Certified Cloud Security Professional

Certification **Exam Outline**

Effective Date: April 2015

(ISC)² INSPIRING A SAFE AND SECURE CYBER WORLD.

About CCSP

(ISC)² and the Cloud Security Alliance (CSA) 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 CCSP is a stand-alone credential that complements and builds upon existing credentials and educational programs, including (ISC)²'s Certified Information Systems Security Professional (CISSP) and CSA's Certificate of Cloud Security Knowledge (CCSK).

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:

- Architectural Concepts & Design Requirements
- Cloud Data Security
- Cloud Platform & Infrastructure Security
- Cloud Application Security
- Operations
- Legal & Compliance

Experience Requirements

Candidates must have a minimum of 5 years cumulative paid full-time 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.

Accreditation

CCSP under ANSI review for compliance with the stringent requirements of ANSI/ISO/IEC Standard 17024.

Job Task Analysis (JTA)

(ISC)² has an obligation to its membership to maintain the relevancy of the CCSP. Conducted at regular intervals, the Job Task Analysis (JTA) is a methodical and critical process of determining the tasks that are performed by security professionals who are engaged in the profession defined by the CCSP. The results of the JTA are used to update the examination. This process ensures that candidates are tested on the topic areas relevant to the roles and responsibilities of today's practicing information security professionals focusing on cloud technologies.

CCSP Examination Information

Length of exam	4 hours
Number of questions	125
Question format	Multiple choice
Passing grade	700 out of 1000 points
Exam availability	English
Testing center	Pearson VUE Testing Center

CCSP Examination Weights

Domains	Weight
1. Architectural Concepts & Design Requirements	19%
2. Cloud Data Security	20%
3. Cloud Platform & Infrastructure Security	19%
4. Cloud Application Security	15%
5. Operations	15%
6. Legal & Compliance	12%
Total:	**100%**

Domain 1: Architectural Concepts and Design Requirements

1.1 Understand Cloud Computing Concepts

- Cloud Computing Definitions (ISO/IEC 17788)
- Cloud Computing Roles (i.e., Cloud Service Customer, Cloud Service Provider, and Cloud Service Partner)
- 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)

1.2 Describe Cloud Reference Architecture

- Cloud Computing Activities (ISO/IEC 17789, Clause 9)
- Cloud Service Capabilities (i.e., application capability type, platform capability type, infrastructure capability types)
- Cloud Service Categories (e.g., SaaS, IaaS, PaaS, NaaS, CompaaS, DSaaS)
- Cloud Deployment Models (e.g., public, private, hybrid, community)
- Cloud Cross-Cutting Aspects (e.g., interoperability, portability, reversibility, availability, security, privacy, resiliency, performance, governance, maintenance and versioning, service levels and service level agreement, auditability, and regulatory)

1.3 Understand Security Concepts Relevant to Cloud Computing

- Cryptography (e.g. encryption, in motion, at rest, key management)
- Access Control
- Data and Media Sanitization (e.g., overwriting, cryptographic erase)
- Network security
- Virtualization Security (e.g., hypervisor security)
- Common Threats
- Security Considerations for different Cloud Categories (e.g., SaaS, PaaS, *aaS)

1.4 Understand Design Principles of Secure Cloud Computing

- Cloud Secure Data Lifecycle
- Cloud Based Business Continuity/Disaster Recovery Planning
- Cost Benefit Analysis
- Functional Security Requirements (e.g., portability, interoperability, vendor lock-in)

1.5 Identify Trusted Cloud Services

- Certification Against Criteria
- System/Subsystem Product Certifications (e.g., common criteria, FIPS 140-2)

Domain 2: Cloud Data Security

2.1 Understand Cloud Data Lifecycle (CSA Guidance)

- Phases
- Relevant Data Security Technologies

2.2 Design and Implement Cloud Data Storage Architectures

- Storage Types (e.g. long term, ephemeral, raw-disk)
- Threats to Storage Types (e.g., ISO/IEC 27040)
- Technologies Available to Address Threats (e.g., encryption)

2.3 Design and Apply Data Security Strategies

- Encryption
- Key Management
- Masking
- Tokenization
- Application of Technologies (e.g., time of storage vs. encryption needs)
- Emerging Technologies (e.g., bit splitting, data obfuscation, homomorphic encryption)

2.4 Understand and Implement Data Discovery and Classification Technologies

- Data Discovery
- Classification

2.5 Design and Implement Relevant Jurisdictional Data Protections for Personally Identifiable Information (PII)

- Data Privacy Acts
- Implementation of Data Discovery
- Classification of Discovered Sensitive Data
- Mapping and Definition of Controls
- Application of Defined Controls for PII (in consideration of customer's Data Privacy Acts)

