Carnegie Mellon University
Heinz College

# 95-746 Cloud Security

**Tues,** 6:30 - 9:20**, Location:** Remote/Zoom

**Semester:** Spring **Year:** 2024

## Instructor information

| | |
|---|---|
| **Name** | George Werbacher |
| **Contact Info** | gwerbach@andrew.cmu.edu<br>george.werbacher@liveoak.bank |
| **Office location** | Remote/Zoom |
| **Office hours** | Available Upon Request |

## TA Information

| | |
|---|---|
| **Name** | Natasha Timothy |
| **Contact Info** | ntimothy@andrew.cmu.edu |
| **Office location** | TBD |
| **Office hours** | TBD |

## Course Description

This course comprehensively explores the intricate security challenges and leading-edge solutions in contemporary cloud environments. Students will develop a deep understanding of fundamental cloud security concepts, architectural models, and risk mitigation strategies. The course delves into the distinctions between conventional and cloud-native security paradigms, addressing evolving risk management philosophies crucial to safeguarding cloud-based assets. The course emphasizes a hands-on approach, enabling students to apply theoretical concepts to practical scenarios within simulated cloud environments. Graduates will possess the expertise to provide immediate strategic value to infrastructure and security teams within any cloud-reliant organization.

Throughout the course, students will engage with contemporary cloud security challenges—from architecting resilient cloud infrastructure and implementing robust data security measures to designing cloud-native Identity and Access Management (IAM) solutions and addressing compliance mandates. The curriculum incorporates emerging trends and technologies, ensuring graduates are equipped to tackle the evolving threat landscape of cloud computing and make informed strategic decisions within organizations that rely on cloud-based services.

## Learning Objectives

- Understand fundamental concepts of cloud security, including principles of data encryption, network security, and access control.
- Compare and contrast conventional security practices with cloud-native security paradigms, identifying key differences and implications for risk management.
- Analyze various architectural models for cloud environments, evaluating their strengths and weaknesses in terms of security posture.
- Assess risks associated with cloud-based assets and formulate effective risk mitigation strategies tailored to cloud environments.
- Develop proficiency in architecting resilient cloud infrastructure to withstand security threats and ensure high availability.
- Implement robust data security measures in cloud environments, including encryption, data masking, and secure data transfer protocols.
- Design and deploy cloud-native Identity and Access Management (IAM) solutions, integrating principles of least privilege and multi-factor authentication.
- Demonstrate compliance with relevant regulatory mandates and industry standards in cloud environments, such as GDPR, HIPAA, and SOC 2.
- Apply theoretical concepts to practical scenarios within simulated cloud environments, gaining hands-on experience with cloud security tools and techniques.
- Evaluate emerging trends and technologies in cloud security, staying abreast of developments to inform strategic decision-making in cloud-reliant organizations

## Learning Resources

- **Readings:** This course uses a textbook rather than a comprehensive set of books, articles, research papers, and reports. All materials are available online via the CMU Library or Canvas.
- **Lab Environments:** The course provided hands-on learning experiences using CMU’s partnership with Amazon Web Services. Students will have the ability to utilize accessible sandbox environments or build their environments. All instructions will be provided via Canvas and/or Github.

## Assessments

The final course grade will be calculated using the following categories:

| Assessment | Percentage of Final Grade |
|---|---|
| Labs | 10% |
| Assignments | 25% |
| Mid-Term Exam | 30% |
| Final Exam | 35% |

- **Labs:** Students will receive access to AWS Academy, which provides a set of labs to help students get hands-on experience with AWS. These labs will be graded for completion.
- **Assignments:** Assignments will be given periodically throughout the course to provide a more in-depth understanding of this course’s topics.
- **Mid-Term Exam:** The Mid-Term Exam will be a multiple-choice exam that will test your knowledge up to that point of the course. This will be a **closed-book exam**.

- **Final Exam:** The Final Exam will be a multiple-choice exam that will test your course knowledge. This will be a **closed-book exam**.
- ***Optional Final Exam:*** Students who wish not to take the final exam will have the opportunity to receive a passing grade (A) on their final exam if they **take and pass** a cloud-related certification exam.

