C|CSE
Certified Cloud Security Engineer

EC-Council
Building A Culture Of Security

Certified Cloud Security Engineer (CCSE) v2

Exam Blueprint

Certified Cloud Security Engineer (CCSE) v2

Exam Blueprint

(Version 2)

S. No.	Domains	Sub-domains	Weightage
1	**Introduction to Cloud Security**	▪ Cloud Computing Fundamentals ▪ Cloud Security Objectives and Issues ▪ Cloud Security Insights ▪ Evaluate CSPs for Security before Consuming a Cloud Service ▪ Security Shared Responsibility Model in Amazon Cloud (AWS) ▪ Security Shared Responsibility Model in Microsoft Azure Cloud ▪ Discuss Security Shared Responsibility Model in Google Cloud Platform (GCP)	**8%**
2	**Platform and Infrastructure Security in Cloud**	▪ Understand Cloud Platform and Infrastructure ▪ Risks and Threats Associated with Cloud Platform and Infrastructure ▪ Secure the Key Components of Cloud Platform and Infrastructure ▪ Design a Secure Data Center in Cloud ▪ Cloud Platform and Infrastructure Security in AWS ▪ Implement Cloud Platform and Infrastructure Security in AWS ▪ Cloud Platform and Infrastructure Security in GCP	**12%**

		▪ Implement Cloud Platform and Infrastructure Security in Google ▪ Cloud Platform and Infrastructure Security in Microsoft Azure ▪ Implement Cloud Platform and Infrastructure Security in Microsoft Azure	
3	**Application Security in Cloud**	▪ Understand Cloud Application Security ▪ Cloud application security risks ▪ Secure Software Development Lifecycle (SSDLC) of Cloud Applications ▪ DevOps and Continuous Integration/ Continuous Deployment (CI/CD) ▪ Cloud application security controls ▪ Application Security Features in AWS ▪ Implement Application Security in AWS ▪ Application Security Features in Azure ▪ Implement Application Security in Azure ▪ Application Security Features in GCP ▪ Implement Application Security in GCP	**12%**
4	**Data Security in Cloud**	▪ Understand Data Security in Cloud ▪ Cloud data storage fundamentals ▪ Cloud storage architecture and life cycle phases ▪ Risks, attacks, and issues in cloud data storage ▪ Data security strategies and technologies in the cloud ▪ Information Rights management Systems ▪ Data retention and archiving strategies ▪ Storage and Analysis of Data events ▪ Storage services in Amazon Webservices (AWS) ▪ Implement data security in Amazon Webservices (AWS)	**12%**

		▪ Storage services in Google Cloud Platform (GCP) ▪ Implement data security in Google Cloud Platform (GCP) ▪ Storage services in Microsoft Azure ▪ Implement data security in Microsoft Azure	
5	**Security Operations in Cloud**	▪ Discuss cloud security operations ▪ Elements (standards and methods) in cloud data center physical/logical Operations ▪ Security Operations to Build Cloud Infrastructure ▪ Perform Security Operations for Cloud Infrastructures ▪ Security Operations to Manage Cloud Infrastructure ▪ Security Configurations Management for Cloud Infrastructure ▪ Monitor Security Operations for Cloud Infrastructure ▪ Security operations in Microsoft Azure ▪ Implement security operations in Microsoft Azure ▪ Security operations in Amazon Webservices (AWS) ▪ Implement security operations in Amazon Webservices (AWS) ▪ Security operations in Google Cloud Platform (GCP) ▪ Implement security operations in Google Cloud Platform (GCP)	**8%**
6	**Penetration Testing in Cloud**	▪ Scope of cloud penetration testing ▪ Generic penetration testing steps in the cloud ▪ AWS-specific penetration testing steps ▪ Azure-specific penetration testing steps ▪ GCP-specific penetration testing steps	**8%**

7	**Incident Response in Cloud**	▪ Understand Cloud Incident Response ▪ Cloud Incident Response Lifecycle ▪ Understand How SOAR Accelerates Incident Response ▪ Security Incident Response in AWS ▪ AWS Investigation and Detection Tools ▪ Security Incident Response in Microsoft Azure Cloud ▪ Security Incident Response in Google Cloud Platform (GCP)	**8%**
8	**Forensic Investigation in Cloud**	▪ Discuss cloud forensics ▪ Investigate security incidents in Amazon Web Services (AWS) ▪ Investigate security incidents in Microsoft Azure ▪ Investigate security incidents in Google Cloud Platform (GCP)	**8%**
9	**Business Continuity and Disaster Recovery in Cloud**	▪ Discuss Cloud Disaster Recovery and Business Continuity ▪ Design Disaster Recovery and Business Continuity in Cloud ▪ Architect Recovery and Resilience in AWS ▪ Implement Recovery and Resilience in AWS ▪ Business Continuity and Disaster Recovery in Microsoft Azure ▪ Disaster Recovery Configurations in Azure ▪ Implement BC/DR with Azure SQL Database ▪ Configure BCDR for Azure Stack Edge VPN ▪ Various Disaster Recovery Scenarios in Azure ▪ Implement BCDR in Azure ▪ Azure Partner Solutions for BCDR ▪ BC/DR in Google Cloud Platform (GCP)	**8%**

		▪ GCP Resources for Disaster Recovery (DR) and Business Continuity Plan (BCP) ▪ Disaster Recovery for Data in GCP ▪ Disaster Recovery for Applications in GCP ▪ Architect DR for Cloud Infrastructure Outages ▪ Implement BCDR in Google Cloud Platform (GCP) ▪ Partners Solutions for Implementing BCDR in GCP	
10	**Governance, Risk Management, and Compliance in Cloud**	▪ Understand GRC in the Cloud ▪ Cloud Governance ▪ Implement and Maintain Governance for Cloud Computing ▪ Risk management in the Cloud ▪ Risk Management Framework and Process in the Cloud ▪ Cloud Compliance ▪ Implement GRC in the cloud ▪ GRC in Amazon Web Services (AWS) ▪ GRC in Azure ▪ GRC in Google Cloud Platform (GCP)	**8%**
11	**Standards, Policies, and Legal Issues in Cloud**	▪ Laws Impacting Cloud Computing ▪ Cloud Computing Standards ▪ Legal Frameworks for Data Protection and Privacy ▪ Audit Planning and Reporting in the Cloud ▪ Outsourcing and Vendor Management ▪ Standards, Policies, and Auditing in AWS ▪ Standards, Policies, and Auditing in Azure ▪ Standards, Policies, and Auditing in GCP	**8%**