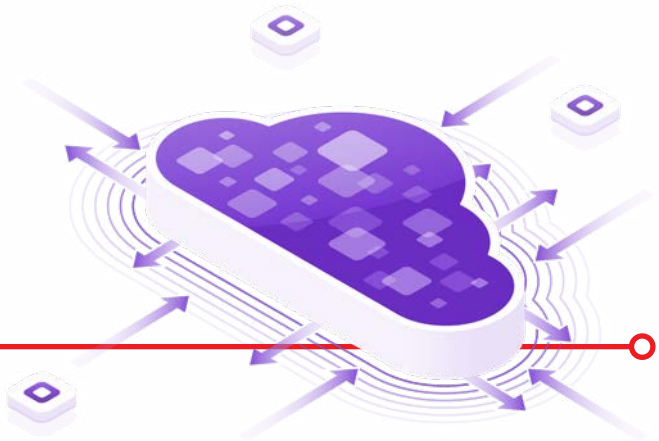

EC-Council
Building A Culture Of Security
Scale Up for a Multi-Cloud Environment
Master Cloud Security Skills Across
aws
Azure
Google Cloud
with the
C|CSE
Certified Cloud Security Engineer
Certified Cloud Security Engineer
The Most Comprehensive Cloud Security Certification Program
www.eccouncil.org

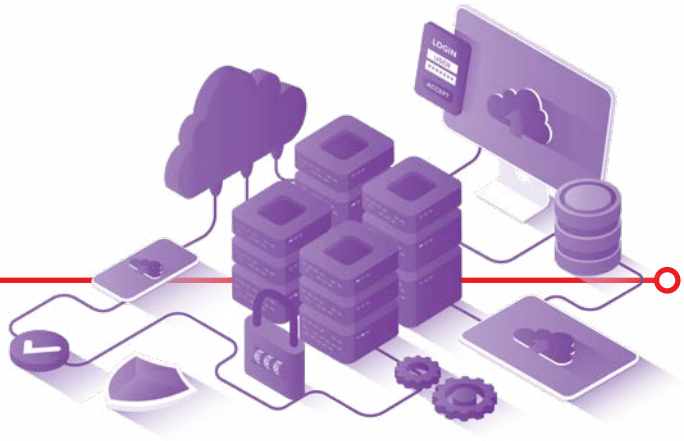
Importance of **Cloud Security**



Cyber criminals are increasingly targeting cloud services due to the large volumes of data stored and processed. While cloud computing offers numerous benefits to streamline and scale up business operations, it is not free of challenges or security concerns. Cloud security has emerged as a top priority for organizations. When a breach occurs in the cloud, there are chances of sensitive information getting exposed, stolen, or compromised, potentially resulting in significant financial losses and reputational damage. The shared responsibility model is a major contributor to cloud security risk. Cloud providers are responsible for protecting the foundation, while clients/customers need to take steps to protect their data and applications in the cloud. Furthermore, misconfigurations, weak security measures, or a lack of security updates also add to the security risks in the cloud.

Organizations need to embrace robust cloud security measures to mitigate these threats. With the widespread adoption of multi-cloud environments and continuous updates from cloud service providers (CSPs), security professionals must have the most up-to-date knowledge and skills to excel in a cloud security role.

About the **Program**



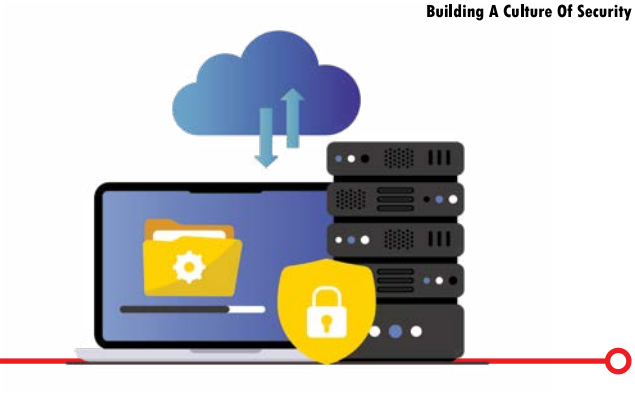
The Certified Cloud Security Engineer (C|CSE) is a multi-cloud security certification program crafted by industry experts. It offers a holistic understanding of cloud security and empowers cybersecurity professionals to apply practical skills to build, operate, and defend their environments regardless of the selected infrastructure.

Our unique approach to designing curriculum allows C|CSE content to match the latest security tools and techniques for the AWS, Azure, and GCP platforms, as well as private and hybrid architectures. This design makes the C|CSE program a perfect blend of vendor-neutral training topics with vendor-specific instruction and performance labs, offering cybersecurity professionals an unbiased learning experience.

C|CSE offers a hands-on practical approach, featuring over 85 labs to ensure candidates gain hands-on experience that can be immediately applied at the workplace to anticipate and overcome cloud security challenges.

With organizations storing and processing more data than ever on multiple cloud environments, multi-cloud security is essential to organizational cyber security initiatives. According to a forecast by Markets and Markets, the multi-cloud security market is expected to grow to USD 10.5 billion by 2027, creating a significant demand across verticals such as BFSI, healthcare, telecommunications, IT, retail, ecommerce, and other industries.

What students Learn in C|CSE

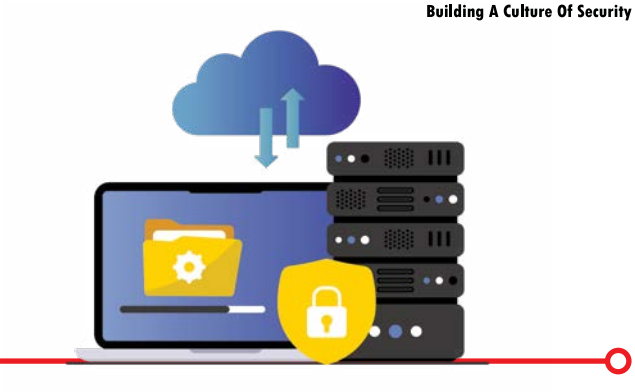


After attending this cloud security course, participants will be able to gather:

Generic Cloud Security Concepts

- Fundamentals of cloud computing and its architecture
- Key concepts and components of cloud security
- Cloud deployment models (public, private, hybrid) and their associated security considerations
- Cloud service models (Infrastructure as a Service, Platform as a Service, Software as a Service) and their respective security challenges
- Common vulnerabilities and threats specific to cloud environments and strategies for their prevention and mitigation
- Cloud security challenges and threats
- Identity and access management (IAM) in cloud environments
- Authentication and authorization mechanisms for cloud services
- Principles of secure data storage and encryption in the cloud
- Network security in cloud environments, including virtual private networks (VPNs) and firewalls
- Security monitoring and logging in to the cloud
- Incident response and disaster recovery strategies for cloud-based systems
- Best practices for securing cloud-based infrastructure and services
- Encryption techniques to safeguard sensitive information in the cloud
- Access control and IAM in the context of cloud environments
- Utilizing security monitoring and incident response mechanisms in the cloud
- Evaluate appropriate cloud service providers based on their security offerings
- Regulatory and compliance requirements related to cloud security
- Cloud security policies and procedures
- Penetration tests, security audits, and assessments to ensure compliance with cloud security standards
- Shared responsibility model and the division of security responsibilities between cloud providers and customers
- Knowledge of cloud security frameworks, such as CSA (Cloud Security Alliance)

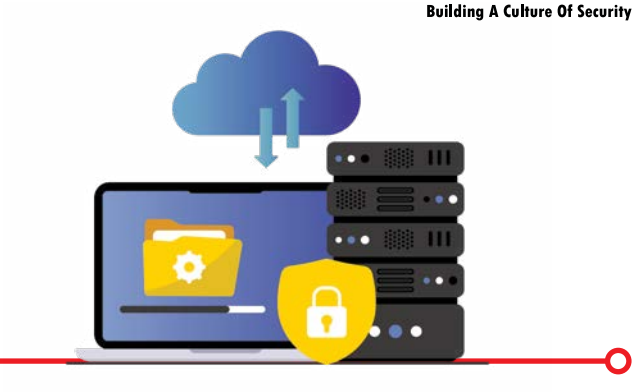
What students Learn in C|CSE



aws Specific Security Concepts

- AWS's **shared responsibility model** and the security responsibilities division between AWS and the customer
- **AWS Cloud Adoption Framework** and its security perspective capabilities
- Fundamental cloud security concepts and best practices in AWS
- Secure AWS identities and access management, including user accounts, groups, and roles
- Access control mechanisms, including **IAM roles, policies, and permissions**
- Configure and secure AWS networking components such as **Virtual Private Cloud (VPC), subnets,** and security groups
- Encryption mechanisms available in AWS, including data-at-rest and data-in-transit encryption
- **AWS Key Management Service (KMS)** and cryptographic keys
- AWS compute resources, such as **EC2 instances and serverless functions**
- AWS monitoring and logging services, including **AWS mCloudTrail** and **Amazon CloudWatch,** for security analysis and incident response
- AWS security services and features such as **AWS WAF (Web Application Firewall), AWS Shield,** and **AWS Inspector,** as well as how to implement them to enhance security
- Best practices for securing **AWS storage services, such as Amazon S3 (Simple Storage Service)** and **Amazon EBS (Elastic Block Store)**
- AWS security compliance programs and frameworks, such as the **AWS Well-Architected Framework,** to implement security controls to meet compliance requirements
- AWS security automation and orchestration tools, such as **AWS CloudFormation and AWS Config,** to automate security deployments and enforce security standards
- **Incident response and disaster recovery** in the AWS environment, including best practices for incident handling and data backup and recovery

