



**SECURE YOUR  
CAREER WITH A**

**CERTIFICATE IN CLOUD  
CYBERSECURITY  
SCENARIOS**

## **WHY EARN A CERTIFICATE IN REAL-WORLD CLOUD CYBERSECURITY SCENARIOS?**

Cloud security is critical for protecting an organization's data and resources in cloud computing environments. Both external and internal threats can arise, and professionals in this industry face unique challenges due to reduced visibility for clients, a reliance on external providers, and the complexities of managing security across multiple stakeholders. This certificate will benefit any organization that utilizes cloud computing.

## **WHAT WILL I LEARN?**

**Completing our online cloud cybersecurity scenarios certificate prepares you to:**

- Identify data loss prevention controls and the main components of the cloud infrastructure
- Describe the cloud data lifecycle and how to secure cloud infrastructure
- Identify how the major service categories of cloud computing apply to different business needs
- Explain the role of identity and access management in cloud computing
- Recognize the layers of the Open Systems Interconnection model
- Identify the considerations in choosing data center site
- Enumerate mitigation strategies for certain threats to cloud applications
- Understand vulnerabilities and mitigation strategies for securing the management plane of a cloud facility
- Explain the role and requirements of forensics in a cloud facility

**For more information and a complete list of courses, visit:**

## CAREER PATHS

The U.S. Bureau of Labor Statistics (BLS) expects that overall employment of cybersecurity professionals, such as cloud security engineers, is projected to grow 33% from 2023 to 2033, much faster than the average for all occupations. About 17,000 openings are projected each year, on average, over the decade.

Common cybersecurity career paths or growth opportunities include:

### Cybersecurity Professionals

Cybersecurity professionals protect an organization's data and other assets from cyberattacks. These professionals often act as the first line of defense against viruses, malicious software, unauthorized users, and natural disasters. Although protecting cloud services is not the focus of their jobs, cybersecurity professionals are usually responsible for helping organizations design, implement, and monitor security measures to protect cloud platforms and applications.

### Cloud Security Engineers

Cloud security engineers create cloud-based systems and use this technology to identify and prevent threats to these systems. They also develop and implement security controls for the cloud, such as access control, data encryption, and network security. Other responsibilities include ensuring security controls are properly implemented and configured in cloud environments, conducting security assessments and audits, and maintaining compliance with relevant security regulations and standards.

### Cloud Security Analysts

Cloud security analysts monitor and protect an organization's cloud infrastructure from threats and vulnerabilities. They are primarily responsible for identifying and addressing threats, assessing current risks and security measures, and developing incident response plans. Many also work with their organizations' cloud service providers to implement security protocols.

**The Certificate in Real-World Cloud Cybersecurity Scenarios is available 100% online.**

The courses included in this certificate carry:

PMI PDU's | IACET CEUs | HRCI Credits | ATD CI Credits | SHRM PDCs

For more information and a complete list of courses, visit: