaken as part of the practical approach to learning.

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

Assessment Description:
Assessment will be through completion of a project in which learners are required to devise policies, strategies and recommendations for securing cloud based service offerings (e.g., an IaaS, PaaS or SaaS service). Learners will be required to deploy and secure a cloud based application as part of the project. 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.

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:
A terminal examination will assess learner's knowledge and analytical skills in regard to the evaluation of the principles of security for cloud based systems.

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.*
Reassessment Description The reassessment strategy for this module will consist of a terminal examination that will assess all learning outcomes.

H9CAS2: Cloud Architectures and Security

Module Workload

Module Target Workload Hours 0 Hours

Workload: Full Time

Workload Type	*Workload Description*	*Hours*	*Frequency*	*Average Weekly Learner Workload*
Lecture	Classroom and demonstrations	24	Per Semester	2.00
Tutorial	Mentoring and small-group tutoring	24	Per Semester	2.00
Independent Learning	Independent learning	202	Per Semester	16.83
			Total Weekly Contact Hours	4.00

Workload: Blended

Workload Type	*Workload Description*	*Hours*	*Frequency*	*Average Weekly Learner Workload*
Lecture	Classroom and demonstrations	12	Per Semester	1.00
Tutorial	Mentoring and small-group tutoring	12	Per Semester	1.00
Directed Learning	Directed e-learning	24	Per Semester	2.00
Independent Learning	Independent learning	202	Per Semester	16.83
			Total Weekly Contact Hours	4.00

Workload: Part Time

Workload Type	*Workload Description*	*Hours*	*Frequency*	*Average Weekly Learner Workload*
Lecture	Classroom and demonstrations	24	Per Semester	2.00
Tutorial	Mentoring and small-group tutoring	24	Per Semester	2.00
Independent Learning	Independent learning	202	Per Semester	16.83
			Total Weekly Contact Hours	4.00

Module Resources

Recommended Book Resources

John R. Vacca. (2016), Cloud Computing Security: Foundations and Challenges, CRC Press, [ISBN: 978-1482260946].

Chris Dotson. (2019), Practical Cloud Security, O'Reilly Media, p.196, [ISBN: 978-1492037514].

Mike Chapple,David Seidl. (2022), (ISC)2 CCSP Certified Cloud Security Professional Official Study Guide, Sybex, p.384, [ISBN: 978-1119909378].

Supplementary Book Resources

Melvin B. Greer (Jr),Kevin L. Jackson. (2016), Practical Cloud Security: A Cross-Industry View, CRC Press, [ISBN: 978-1498729437].

Raj Samani,Jim Reavis,Brian Honan. (2014), CSA Guide to Cloud Computing, Syngress Press, p.216, [ISBN: 978-0124201255].

This module does not have any article/paper resources

Other Resources

[Website], NIST. (2012). Cloud Computing Synopsis and Recommendations. Available at:, https://www.nist.gov/publications/cloud- computing-synopsis-and-recommendations

[Website], CSA. (2017). Security Guidance For Critical Areas of Focus In Cloud Computing v4.0.Available at:, https://downloads.cloudsecurityalliance. org/assets/research/security-guidance/se curity-guidance-v4-FINAL.pdf

Discussion Note:	