The Hong Kong University of Science and Technology

UG Course Syllabus (Summer 2025-26)

[Course Title] Practical Cloud Computing Security

[Course Code] COMP4635

[No. of Credits] 3

[Any pre-/co-requisites] Pre-requisites: COMP 2611 OR COMP 2633

Name: IEONG Sze Chung Ricci

Email: ricci@ust.hk

Course Description

The practical cloud security course covers a wide range of topics to address the security issues in cloud computing. It explores the basics of cloud computing, common threats, and attacks, security architecture in different cloud service and deployment models, software-based security tools, identity and access management, patch management, data security controls, and more. The course emphasizes practical implementation work and application development to provide students with hands-on experience. By the end of the course, participants will have gained the knowledge and skills necessary to secure cloud environments effectively and protect against evolving security threats.

The course covers current security trends, practices in IT security industry, design requirements for secure cloud computing environment in various cloud platform – AWS, Azure, etc.

All students will have to setup the web, application and database servers into the AWS EC2 environment where web and network attack will be launched to the servers in EC2 and Security Groups, accounts will be further configured in the security configuration.

The major topics to be discussed in the course are:

1. Virtualization, Data Center Operations, and Introduction of Cloud Computing
2. Cloud Computing Concept, Cloud Service Model (IaaS, PaaS, SaaS), Cloud Deployment Model (Public, Private, Community and Hybrid)
3. Security threats in Cloud and Virtualization Security, Top Cloud Security threats
4. Cloud Computing, Governance, Compliance, Audit and Legal requirements, SLA
5. Common Infrastructure security in Cloud Infrastructure - Physical Security, virtualization & network security, Patch Management, Storage and Data architecture
6. IaaS specific security, Storage and encryption, workload security
7. PaaS security, Container, Function as a Service, Serverless security, DevOps and Microservices
8. SaaS security, IAM Security, data privacy, Compliance
9. Cloud Security Audit and Cloud Security Assessment
10. Cloud Security Incident Response, BCP, DR
11. Other Cloud Computing related security technology - Zero Trust Architecture, Cloud Security Posture

Intended Learning Outcomes (ILOs)

By the end of this course, students should be able to:

1. Understand the current security threat and future trend of Cloud Computing Security

2. Design and develop applications with security features in Cloud Environment according to NIST standards

3. Incorporate best security practices in Cloud Environment (such as latest Cloud Security Alliance Security Guidance, Cloud Control Matrix, ISO 27000 series, OWASP Top 10 risks)

4. Apply Information security governance and risk management to real life scenario

5. Perform Cloud Computing Architecture Design (IaaS, PaaS, SaaS)

6. Launch secure cloud application environment

7.Set up and conduct security testing/assessment tools

Assessment and Grading

This course will be assessed using criterion-referencing and grades will not be assigned using a curve. Detailed rubrics for each assignment are provided below, outlining the criteria used for evaluation.

Assessments:

[List specific assessed tasks, exams, quizzes, their weightage, and due dates; perhaps, add a summary table as below, to precede the details for each assessment.]

Assessment Task	Contribution to Overall Course grade (%)	Due date
Class assignment	30%	Every week
Class participation	10%	Every week
In class tests	10%	04/07/2026 (W3), 25/07/2026 (W6)
Project	30%	08/08/2026 (W8)
Final examination	20%	08/08/2026 (W8)

* Assessment marks for individual assessed tasks will be released within two weeks of the due date.

Mapping of Course ILOs to Assessment Tasks

[add to/delete table as appropriate]

Assessed Task	Mapped ILOs	Explanation
Class assignment	CILO-5, CILO-6, CILO-7	5 lab sessions where students will have to follow the instructions to setup and configure the cloud environment securely.
Class participation (Group)	CILO-5, CILO-6, CILO-7	There will be group discussion where students will have to answer questions after group discussions.
In-class tests	CILO-1, CILO-2, CILO-3	Students will have to answers 15 MC/MA questions via Canvas.

Project	CILO-3, CILO-4, CILO5, CILO6, CILO-7	This is the group project where students will have to take what they learn and setup a cloud application using the cloud environment and then develop a cloud security testing plan to evaluate the security posture of their cloud application? The application implemented, test results and testing plan will be evaluated through the provided report and the presentation.
Final examination	CILO-1, CILO-2, CILO-3	This will be the final exam of the course where student will have to answer MC/MA and scenario based questions to evaluate their knowledge in performing Cloud Security review.

Grading Rubrics

[Detailed rubrics for each assignment will be provided. These rubrics clearly outline the criteria used for evaluation. Students can refer to these rubrics to understand how their work will be assessed.]

Final Grade Descriptors:

[As appropriate to the course and aligned with university standards]

Grades	Short Description	Elaboration on subject grading description
A	Excellent Performance	[Example: Demonstrates a comprehensive grasp of subject matter, expertise in problem-solving, and significant creativity in thinking. Exhibits a high capacity for scholarship and collaboration, going beyond core requirements to achieve learning goals.]
B	Good Performance	[Example: Shows good knowledge and understanding of the main subject matter, competence in problem-solving, and the ability to analyze and evaluate issues. Displays high motivation to learn and the ability to work effectively with others.]
C	Satisfactory Performance	[Example: Possesses adequate knowledge of core subject matter, competence in dealing with familiar problems, and some capacity for analysis and critical thinking. Shows persistence and effort to achieve broadly defined learning goals.]
D	Marginal Pass	[Example: Has threshold knowledge of core subject matter, potential to achieve key professional skills, and the ability to make basic judgments. Benefits from the course and has the potential to develop in the discipline.]
F	Fail	[Example: Demonstrates insufficient understanding of the subject matter and lacks the necessary problem-solving skills. Shows limited ability to think critically or analytically and exhibits minimal effort towards achieving learning goals. Does not meet the threshold requirements for professional practice or development in the discipline.]

Course AI Policy

Submitted work must be written by the student. AI use for research an learning further is allowed; however, in submitted project a student needs to present the results in his/her own works highlighting his or her understanding not by copying AI text. All submitted work will go through plagiarism and AI detection software and penalties will be taken after consultation with the student. AI tools are not allowed for the quiz and exams.

Communication and Feedback

Assessment marks for individual assessed tasks will be communicated via Canvas within two weeks of submission. Feedback on assignments will include [specific details, e.g., strengths, areas for improvement]. Students who have further questions about the feedback including marks should consult the instructor within five working days after the feedback is received.

Resubmission Policy

Resubmission is not permitted for the course.

Required Texts and Materials

Samani, R., Honan, B., & Reavis, J. (2014). *CSA guide to cloud computing: Implementing cloud privacy and security*. Syngress.

Dotson, C. (2023). *Practical cloud security*. " O'Reilly Media, Inc.".

Alliance C., (2024). “Security guidance for critical areas of focus in cloud computing v5.0”, Cloud Security Alliance, https://cloudsecurityalliance.org/research/guidance

Additional materials from Cloud Security Alliance, Amazon AWS and Azure Cloud web sites.

Academic Integrity

Students are expected to adhere to the university’s academic integrity policy. Students are expected to uphold HKUST’s Academic Honor Code and to maintain the highest standards of academic integrity. The University has zero tolerance of academic misconduct. Please refer to Academic Integrity | HKUST – Academic Registry for the University’s definition of plagiarism and ways to avoid cheating and plagiarism.

[Optional] Additional Resources

[List any additional resources, such as online platforms, library resources, etc.]