CCSP Certified Cloud Security Professional Certification Preparation

Learn via: **Classroom**

Duration: **5 Day**

https://bilginc.com/en/training/ccsp-certified-cloud-security-professional-certification-preparation-1453-training/

Overview

(ISC)^2 developed the Certified Cloud Security Professional (CCSP) credential to ensure that cloud security professionals have the required knowledge, skills, and abilities in cloud security design, implementation, architecture, operations, controls, and compliance with regulatory frameworks. A CCSP applies information security expertise to a cloud computing environment and demonstrates competence in cloud security architecture, design, operations, and service orchestration. This professional competence is measured against a globally recognized body of knowledge.

The topics included in the CCSP Common Body of Knowledge (CBK) ensure its relevancy across all disciplines in the field of cloud security. Successful candidates are competent in the following 6 domains:

- Cloud Concepts, Architecture and Design
- Cloud Data Security
- Cloud Platform & Infrastructure Security
- Cloud Application Security
- Cloud Security Operations
- Legal, Risk and Compliance

The (ISC)^2 CCSP exam is included in this course.

Prerequisites

Candidates must have a minimum of 5 years cumulative paid work experience in information technology, of which 3 years must be in information security and 1 year in 1 or more of the 6 domains of the CCSP CBK. Earning CSA's CCSK certificate can be substituted for 1 year of experience in 1 or more of the 6 domains of the CCSP CBK. Earning (ISC)^2's CISSP credential can be substituted for the entire CCSP experience requirement.

A candidate that doesn't have the required experience to become a CCSP may become an Associate of (ISC)^2 by successfully passing the CCSP examination. The Associate of (ISC)^2 will then have 6 years to earn the 5 years required experience. You can learn more about CCSP experience requirements and how to account for part-time work and internships at www.isc2.org/Certifications/CCSP/experience-requirements.

What You Will Learn

You will learn how to:

- Identify and explain the five characteristics required to satisfy the NIST definition of cloud computing
- Differentiate between various as-a-service delivery models and frameworks that are incorporated into the cloud computing reference architecture
- Explain strategies for protecting data at rest and data in motion
- Discuss strategies for safeguarding data, classifying data, ensuring privacy, assuring compliance with regulatory agencies, and working with authorities during legal investigations
- Contrast between forensic analysis in corporate data center and cloud computing environments

Outline

On August 1, 2022, (ISC)^2 will refresh the CCSP credential exam. These updates are the result of the Job Task Analysis (JTA), which is an analysis of the current content of the credential evaluated by (ISC)^2 members on a triennial cycle. The domain weights for the CCSP have changed as noted inbelow:

CCSP Domains Weight:

- Cloud Concepts, Architecture and Design 17%
- Cloud Data Security 20%
- Cloud Platform & Infrastructure Security 17%
- Cloud Application Security 17%
- Cloud Security Operations 16%

- Legal, Risk and Compliance 13%

Domain 1: Cloud Concepts, Architecture and Design

- Understand Cloud Computing Concepts
  - Cloud Computing Definitions
  - Cloud Computing Roles (e.g., cloud service customer, cloud service provider, cloud service partner, cloud service broker)
  - Key Cloud Computing Characteristics (e.g., on-demand self-service, broad network access, multi-tenancy, rapid elasticity and scalability, resource pooling, measured service)
  - Building Block Technologies (e.g., virtualization, storage, networking, databases, orchestration)
- Describe Cloud Reference Architecture
- Understand Security Concepts Relevant to Cloud Computing
- Understand Design Principles of Secure Cloud Computing
  - Cloud Secure Data Lifecycle
  - Cloud based Disaster Recovery (DR) and Business Continuity (BC) planning
  - Cost Benefit Analysis
  - Functional Security Requirements (e.g., portability, interoperability, vendor lock-in)
  - Security Considerations for Different Cloud Categories (e.g., Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS))
- Evaluate Cloud Service Providers
  - Verification Against Criteria (e.g., International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27017, Payment Card Industry Data Security Standard (PCI DSS))
  - System/subsystem Product Certifications (e.g., Common Criteria (CC), Federal Information Processing Standard (FIPS) 140-2)
  - Cloud Computing Activities
  - Cloud Service Capabilities (e.g., application capability types, platform capability types, infrastructure capability types)
  - Cloud Service Categories (e.g., Software as a Service (SaaS), Infrastructure as a Service (IaaS),
  - Platform as a Service (PaaS))
  - Cloud Deployment Models (e.g., public, private, hybrid, community)
  - Cloud Shared Considerations (e.g., interoperability, portability, reversibility, availability, security, privacy, resiliency, performance, governance, maintenance and versioning, service levels and Service Level Agreements (SLA), auditability, regulatory)
  - Impact of Related Technologies (e.g., machine learning, artificial intelligence, blockchain,
  - Internet of Things (IoT), containers, quantum computing)
  - Cryptography and Key Management
  - Access Control
  - Data and Media Sanitization (e.g., overwriting, cryptographic erase)
  - Network Security (e.g., network security groups)
  - Virtualization Security (e.g., hypervisor security, container security)
  - Common Threats
- Describe Cloud Data Concepts
  - Cloud Data Life Cycle Phases
  - Data Dispersion
- Design and Implement Cloud Data Storage Architectures
  - Storage Types (e.g. long term, ephemeral, raw-disk)
  - Threats to Storage Types
- Design and Apply Data Security Technologies and Strategies
- Implement Data Discovery
  - Structured Data
  - Unstructured Data
- Implement Data Classification
- Design and Implement Information Rights Management (IRM)
  - Objectives (e.g., data rights, provisioning, access models)
  - Appropriate Tools (e.g., issuing and revocation of certificates)

Domain 2: Cloud Data Security

- Encryption and Key Management
- Hashing
- Masking
- Tokenization
- Data Loss Prevention (DLP)
- Data Obfuscation
- Data De-identification (e.g., anonymization)
- Mapping
- Labelling
- Sensitive data (e.g., Protected Health Information (PHI), Personally Identifiable Information (PII), card holder data)
- Plan and Implement Data Retention, Deletion and Archiving Policies
- Data Retention Policies
- Data Deletion Procedures and Mechanisms
- Data Archiving Procedures and Mechanisms
- Legal Hold
- Design and Implement Auditability, Traceability and Accountability of Data Events
  - Definition of Event Sources and Requirement of Identity Attribution

    - Logging, Storage and Analysis of Data Events
    - Chain of Custody and Non-repudiation
- Comprehend Cloud Infrastructure Components
- Design a Secure Data Center
    - Logical Design (e.g., tenant partitioning, access control)
    - Physical Design (e.g. location, buy or build)
    - Environmental Design (e.g., Heating, Ventilation and Air Conditioning (HVAC), multi-vendor pathway connectivity)
- Analyze Risks Associated with Cloud Infrastructure
- Design and Plan Security Controls
- Plan Disaster Recovery (DR) and Business Continuity (BC)

Domain 3: Cloud Platform and Infrastructure Security

- Physical Environment
- Network and Communications
- Compute
- Virtualization
- Storage
- Management Plane
- Risk Assessment and Analysis
- Cloud Vulnerabilities, Threats and Attacks
- Virtualization Risks
- Counter-measure Strategies
- Physical and Environmental Protection (e.g., on-premise)
- System and Communication Protection
- Virtualization Systems Protection
- Identification, Authentication and Authorization in Cloud Infrastructure
- Audit Mechanisms (e.g., log collection, packet capture)
- Risks Related to the Cloud Environment
- Business Requirements (e.g., Recovery Time Objective (RTO), Recovery Point Objective (RPO), Recovery Service Level (RSL))
- Business Continuity/Disaster Recovery Strategy
- Creation, Implementation and Testing of Plan

Domain 4:Cloud Application Security

- Advocate Training and Awareness for Application Security
    - Cloud Development Basics
    - Common Pitfalls
    - Common Cloud Vulnerabilities
- Describe the Secure Software Development Life Cycle (SDLC) Process
    - Business Requirements
    - Phases and Methodologies
- Apply the Secure Software Development Life Cycle (SDLC)
- Apply Cloud Software Assurance and Validation
    - Functional Testing
    - Security Testing Methodologies
- Use Verified Secure Software
    - Approved Application Programming Interfaces (API)
    - Supply-chain Management
    - Third Party Software Management
    - Validated Open Source Software
    - Avoid Common Vulnerabilities During Development
    - Cloud-specific Risks
    - Quality Assurance
    - Threat Modelling
    - Software Configuration Management and Versioning
- Comprehend the Specifics of Cloud Application Architecture
- Supplemental Security components (e.g., Web Application Firewall (WAF), Database Activity Monitoring
- (DAM), Extensible Markup Language (XML) firewalls, Application Programming Interface (API) gateway)
    - Cryptography
    - Sandboxing
    - Application Virtualization and Orchestration
- Design Appropriate Identity and Access Management (IAM) Solutions
    - Federated Identity
    - Identity Providers
    - Single Sign-On (SSO)
    - Multi-factor Authentication
    - Cloud Access Security Broker (CASB)
- Implement and Build Physical and Logical Infrastructure for Cloud Environment
    - Hardware Specific Security Configuration Requirements (e.g., Basic Input Output System (BIOS), settings for virtualization and Trusted Platform Module (TPM), storage controllers, network controllers)
    - Installation and Configuration of Virtualization Management Tools

    - Virtual Hardware Specific Security Configuration Requirements (e.g., network, storage, memory, Central Processing Unit (CPU)
    - Installation of Guest Operating System (OS) Virtualization Toolsets
- Operate Physical and Logical Infrastructure for Cloud Environment
- Manage Physical and Logical Infrastructure for Cloud Environment