Students will be assigned the following final letter grades based on calculations from the course assessment section. All grades will be rounded to the nearest whole number.

| **Grade** | **Percentage Interval** |
|---|---|
| A+ | 98-100% |
| A | 92-97% |
| A- | 90-91% |
| B+ | 88-89% |
| B | 82-87% |
| B- | 80-81% |
| C+ | 78-79% |
| C | 72-71% |
| C- | 70-71% |
| D | 50-69% |
| F | 0-49% |

## Grading Policies

- **Late-work policy**: To encourage timely submissions and ensure fair and prompt grading for all students, assignments should be submitted by 11:59 PM on the due date. For those facing unforeseen circumstances, assignments may be submitted up to 24 hours late for up to 90% of the original grade, with incremental reductions after that. No assignments will be marked after ten (10) days.

## Course Policies

- **Academic Integrity & Collaboration:** Students are expected to strictly follow Carnegie Mellon University's rules of academic integrity in this course. This means that unless otherwise specified, Individual assignments are to be the work of the individual student using only permitted material and without any cooperation of other students or third parties. It also means that using work by others is only allowed in the form of quotations, and any such quotation must be distinctively marked to identify the student's work and own ideas. All external sources must be cited appropriately, including author name(s), publication title, year of publication, and a complete reference needed for retrieval. The same work may not be submitted for credit in multiple courses. Violations will be penalized to the full extent mandated by the CMU policies. There will be no exceptions.

- **Use of Generative AI Tools:** We encourage students to explore using generative artificial intelligence (AI) tools, such as ChatGPT, for all individual assignments. Any such use must be appropriately acknowledged and cited, including the specific version of the tool used. Submitted work should include the exact prompt to generate the content and the AI's complete response in an Appendix. Because AI-generated content is not necessarily accurate or appropriate, each student must assess the validity and applicability of any generative AI output submitted. You may not earn full credit if inaccurate, invalid, or inappropriate information is found in your work. Deviations from these guidelines will be considered violations of CMU's academic integrity policy
- **Accommodations for students with disabilities**: If you have a disability and require accommodations, please contact Catherine Getchell, Director of Disability Resources, at 412-268-6121, getchell@cmu.edu. If you have an accommodations letter from the Disability Resources office, I encourage you to discuss your accommodations and needs with me as early in the semester as possible. I will work with you to ensure that accommodations are provided as appropriate.
- **Statement on student wellness**: As a student, you may experience a range of challenges that can interfere with learning, such as strained relationships, increased anxiety, substance use, feeling down, difficulty concentrating, and/or lack of motivation. These mental health concerns or stressful events may diminish your academic performance and/or reduce your ability to participate in daily activities. CMU services are available, and treatment does work. You can learn more about confidential mental health services at the Counseling and Psychological Services (CaPS) - Division of Student Affairs - Carnegie Mellon University. Support is always available (24/7) from Counseling and Psychological Services: 412-268-2922.

## Course Schedule

| Date | Theme/Topic | Required Readings |
|---|---|---|
| 03/12/24 | Welcome + Module 1: Cloud Computing & Security Foundations | PCS Chapter 1<br>CSA Domain 1<br>NIST 500-291<br>**Deadline to Add/Drop/Audit/Pass/No Pass - 3/15/24** |
| 03/19/24 | Module 2: Cloud Infrastructure Security | CSA Domain 6<br>CSA Domain 8<br>Google Drive<br>**Assignment 1 Due - 03/25/24** |
| 03/26/24 | Module 3: Cloud Identity and Access Management | PCS Chapter 3<br>Google Drive |
| 04/02/24 | Module 4: Cloud Data Protection | **Mid-Term Exam Due - 04/08/24**<br>**Module 1-3** |
| 04/09/24 | Module 5: Cloud Network Security | PCS Chapter 4<br>CSA Domain 12<br>Google Drive |
| 04/16/24 | Module 6: Cloud Threat Management and Incident Response | PCS Chapter 6<br>CSA Domain 6<br>Google Drive<br>**Assignment 2 Due - 04/22/24** |

| | | |
|---|---|---|
| 04/23/24 | Module 7: Cloud Security Compliance | PCS Chapter 5<br>PCS Chapter 6<br>CSA Domain 2<br>CSA Domain 4 |
| 04/29/24 | **No Class - Finals Week** | **Final Exam Due - 05/03/24**<br>**Modules 1-5** |