

NEW YORK CITY COLLEGE OF TECHNOLOGY/CUNY
Computer Systems Technology Department
Cloud Security
CST4716

(2 class hours, 2 lab hours, 3 credits)

Instructor:

Course Description:

Cloud computing has evolved in recent years and has expanded its reach to most enterprises and industries across the world. With this expansion comes the need for IT professionals who understand how to secure such environments. This course attempts to fill this gap by providing students with the knowledge and technical skills required to design, manage and secure data, infrastructure and applications in the cloud using best current practices. This course will cover cloud in general without restricting itself to certain cloud technologies like AWS and Azure. Exposure to multiple cloud technologies though will be achieved via the course lab exercises. To ensure the course fully aligns with the industry, the textbook used in this course is the official body of knowledge for CCSP (Certified Cloud Security Professional) credential.

Course Objectives:

Upon successful completion of the course, the student should be able to:

1. Demonstrate knowledge of the core concepts of cloud computing
2. Demonstrate knowledge of the core concepts of cloud security
3. Design and Apply basic Cloud Security technologies and strategies
4. Demonstrate the ability to perform basic cloud security operation tasks

Required Materials:

The Official (ISC)2 CCSP CBK Reference, 4th Edition
Aaron Kraus, ISBN: 978-1-119-90903-3

The course is divided into 6 domains in line with the CCSP structure.

- Domain 1. Cloud Concepts, Architecture and Design
- Domain 2. Cloud Data Security
- Domain 3. Cloud Platform & Infrastructure Security
- Domain 4. Cloud Application Security
- Domain 5. Cloud Security Operations
- Domain 6. Legal, Risk and Compliance

The students also need an account and access to AWS for the labs.

Prerequisites: CST2410

Attendance Policy:

Attendance is expected at all sessions.

Academic Integrity Standards:

Students and all others who work with information, ideas, texts, images, music, inventions, and other intellectual property owe their audience and sources accuracy and honesty in using, crediting, and citing sources. As a community of intellectual and professional workers, the College recognizes its responsibility for providing instruction in information literacy and academic integrity, offering models of good practice, and responding vigilantly and appropriately to infractions of academic integrity. Accordingly, academic dishonesty is prohibited in The City University of New York and at New York City College of Technology and is punishable by penalties, including failing grades, suspension, and expulsion. The complete text of the College policy on Academic Integrity may be found in the catalog.

The instructor of the course has the authority to give a grade of F if the student submits the work of another person in a manner that represents his/her work or knowingly permits one's work to be submitted by another person without the instructor's permission (see College Catalog).

Progression Requirements

Students majoring in CIB must earn a grade of "C" or better in this course to progress to the next level courses. If grade earned is less than "C", the course must be repeated.

Homework Assignments

All assignment are to be submitted by the due date on SafeAssign. Late assignments, as well as assignments not submitted through SafeAssign will not be accepted.

Grading Procedure:

Exams	45%
Assignments	45%
Labs	10%
	==
TOTAL	100%

Letter Grade	A	A-	B+	B	B-	C+	C	D	F
Numerical Grade	93-100	90-92.9	87-89.9	83-86.9	80-82.9	77-79.9	70-76.9	60-69.9	<=59.9

Course Outline:

Week	Topics	Reading
------	--------	---------

1	Understand Cloud Computing Concepts: Cloud Computing Definitions and roles Key Cloud Computing Characteristics Building Block Technologies Cloud Reference Architecture Cloud Computing Activities, and Capabilities Cloud Service Categories and Deployment Models Cloud Shared Considerations	Pages 1-22
2	Security Concepts Relevant to Cloud Computing Cryptography and Key Management Access Control Data and Media Sanitization Network Security Virtualization Security Common Threats Understand Design Principles of Secure Cloud Computing Cloud Secure Data Lifecycle Cloud-Based Disaster Recovery and Business Continuity Planning Functional Security Requirements and Security Considerations for Different Cloud Categories Lab 1	Pages 23-40
3	Cloud Data Security Cloud Data Concepts and Lifecycle Phases Data Dispersion Design and Implement Cloud Data Storage Architectures Storage Types Threats to Storage Types Design and Apply Data Security Technologies and Strategies Encryption and Key Management Hashing, Masking, and Tokenization Data Loss Prevention, Obfuscation, and De-identification Implement Data Discovery Exam 1	Pages 40-69
4	Design and Implement Information Rights Management Plan. Implement Data Retention, Deletion, and Archiving Policies Design and Implement Auditability, Traceability, and Accountability of Data Events	Pages 70-85
5	Cloud Platform and Infrastructure Security Design a Secure Data Center Analyze Risks Associated with Cloud Infrastructure Design and Plan Security Controls Identification, Authentication, and Authorization in Cloud Infrastructure Plan Disaster Recovery and Business Continuity Lab 2	Pages 85-116

6	Cloud Application Security Cloud Development Basics and Common Cloud Vulnerabilities Secure Software Development Lifecycle Process NIST Secure Software Development Framework OWASP Software Assurance Security Model Cloud-Specific Risks, Quality Assurance, and Threat Modeling Software Configuration Management and Versioning Secure Testing Methodologies Exam 2	Pages 117-132
7	Cloud Application Security - Continued Cryptography, Sandboxing, and Application Virtualization and Orchestration Identity and Access Management Solutions Federated Identity Identity Providers Single Sign-On Multifactor Authentication Cloud Access Security Broker Lab 3	Pages 133-144
8	Cloud Security Operations Hardware-Specific Security Configuration Requirements Installation and Configuration of Virtualization Management Tools Virtual Hardware–Specific Security Configuration Requirements Installation of Guest Operating System Virtualization Toolsets Configure Access Control for Local and Remote Access Secure Network Configuration Operating System Hardening through the Application of Baselines	Pages 145-165
9	Cloud Security Operations Operating System Baseline Compliance Monitoring and Remediation Patch Management Performance and Capacity Monitoring Hardware Monitoring Configuration of Host and Guest Operating System Backup and Restore Functions Network Security Controls and Management Plane Exam 4	165-181

10	Implement Operational Controls and Standards Change Management, and Continuity Management Information Security Management Continual Service Improvement Management Incident, Problem, Release, Deployment, Configuration, Service Level, Availability, and Capacity Management Lab 4	182-197
11	Forensics Forensic Data Collection Methodologies, and Evidence Management Collect, Acquire, and Preserve Digital Evidence Manage Communication with Relevant Parties Shared Responsibility Model Stakeholders Manage Security Operations Security Operations Center Monitoring of Security Controls Log Capture and Analysis Incident Management	198-220
12	Evaluation of Legal Risks Specific to Cloud Computing Understanding Audit Process, Methodologies, and Required Adaptations for a Cloud Environment Lab 5	221-250
13	Understand Implications of Cloud to Enterprise Risk Management Assess Providers Risk Management Programs 266 Differences Between Data Owner/Controller vs. Data Custodian/Processor Risk Treatment and Risk Frameworks Metrics for Risk Management Assessment of Risk Environment	251-285
14	Final Review	
15	Exam 5	

Assessment Criteria:

For the successful completion of this course a student should be able to:	Evaluation methods and criteria
Demonstrate knowledge of the core concepts of cloud computing	Exams, and assignments

Demonstrate knowledge of the core concepts of cloud security	Exams, and assignments
Design and Apply basic Cloud Security Technologies and Strategies	Exams, and assignments
Demonstrate the ability to perform basic cloud security operation tasks	Labs