Domain 5: Cloud Security Operations

- Access Controls for Remote Access (e.g., Remote Desktop Protocol (RDP), Secure Terminal Access, Secure Shell (SSH))
- Operating System (OS) Baseline Compliance
- Monitoring and Remediation
- Patch Management
- Performance and Capacity Monitoring (e.g., network, compute, storage, response time)
- Hardware Monitoring (e.g., Disk, Central Processing Unit (CPU), fan speed, temperature)
- Configuration of Host and Guest Operating System (OS) Backup and Restore Functions
- Network Security Controls (e.g., firewalls, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), honeypots, vulnerability assessments, network security groups)
- Management Plane (e.g., scheduling, orchestration, maintenance)
- Configure Access Control for Local and Remote Access (e.g., Secure Keyboard Video Mouse (KVM), console-based access mechanisms, Remote Desktop Protocol (RDP))
- Secure Network Configuration (e.g., Virtual Local Area Networks (VLAN), Transport Layer Security (TLS), Dynamic Host Configuration Protocol (DHCP), Domain Name System (DNS), Virtual Private Network (VPN))
- Operating System (OS) Hardening Through the Application of Baselines (e.g., Windows, Linux, VMware)
- Availability of Stand-Alone Hosts
- Availability of Clustered Hosts (e.g., Distributed Resource Scheduling (DRS), Dynamic
- Optimization (DO), storage clusters, maintenance mode, High Availability)
- Availability of Guest Operating System (OS)
- Change Management
- Continuity Management
- Information Security Management
- Continual Service Improvement Management
- Incident Management
- Problem Management
- Release Management
- Deployment Management
- Configuration Management
- Service level Management
- Availability Management
- Capacity Management
- Vendors
- Customers
- Partners
- Regulators
- Other Stakeholders
- Implement Operational Controls and Standards (e.g., Information Technology
- Infrastructure Library (ITIL), International Organization for Standardization/International
- Electrotechnical Commission (ISO/IEC) 20000-1)
- Support Digital Forensics
    - Forensic Data Collection Methodologies
    - Evidence Management
    - Collect, Acquire and Preserve Digital Evidence
- Manage Communication with Relevant Parties
- Manage Security Operations
    - Security Operations Center (SOC)
    - Monitoring of Security Controls (e.g., firewalls, Intrusion Detection Systems (IDS),
    - Intrusion Prevention Systems (IPS), honeypots, vulnerability assessments, network security groups)
    - Log Capture and Analysis (e.g., Security Information and Event Management (SIEM), log management)
    - Incident Management
- Articulate Legal Requirements and Unique Risks within the Cloud Environment
- Understand Privacy Issues
    - Difference Between Contractual and Regulated Private Data (e.g., Protected Health Information (PHI), Personally Identifiable Information (PII))
    - Country-Specific Legislation Related to Private Data (e.g., Protected Health Information (PHI), Personally Identifiable Information (PII))
    - Jurisdictional Differences in Data Privacy
    - Standard Privacy Requirements (e.g., International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27018, Generally Accepted Privacy Principles (GAPP), General Data Protection Regulation (GDPR))
- Understand Audit Process, Methodologies, and Required Adaptations for a Cloud Environment

Domain 6: Legal, Risk and Compliance

- Conflicting International Legislation
- Evaluation of Legal Risks Specific to Cloud Computing
- Legal Framework and Guidelines
- eDiscovery (e.g., International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27050, Cloud Security Alliance

(CSA) Guidance)
- Forensics Requirements
- Internal and External Audit Controls
- Impact of Audit Requirements
- Identify Assurance Challenges of Virtualization and Cloud
- Types of Audit Reports (e.g., Statement on Standards for Attestation Engagements (SSAE), Service Organization Control (SOC), International Standard on Assurance Engagement (ISAE))
- Restrictions of Audit Scope Statements (e.g., Statement on Standards for Attestation Engagements (SSAE), International Standard on Assurance Engagements (ISAE))
- Gap Analysis
- Audit Planning
- Internal Information Security Management System (ISMS)
- Internal Information Security Controls System
- Policies (e.g., organizational, functional, cloud computing)
- Identification and Involvement of Relevant Stakeholders
- Specialized Compliance Requirements for Highly-Regulated Industries (e.g., North American Electric Reliability Corporation/ Critical Infrastructure Protection (NERC/CIP), Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry (PCI))
- Impact of Distributed Information Technology (IT) Model (e.g., diverse geographical locations and crossing over legal jurisdictions)
- Understand Implications of Cloud to Enterprise Risk Management
- Understand Outsourcing and Cloud Contract Design
    - Business Requirements (e.g., Service Level Agreement (SLA), Master Service Agreement (MSA), Statement of Work (SOW))
    - Vendor Management
    - Contract Management (e.g., right to audit, metrics, definitions, termination, litigation, assurance, compliance, access to cloud/data, cyber risk insurance)
    - Supply-Chain Management (e.g., International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27036)