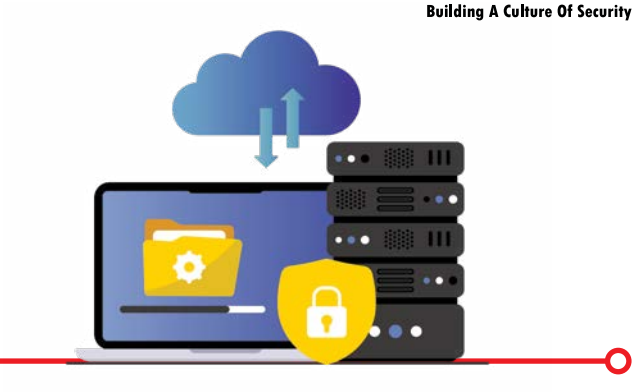
What students Learn in C|CSE



Azure Specific Security Concepts

- Principles, concepts, and components of cloud security
- Shared responsibility model and its application
- **Microsoft Cloud Adoption Framework for Azure** to achieve cloud adoption goals
- Security measures to protect Azure resources such as **virtual machines, databases, storage accounts, and networking components**
- User identities, roles, and access controls management in Azure, including implementing **Azure Active Directory (AAD), role-based access control (RBAC),** and **multi-factor authentication (MFA)**
- **Azure Virtual Network (VNet)** and implementation of network security groups (NSGs), virtual network service endpoints, and private endpoints to secure network traffic within Azure using **Azure Firewall** and **Azure DDoS Protection**
- Protect data at rest and in transit using Azure features like **Azure Disk Encryption, Azure Storage Service Encryption, Azure Key Vault, and Azure Information Protection**
- Implement **Azure Key Vault** to manage and safeguard cryptographic keys, secrets, and certificates
- Azure AD security enhancement through the implementation of features like **multi-factor authentication (MFA), conditional access, Privileged Identity Management (PIM), and Azure AD Identity Protection**
- **Microsoft Defender** for the cloud to monitor, assess, and improve the security posture of Azure resources, including **virtual machines, containers,** and **Azure services,** and implement security recommendations and best practices
- **Azure Monitor, Azure Sentinel,** and **Microsoft Defender** for the cloud's threat intelligence capabilities to detect and respond to security incidents effectively
- **Azure governance frameworks** and best practices for maintaining compliance and meeting regulatory requirements, including **Azure Policy, Azure Blueprints,** and **Azure Audit and Security Logs**
- Secure Azure virtual machines, including implementing **Azure Bastion** for secure remote access and using **Microsoft Defender** for cloud for VM monitoring and threat detection
- Best practices for securing Azure resources and implementing security controls
- Incident response procedures, disaster recovery planning, and utilizing Azure services such as **Azure Site Recovery** and **Azure Backup**
- Additional security services and solutions in Azure, including **Azure DDoS Protection** and **Azure Advanced Threat Protection**
- Best practices for securing **Azure Storage** accounts, **Azure App Service,** and **Azure SQL Database**
- **Azure Backup and Azure Site Recovery** for data protection and disaster recovery scenarios

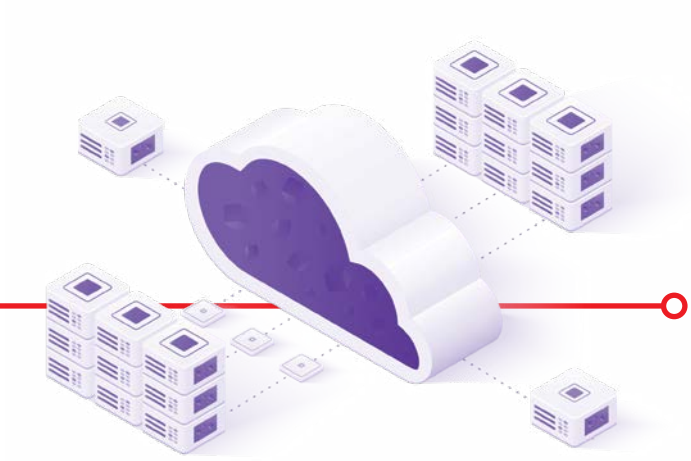
What students Learn in C|CSE



Google Cloud Specific Security Concepts

- Key concepts, principles, and best practices for securing applications and data
- Fundamentals of cloud security and shared responsibility
- **Google Cloud Adoption Framework**
- GCP security concepts, tools, and services for protecting cloud-based resources
- Implement and configure **IAM roles, policies, and permissions to control access to GCP** resources, services, and data
- Design and configure secure virtual networks (VPCs) in GCP, including **network segmentation, firewall rules, subnetworks, and VPC peering**
- GCP's network security features and tools, such as **Cloud Armor, Cloud Load Balancing, Cloud VPN,** and **Cloud DNS** to protect network traffic and prevent unauthorized access
- Protect sensitive data in GCP using **encryption techniques, including encryption at rest and in transit, key management,** and **Google Cloud Key Management Service** (KMS)
- Set up and configure logging and monitoring mechanisms to detect and respond to security incidents using tools like the **Google Cloud Security Command Center** and **Operations Suite Logging**
- Best practices for **secure application development on GCP,** including secure coding techniques, vulnerability management, and integration with security services like **Cloud Security Scanner** and **Cloud Security Command Center**
- **GCP's compliance frameworks, certifications, and regulatory requirements** to implement security controls and practices to meet industry standards and compliance obligations
- **Incident response planning, security incident management, and disaster recovery techniques specific to GCP,** including incident detection, containment, and remediation procedures
- Recommended security practices and configurations for different GCP services and resources, including **Compute Engine, Cloud Storage, Cloud SQL, and Google Kubernetes Engine (GKE)**
- Additional GCP services like **Cloud Identity-Aware Proxy (IAP), Security Key Enforcement, and Identity Platform** to enhance authentication and access control

The Latest **Technologies and Concepts** Added to C|CSE



This comprehensive program will give you a deep and practical understanding of cloud security principles, techniques, and best practices. Gain mastery in securing cloud environments by exploring various topics, including network security, access management, data protection, encryption, incident response, compliance, and more. Dive into hands-on labs and real-world scenarios to build essential skills in securing cloud platforms like AWS, Azure, and GCP.

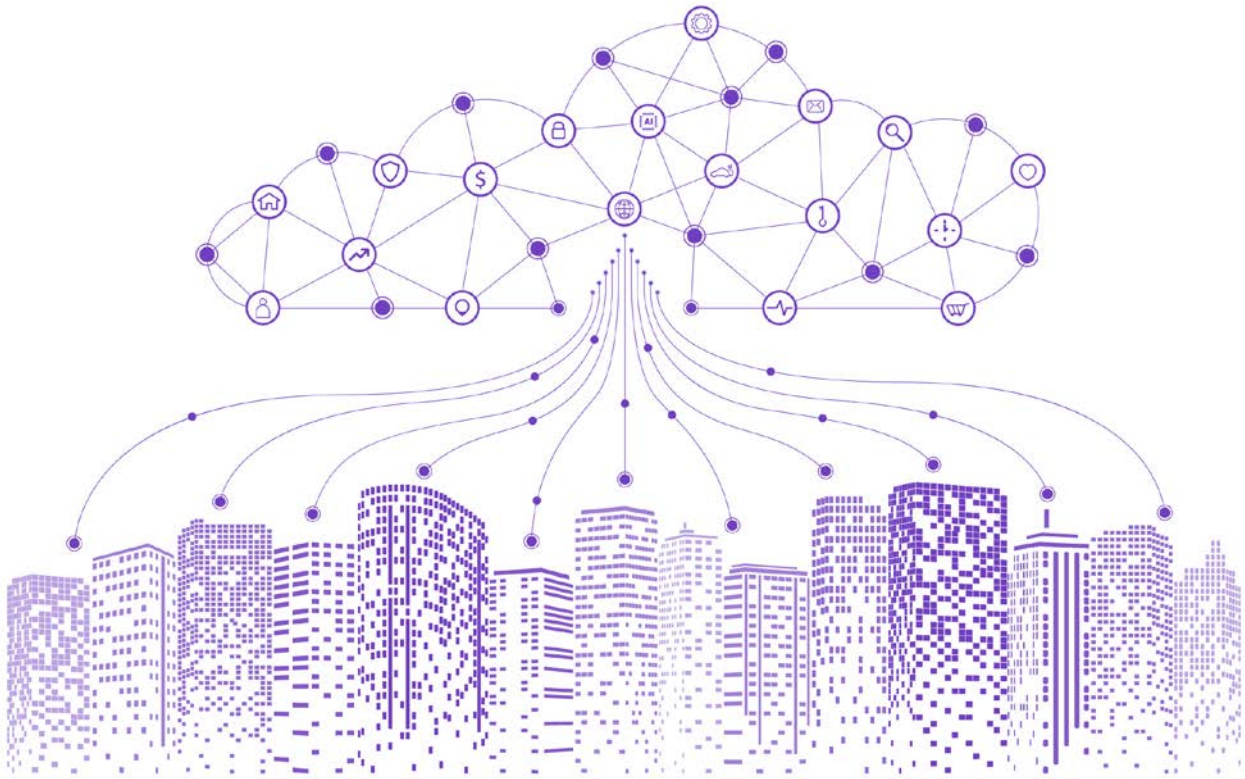
By the end of the course, participants will be equipped to confidently design, implement, and manage robust security measures in cloud environments, ensuring the utmost protection for valuable data and resources.

A few important AWS, Azure, and GCP concepts covered in this certification include the following:

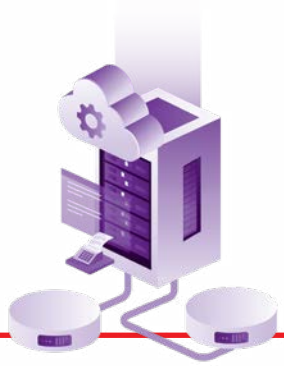
1. Application Security
2. Data Security
3. Storage Services
4. Penetration Testing Steps in the Cloud
5. Shared Responsibility Model for Security of Each Service Provider
6. Implementation of Security Operations
7. Investigating Security Incidents
8. Security Operations to Build Cloud Infrastructure
9. Elements of Cloud Data Center Physical/Logical Operations
10. Cross-Vendor Cloud Security Operations
11. Accessing Cloud Resources Through Identity and Access Management (IAM)
12. Risks and Threats Associated with Cloud Platforms and Infrastructure
13. Designing a Secure Data Center in the Cloud
14. Cloud Platform and Infrastructure Security

15. Evaluate the Risks, Attacks, and Issues in Cloud Data Storage
16. Designing Disaster Recovery and Business Continuity in the Cloud
17. Business Continuity and Disaster Recovery Configurations, Implementation, and Understanding Various Disaster Recovery Scenarios
18. Designing and Implementing a Cloud Governance Framework
19. Cloud Risk Management Framework and Process
20. Cloud Compliance
21. Governance, Risk, and Compliance
22. Legal Frameworks for Data Protection and Privacy
23. Outsourcing and Vendor Management
24. Standards, Policies, and Auditing

...and more!



Benefits of the **Certified Cloud Security Engineer Certification (C|CSE)** Program



1

Extensive Knowledge:

The C|CSE offers comprehensive knowledge and practical learning of security practices, tools, and techniques used to configure AWS, Azure, and GCP.

2

Cost Benefit Analysis:

The program enables professionals to understand the need to perform a cost-benefit analysis of all the top CSPs.

3

Holistic Approach:

The C|CSE delivers a more holistic approach, covering both technical and operational aspects of cloud security without restricting learners to a single cloud vendor or platform.

4

Best Practices:

This certification equips cybersecurity professionals with the ability to integrate best practices to control, protect, and enhance cloud network security and architecture.

5

Security Audits:

The C|CSE demonstrates how to perform cloud computing security audits and penetration testing to help organizations comply with the standards, policies, procedures, and regulations governing cloud environments.

6

Rewarding career:

The program provides a simulated environment with over 85 complex labs to equip future cloud security professionals with the necessary skills to ensure job readiness.

7

Real-World Skills:

The C|CSE enables participants to learn the skills required in real-world threat scenarios from industry experts and is mapped with cloud security professionals' current job roles and responsibilities.

8

Industry Experts:

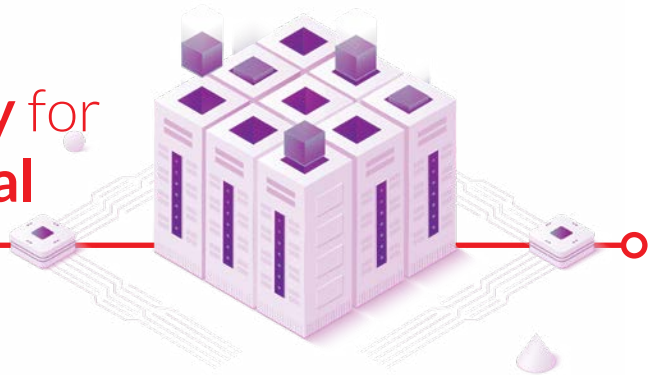
C|CSE courses are taught by instructors who are subject matter experts certified by EC-Council.

9

Cloud Security Skills:

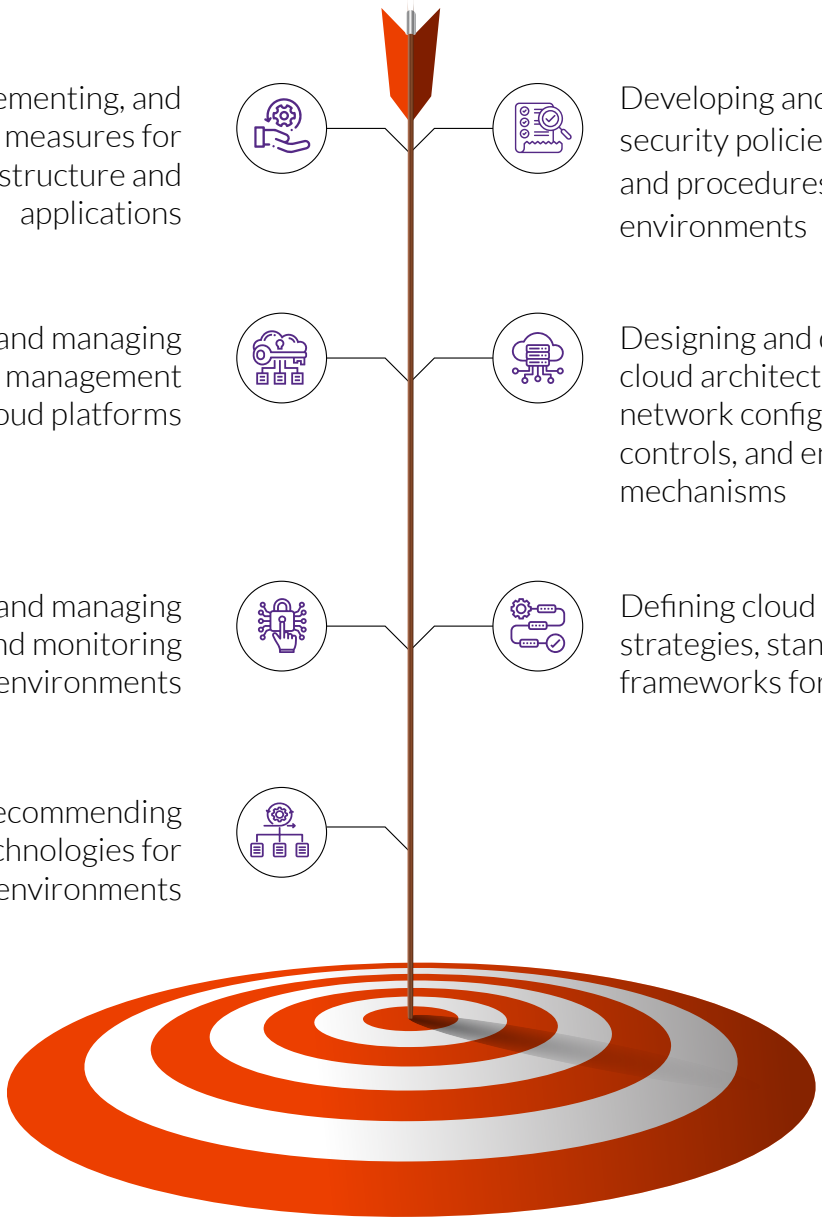
The C|CSE plays an active role in enhancing the organization's security posture by teaching topics such as how to plan, configure, implement, and maintain a secure cloud environment.

How the C|CSE Program Enables Technical Efficiency for a Cybersecurity Professional



From a technical cloud security standpoint, the C|CSE is dedicated to fortifying the underlying infrastructure of cloud services through robust measures, spanning secure configuration and testing across AWS, GCP, and Azure, as well as private and Hybrid cloud environments. Cloud Security Professionals will learn a host of skills from configuring, hardening and protecting while focusing on governance, compliance, and policy controls in cloud environments. It aims to ensure uncompromising protection for cloud servers, networks, and storage systems.

Examples of job role activities related to technical cloud security after becoming a Certified Cloud Security Engineer include the following:



- Designing, implementing, and maintaining security measures for cloud-based infrastructure and applications
- Developing and enforcing security policies, standards, and procedures for cloud environments
- Implementing and managing identity and access management (IAM) solutions for cloud platforms
- Designing and deploying secure cloud architectures, including network configuration, access controls, and encryption mechanisms
- Implementing and managing security controls and monitoring tools in cloud environments
- Defining cloud security strategies, standards, and frameworks for the organization
- Evaluating and recommending security tools and technologies for cloud environments

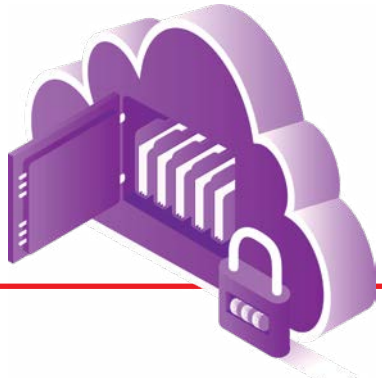
How the C|CSE Certification Will Positively Impact the Operational Aspects of a Cybersecurity Professional

From an operational cloud security standpoint, the C|CSE will help professionals manage and secure the cloud environment's day-to-day operations. This includes processes and procedures for incident response, security monitoring, disaster recovery and business continuity, forensics investigations, compliance management, etc.

Examples of job role activities related to operational cloud security after becoming a Certified Cloud Security Engineer:

- Conducting vulnerability assessments and penetration testing to identify and address security vulnerabilities.
- Monitoring and responding to security incidents and providing incident response and remediation support.

- Assisting in forensics Investigation and helping resolve security incidents when required.
- Developing and implementing cloud security strategies and solutions for business continuity and disaster recovery (BCDR) purposes



Certified Cloud Security Engineer
Program Modules:

MODULE 01 : Introduction to Cloud Security

This module provides a basic understanding of cloud computing and its service models, including the various threats and vulnerabilities found in the cloud. It highlights various factors for evaluating service providers and understanding the shared security responsibility model of service providers. Understanding the shared responsibility model provided by the cloud service provider is essential to configuring the cloud environment securely and protecting organizational resources.

MODULE 02 : Platform and Infrastructure Security in the Cloud

This module explains the key components and technology that make the architecture of the cloud and the various techniques involved in securing the multi-tenancy, virtualized, physical, and logical cloud components. It demonstrates the configurations to secure the physical data center. Users can learn the best practices to secure the workload, computing resources, and networks in the cloud. This module demonstrates the use of various services and tools provided for network and computing security in Azure, AWS, and Google cloud.

MODULE 03 : Application Security in the Cloud

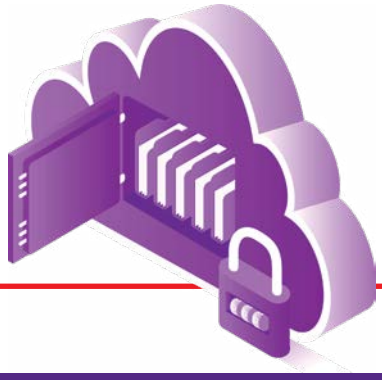
This module focuses on securing cloud applications, from designing to deployment of an application in the cloud. It explains the changes in the Secure Software Development Life Cycle (SSDLC) in the cloud. It shows how service providers' identity and access management features help implement authentication and authorization and restrict unauthorized users from accessing cloud resources. It teaches the implementation of security controls throughout the software development life cycle. This module highlights integrating security into DevOps and the continuous integration/continuous deployment (CI/CD) model for developing and deploying cloud applications. This module demonstrates the use of various services and tools provided for application security in Azure, AWS, and Google Cloud.

MODULE 04 : Data Security in the Cloud

Data security is the major concern while migrating to the cloud. This module covers the basics of cloud data storage, its life cycle, and various controls to protect data-in-rest and data-in-transit in the cloud. This module includes data storage features and various services and tools for securing the data stored in Azure, AWS, and Google Cloud.

MODULE 05 : Operation Security in the Cloud

This module includes the security controls for building, implementing, operating, managing, and maintaining physical and logical infrastructure for cloud environments. It covers the services, features, and tools AWS, Azure, and Google Cloud provide for operational security.



Certified Cloud Security Engineer **Program Modules:**

MODULE 06 : Penetration Testing in the Cloud

This module demonstrates how to implement a comprehensive penetration testing methodology for assessing the security of an organization's cloud infrastructure. It demonstrates the various services and tools used to perform penetration testing in AWS, Azure, and Google Cloud.

MODULE 07 : Incident Detection and Response in the Cloud

An incident response (IR) plan is crucial to prevent security breaches in the cloud. This module describes the incident response life cycle and highlights the considerations for responders in each phase of the IR plan in a cloud environment. It highlights the use of SOAR in automating incident response in the cloud. This module explores the incident response capabilities provided by AWS, Azure, and Google Cloud. It demonstrates various tools and services for incident detection and response.

MODULE 08 : Forensics Investigation in the Cloud

Access to forensic data and the forensic investigation process in a cloud computing environment differ from the network forensic investigation process. This module highlights various cloud forensic challenges and data collection methodologies. It demonstrates how to investigate security incidents in the cloud using various tools provided by AWS, Azure, and Google Cloud.

MODULE 09 : Business Continuity and Disaster Recovery in the Cloud

Business Continuity and Disaster Recovery (BC/DR) is important in the cloud because a third party manages the resources. This module teaches the role of the business continuity and disaster recovery plan in the cloud. It explains backup and recovery tools and the services and features provided by service providers such as AWS, Azure, and Google Cloud to prepare and manage outages to ensure business continuity.

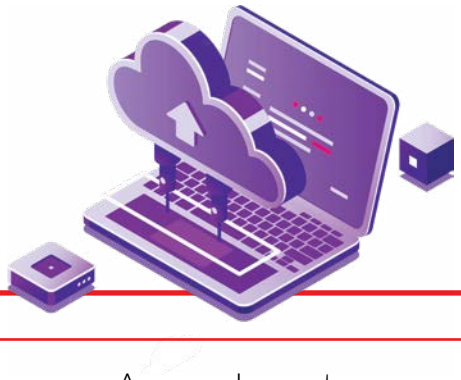
MODULE 10 : Governance, Risk Management, and Compliance in the Cloud

This module highlights the standards, policies, and legal issues related to the cloud. It highlights various legal and compliance issues found in a cloud environment. It discusses various cloud security standards and audit planning in the cloud. It demonstrates the features, services, and tools for compliance and auditing in Azure, AWS, and Google Cloud.

MODULE 11 : Standards, Policies, and Legal Issues in the Cloud

This module highlights the standards, policies, and legal issues related to the cloud. It highlights various legal and compliance issues found in a cloud environment. It discusses various cloud security standards and audit planning in the cloud. It demonstrates the features, services, and tools for compliance and auditing in Azure, AWS, and Google Cloud.

Glimpse of Top tools Covered in the **Certified Cloud Security Engineer (C|CSE)**



aws

- AWS IAM
- AWS KMS
- AWS VPC
- Web Application Firewall Cloud Front
- Amazon RDS
- Amazon Backup
- Amazon Inspector
- AWS Cloud Trial
- CloudWatch
- Amazon Macie
- AWS Security Hub
- AWS Trusted Advisor

Azure

- Microsoft Defender for Cloud
- Azure Active Directory
- Azure Monitor
- Network Watcher
- Azure Storage Analytics
- Azure Policy
- ScoutSuite
- Azure Blueprints
- Cloud Security Suite
- PowerZure

Google Cloud

- App Engine Firewall
- Cloud Identity
- Cloud Monitoring
- Security Command Center
- Web Application and API protection
- Google Cloud Armor
- Cloud Security Scanner
- GCP-IAM-Privilege-Escalation
- Secrets Manager
- Chronicle Detect
- Cloud Key Management

Vendor-Specific **Labs:**

aws **38** Labs

Azure **19** Labs

Google Cloud **31** Labs

Who Can Apply for the **Certified Cloud Security Engineer (C|CSE)?**

The Certified Cloud Security Engineer (C|CSE) program is tailored for an intermediate level and is ideally suited for individuals with prior experience in cybersecurity. The program offers a comprehensive exploration of advanced cloud security concepts, equipping working professionals with a holistic perspective covering a wide range of cloud platforms and service providers.

Professionals with experience in any of the below domains can apply:

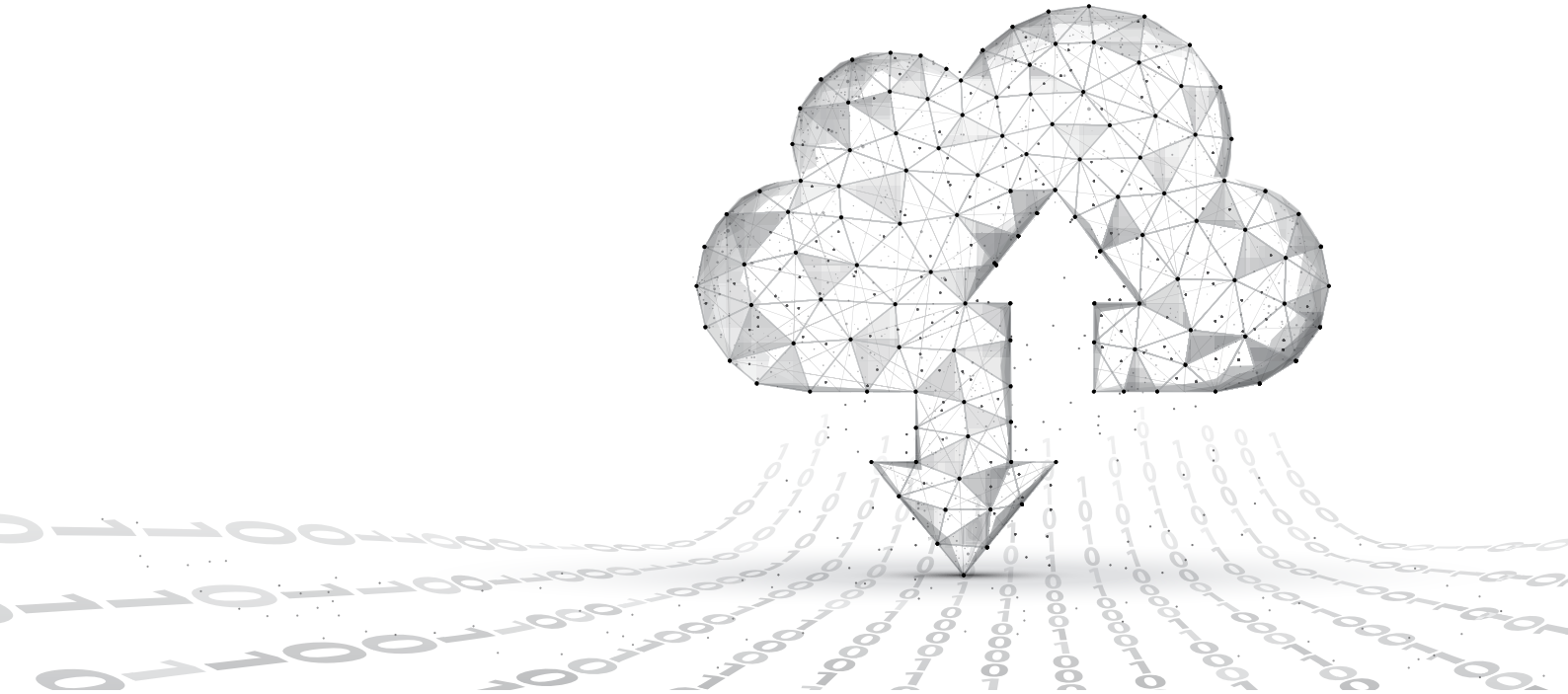
- Network Security: Administrator/Engineer/Analyst:
- Cybersecurity: Engineer/Analyst
- Cloud: Administrator/Analyst/Engineer
- InfoSec professionals
- C|ND professionals

OR

- Any other role that involves network/cloud administration, management, and operations

Certification Prerequisites:

- Should have a working knowledge of network security management
- Basic understanding of cloud computing concepts



Certified Cloud Security Engineer (C|CSE) Training and Examination:

Training:

Delivery Mode: Online via iClass (Asynchronous)
Training Duration: 5 Days

Examination:

- **Exam Code:** 312-40
- **Number of Questions:** 125
- **Duration:** 4 hours
- **Test Format:** Multiple Choice
- **Cut scores range:** 60% to 78%
- **Availability:** EC-Council Exam Portal

More Reasons to Choose the C|CSE Program

- Professional Instruction, Comprehensive Courseware, Hands-on Labs, and Certification Examination Vouchers are all included in the program fee.
- Participants will receive 1 full year's access to the training materials and access and reinforce skills and abilities learned throughout the year.
- Practice and hone Cloud Security skills with 6 months of access to the hands-on labs.
- Participants who successfully pass the certification exam receive a certification and digital badge.

About **EC-Council**

EC-Council invented the Certified Ethical Hacker. Founded in 2001 in response to 9/11, EC-Council's mission is to provide the training and certifications apprentice and experienced cybersecurity professionals need to keep corporations, government agencies, and others who employ them safe from attack.

Best known for its Certified Ethical Hacker program, EC-Council today offers 200 different trainings, certificates, and degrees in everything from Computer Forensic Investigation and Security Analysis to Threat Intelligence and Information Security. An ISO/IEC 17024 Accredited Organization recognized under the US Defense Department Directive 8140/8570 and many other authoritative cybersecurity bodies worldwide, the company has certified over 350,000 professionals across the globe. EC-Council is the gold standard in cybersecurity education and certification, trusted by seven of the Fortune 10, half of the Fortune 100, and the intelligence communities of 140 nations.

A truly global organization with a driving belief in bringing diversity, equity, and inclusion to the modern cybersecurity workforce, EC-Council maintains 11 offices in the US, the UK, India, Malaysia, Singapore, and Indonesia. The company can be reached online at **www.eccouncil.org**

EC-Council

Building A Culture Of Security

C|CSE

Certified Cloud Security Engineer

www.eccouncil.org