2.6 Design and Implement Data Rights Management

- Data Rights Objectives (e.g. provisioning, users and roles, role-based access)
- Appropriate Tools (e.g., Issuing and replication of certificates)

2.7 Plan and Implement Data Retention, Deletion, and Archiving Policies

- Data Retention Policies
- Data Deletion Procedures and Mechanisms
- Data Archiving Procedures and Mechanisms

2.8 Design and Implement Auditability, Traceability and Accountability of Data Events

- Definition of Event Sources and Identity Attribution Requirement
- Data Event Logging
- Storage and Analysis of Data Events (e.g. security information and event management)
- Continuous Optimizations (e.g. new events detected, add new rules, reductions of false positives)
- Chain of Custody and Non-repudiation

Domain 3: Cloud Platform and Infrastructure Security

3.1 Comprehend Cloud Infrastructure Components

- Physical Environment
- Network and Communications
- Compute
- Virtualization
- Storage
- Management Plane

3.2 Analyze Risks Associated to Cloud Infrastructure

- Risk Assessment/Analysis
- Cloud Attack Vectors
- Virtualization Risks
- Counter-Measure Strategies (e.g., access controls, design principles)

3.3 Design and Plan Security Controls

- Physical and Environmental Protection (e.g., on-premise)
- System and Communication Protection
- Virtualization Systems Protection
- Management of Identification, Authentication and Authorization in Cloud Infrastructure
- Audit Mechanisms

3.4 Plan Disaster Recovery and Business Continuity Management

- Understanding of the Cloud Environment
- Understanding of the Business Requirements
- Understanding of the Risks
- Disaster Recovery/Business Continuity strategy
- Creation of the Plan
- Implementation of the Plan

Domain 4: Cloud Application Security

4.1 Recognize the need for Training and Awareness in Application Security

- Cloud Development Basics (e.g., RESTful)
- Common Pitfalls
- Common Vulnerabilities (e.g. OWASP Top 10)

4.2 Understand Cloud Software Assurance and Validation

- Cloud-based Functional Testing
- Cloud Secure Development Lifecycle
- Security Testing (e.g., SAST, DAST, Pen Testing)

4.3 Use Verified Secure Software

- Approved API
- Supply-Chain Management
- Community Knowledge

4.4 Comprehend the Software Development Life-Cycle (SDLC) Process

- Phases & Methodologies
- Business Requirements
- Software Configuration Management & Versioning

4.5 Apply the Secure Software Development Life-Cycle

- Common Vulnerabilities (e.g., SQL Injection, XSS, XSRF, Direct Object Reference, Buffer Overflow)
- Cloud-Specific Risks
- Quality of Service
- Threat Modeling

4.6 Comprehend the Specifics of Cloud Application Architecture

- Supplemental Security Devices (e.g., WAF, DAM, XML firewalls, API gateway)
- Cryptography (e.g. TLS, SSL, IPSEC)
- Sandboxing
- Application Virtualization

4.7 Design Appropriate Identity and Access Management (IAM) Solutions

- Federated Identity
- Identity Providers
- Single Sign-On
- Multi-factor Authentication

Domain 5: Operations

5.1 Support the Planning Process for the Data Center Design

- Logical Design (e.g., tenant partitioning, access control)
- Physical Design (e.g., location, buy or build)
- Environmental Design (e.g., HVAC, multi-vendor pathway connectivity)

5.2 Implement and Build Physical Infrastructure for Cloud Environment

- Secure Configuration of Hardware Specific Requirements (e.g., BIOS settings for virtualization and TPM, storage controllers, network controllers)
- Installation and Configuration of Virtualization Management Tools for the Host

5.3 Run Physical Infrastructure for Cloud Environment

- Configuration of Access Control for Local Access (e.g., Secure KVM, Console based access mechanisms)
- Securing Network Configuration (e.g., VLAN's, TLS, DHCP, DNS, IPSEC)
- OS Hardening via Application of Baseline (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)

5.4 Manage Physical Infrastructure for Cloud Environment

- Configuring Access Controls for Remote Access (e.g., RDP, Secure Terminal Access)
- OS Baseline Compliance Monitoring and Remediation
- Patch Management
- Performance Monitoring (e.g., network, disk, memory, CPU)
- Hardware Monitoring (e.g., disk I/O, CPU temperature, fan speed)
- Backup and Restore of Host Configuration
- Implementation of Network Security Controls (e.g., firewalls, IDS, IPS, honeypots, vulnerability assessments)
- Log Capture and Analysis (e.g., SIEM, Log Management)
- Management Plane (e.g., scheduling, orchestration, maintenance)

5.5 Build Logical Infrastructure for Cloud Environment

- Secure Configuration of Virtual Hardware Specific Requirements (e.g., network, storage, memory, CPU)
- Installation of Guest O/S Virtualization Toolsets

5.6 Run Logical Infrastructure for Cloud Environment

- Secure Network Configuration (e.g., VLAN's, TLS, DHCP, DNS, IPSEC)
- OS Hardening via Application of a Baseline (e.g., Windows, Linux, VMware)
- Availability of the Guest OS

5.7 Manage Logical Infrastructure for Cloud Environment

- Access Control for Remote Access (e.g., RDP)
- OS Baseline Compliance Monitoring and Remediation
- Patch Management
- Performance Monitoring (e.g., Network, Disk, Memory, CPU)
- Backup and Restore of Guest OS Configuration (e.g., Agent based, SnapShots, Agentless)
- Implementation of Network Security Controls (e.g., firewalls, IDS, IPS, honeypots, vulnerability assessments)
- Log Capture and Analysis (e.g., SIEM, log management)
- Management Plane (e.g., scheduling, orchestration, maintenance)

5.8 Ensure Compliance with Regulations and Controls (e.g., ITIL, ISO/IEC 20000-1)

- 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

5.9 Conduct Risk Assesment to Logical and Physical Infrastructure

5.10 Understand the Collection, Acquisition and Preservation of Digital Evidence

- Proper Methodologies for Forensic Collection of Data
- Evidence Management

5.11 Manage Communication with Relevant Parties

- Vendors
- Customers
- Partners
- Regulators
- Other Stakeholders

Domain 6: Legal and Compliance

6.1 Understand Legal Requirements and Unique Risks within the Cloud Environment

- International Legislation Conflicts
- Appraisal of Legal Risks Specific to Cloud Computing
- Legal Controls
- eDiscovery (e.g., ISO/IEC 27050, CSA Guidance)
- Forensics Requirements

6.2 Understand Privacy Issues, Including Jurisdictional Variation

- Difference between Contractual and Regulated PII
- Country-Specific Legislation Related to PII / Data Privacy
- Difference Among Confidentiality, Integrity, Availability, and Privacy

6.3 Understand Audit Process, Methodologies, and Required Adaptations for a Cloud Environment

- Internal and External Audit Controls
- Impact of Requirements Programs by the Use of Cloud
- Assurance Challenges of Virtualization and Cloud
- Types of Audit Reports (e.g., SAS, SSAE, ISAE)
- Restrictions of Audit Scope Statements (e.g., SAS 70)
- Gap Analysis
- Audit Plan
- Standards Requirements (e.g., ISO/IEC 27018, GAPP)
- Internal Information Security Management System
- Internal information Security Controls System
- Policies
- Identification and Involvement of Relevant Stakeholders
- Specialized Compliance Requirements for Highly Regulated Industries
- Impact of Distributed IT Model (e.g., diverse geographical locations and crossing over legal jurisdictions)

6.4 Understand Implications of Cloud to Enterprise Risk Management

- Access Providers Risk Management
- Difference between Data Owner/Controller vs. Data Custodian/Processor (e.g., risk profile, risk appetite, responsibility)
- Provision of Regulatory Transparency Requirements
- Risk Mitigation
- Different Risk Frameworks
- Metrics for Risk Management
- Assessment of Risk Environment (e.g., service, vendor, ecosystem)

6.5 Understand Outsourcing and Cloud Contract Design

- Business Requirements (e.g., SLA, GAAP)
- Vendor Management (e.g., selection, common certification framework)
- Contract Management (e.g., right to audit, metrics, definitions, termination, litigation, assurance, compliance, access to cloud/data)

6.6 Execute Vendor Management

- Supply-chain Management (e.g., ISO/IEC 27036)

Additional Examination Information

Supplementary References

Candidates are encouraged to supplement their education and experience by reviewing relevant resources that pertain to the CBK and identifying areas of study that may need additional attention.

View the full list of supplementary references at www.isc2.org/ccsp-cbk-references.

Examination Policies and Procedures

(ISC)² recommends that CCSP candidates review exam policies and procedures prior to registering for the examination. Read the comprehensive breakdown of this important information at www.isc2.org/exam-policies-procedures.

Legal Info

For any questions related to (ISC)²'s legal policies, please contact the (ISC)² Legal Department at legal@isc2.org.

Any Questions?

(ISC)² Candidate Services
311 Park Place Blvd, Suite 400
Clearwater, FL 33759

(ISC)² Americas
Tel: +1.727.785.0189
Email: info@isc2.org

(ISC)² Asia Pacific
Tel: +(852) 28506951
Email: isc2asia@isc2.org

(ISC)² EMEA
Tel: +44 (0)203 300 1625
Email: info-emea@isc2.org

(ISC)² INSPIRING A SAFE AND SECURE CYBER WORLD.