Course Specifications

Course Title:	**Cloud Security**
Course Code:	**CSEC 414**
Program:	**Information and Computer Science**
Department:	**Computer Science and Information**
College:	**College of Science**
Institution:	**Majmaah University**

Table of Contents

A. Course Identification

1. Credit hours:3
2. Course type **a.** University ☐ College ☐ Department ☐ Others ☐ **b.** Required ☐ Elective ☑
3. Level/year at which this course is offered:
4. Pre-requisites for this course (if any)**:** Cloud Computing ICS 327 and Cyber security principles CSEC 313
5. Co-requisites for this course (if any)**:** N/A

6. Mode of Instruction (mark all that apply)

No	Mode of Instruction	Contact Hours	Percentage
1	**Traditional classroom**	48	80%
2	**Blended**	6	10%
3	**E-learning**	6	10%
4	**Correspondence**	0	0
5	**Other**	0	0

7. Actual Learning Hours (based on academic semester)

No	Activity	Learning Hours
Contact Hours		
1	**Lecture**	30
2	**Laboratory/Studio**	15
3	**Tutorial**	15
4	**Others** (specify)	0
	Total	60
Other Learning Hours*		
1	**Study**	45
2	**Assignments**	15
3	**Library**	10
4	**Projects/Research Essays/Theses**	10
5	**Others** (specify)	0
	Total	80

* The length of time that a learner takes to complete learning activities that lead to achievement of course learning outcomes, such as study time, homework assignments, projects, preparing presentations, library times

B. Course Objectives and Learning Outcomes

1. Course Description

This course provides the ground-up coverage on the high-level concepts of cloud landscape, architectural principles, techniques, design patterns and real-world best practices applied to Cloud service providers and consumers and delivering secure Cloud based services. The course will describe the Cloud security architecture and explore the guiding security design principles, design patterns, industry standards, applied technologies and addressing regulatory compliance requirements critical to design, implement, deliver and manage secure cloud-based services. The course delves deep into the secure cloud architectural aspects with regards to identifying and mitigating risks, protection and isolation of physical & logical infrastructures including compute, network and storage, comprehensive data protection at all OSI layers, end-to-end identity management & access control, monitoring and auditing processes and meeting compliance with industry and regulatory mandates. The course will leverage cloud computing security guidelines set forth by ISO, NIST, ENISA and Cloud Security Alliance (CSA)

2. Course Main Objective

1Fundamentals of cloud computing architectures based on current standards, protocols, and best practices intended for delivering Cloud based enterprise IT services and business applications.
2Approaches to designing cloud services that meets essential Cloud infrastructure characteristics – on-demand computing, shared resources, elasticity and measuring usage
3Design security architectures that assures secure isolation of physical and logical infrastructures including compute, network and storage, comprehensive data protection at all layers, end-to-end identity and access management, monitoring and auditing processes and compliance with industry and regulatory mandates.

3. Course Learning Outcomes

	CLOs	Aligned PLOs
1	**Knowledge:**	
1.1	1Identify the known threats, risks, vulnerabilities and privacy issues associated with Cloud based IT services.	K3-CSEC
1.2		
2	**Skills :**	
2.1	2Understand the concepts and guiding principles for designing and implementing appropriate safeguards and countermeasures for Cloud based IT services	S3-CSEC
2.2	3Understand the industry security standards, regulatory mandates, audit policies and compliance requirements for Cloud based infrastructures	
3	**Competence:**	
3.1	explore the guiding security design principles, design patterns, industry standards, and applied technologies	C3-CSEC
3.2		

C. Course Content

No	List of Topics	Contact Hours
1	Fundamentals of Cloud Computing and Architectural Characteristics.	12
2	Security Design and Architecture for Cloud Computing.	12
3	Secure Isolation of Physical & Logical Infrastructure.	12
4	Data Protection for Cloud Infrastructure and Services.	12

5	Enforcing Access Control for Cloud Infrastructure based Services.	12
Total		60

D. Teaching and Assessment

1. Alignment of Course Learning Outcomes with Teaching Strategies and Assessment Methods

Code	Course Learning Outcomes	Teaching Strategies	Assessment Methods
1.0	**Knowledge**		
1.1	Fundamentals of cloud computing architectures based on current standards, protocols, and best practices intended for delivering Cloud based enterprise IT services and business applications.	Lectures Lab demonstrations Case studies Individual presentations	Written Exam Homework assignments Lab assignments Class Activities Quizzes
1.2	Approaches to designing cloud services that meets essential Cloud infrastructure characteristics.		
2.0	**Skills**		
2.1	Design security architectures that assures secure isolation of physical and logical infrastructures	Lectures Lab demonstrations Case studies Individual presentations Brainstorming	Written Exam Homework assignments Lab assignments Class Activities Quizzes Observations
2.2	Design security architectures that compliance with industry and regulatory mandates.		
3.0	**Competence**		
3.1	Work to excel as an individual for the benefit of the group.	Small group discussion Whole group discussion Brainstorming Presentation	Observations Homework assignments Lab assignments Class
3.2	Explore the guiding security design principles, design patterns, industry standards, and applied technologies		

2. Assessment Tasks for Students

#	Assessment task*	Week Due	Percentage of Total Assessment Score
1	First written mid-term exam	6	15%
2	Second written mid-term exam	12	15%
3	Presentation, class activities, and group discussion	Every week	10%
4	Homework assignments	After each chapter	10%
5	Implementation of presented protocols	Every two weeks	10%
6	Final written exam	16	40%
7	Total		100%

***Assessment task** (i.e., written test, oral test, oral presentation, group project, essay, etc.)

E. Student Academic Counseling and Support

Arrangements for availability of faculty and teaching staff for individual student consultations and academic advice :

F. Learning Resources and Facilities

1.Learning Resources

Required Textbooks	Tounsi, W. (2019). Cyber-Vigilance and Digital Trust: Cyber Security in the Era of Cloud Computing and IoT. John Wiley & Sons
Essential References Materials	Rittinghouse, John W., and James F. Ransome, ―Cloud Computing: Implementation, anagement and Security‖, CRC Press, 2017.
Electronic Materials	https://www.elsevier.com/
Other Learning Materials	Video and presentation will be available during the time of classes

2. Facilities Required

Item	Resources
Accommodation (Classrooms, laboratories, demonstration rooms/labs, etc.)	Classroom and Labe available at College of science in Zulfi.
Technology Resources (AV, data show, Smart Board, software, etc.)	All resource is available in the halls
Other Resources (Specify, e.g. if specific laboratory equipment is required, list requirements or attach a list)	N/A

G. Course Quality Evaluation

Evaluation Areas/Issues	Evaluators	Evaluation Methods
Effectiveness of teaching and assessment	Students Reviewers	Questionnaires (course evaluation) filled by the students and electronically organized by the university. Student-faculty and management meetings.
Quality of learning resources	Program Leaders	Direct/indirect

Evaluation areas (e.g., Effectiveness of teaching and assessment, Extent of achievement of course learning outcomes, Quality of learning resources, etc.)
Evaluators (Students, Faculty, Program Leaders, Peer Reviewer, Others (specify)
Assessment Methods (Direct, Indirect)

H. Specification Approval Data

Council / Committee	
Reference No.	
Date	