CCSP®

Certified Cloud Security Professional

An (ISC)² Certification

Certification **Exam Outline**

Effective Date: August 1, 2022

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

About CCSP

(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 six domains:

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

Experience Requirements

Candidates must have a minimum of five years cumulative paid work experience in information technology, of which three years must be in information security and one year in one or more of the six domains of the CCSP CBK. Earning CSA's CCSK certificate can be substituted for one year of experience in one or more of the six 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 six years to earn the five 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.

Accreditation

CCSP is in 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	3 hours
Number of items	125
Item format	Multiple choice
Passing grade	700 out of 1000 points
Exam availability	English, Japanese
Testing center	Pearson VUE Testing Center

CCSP Examination Weights

Domains	Weight
1. Cloud Concepts, Architecture and Design	17%
2. Cloud Data Security	20%
3. Cloud Platform and Infrastructure Security	17%
4. Cloud Application Security	17%
5. Cloud Security Operations	16%
6. Legal, Risk and Compliance	13%
Total:	**100%**

Domain 1:
Cloud Concepts, Architecture and Design

1.1 Understand cloud computing concepts

- Cloud computing definitions
- Cloud computing roles and responsibilities (e.g., cloud service customer, cloud service provider, cloud service partner, cloud service broker, regulator)
- 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)

1.2 Describe cloud reference architecture

- 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, multi-cloud)
- 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, outsourcing)
- Impact of related technologies (e.g., data science, machine learning, artificial intelligence (AI), blockchain, Internet of Things (IoT), containers, quantum computing, edge computing, confidential computing, DevSecOps)

1.3 Understand security concepts relevant to cloud computing

- Cryptography and key management
- Identity and access control (e.g., user access, privilege access, service access)
- Data and media sanitization (e.g., overwriting, cryptographic erase)
- Network security (e.g., network security groups, traffic inspection, geofencing, zero trust network)
- Virtualization security (e.g., hypervisor security, container security, ephemeral computing, serverless technology)
- Common threats
- Security hygiene (e.g., patching, baselining)

1.4 Understand design principles of secure cloud computing

- Cloud secure data lifecycle
- Cloud-based business continuity (BC) and disaster recovery (DR) plan
- Business impact analysis (BIA) (e.g., cost-benefit analysis, return on investment (ROI))
- Functional security requirements (e.g., portability, interoperability, vendor lock-in)
- Security considerations and responsibilities for different cloud categories (e.g., Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS))
- Cloud design patterns (e.g., SANS security principles, Well-Architected Framework, Cloud Security Alliance (CSA) Enterprise Architecture)
- DevOps security

1.5 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)

Domain 2: Cloud Data Security

2.1 Describe cloud data concepts

- Cloud data life cycle phases
- Data dispersion
- Data flows

2.2 Design and implement cloud data storage architectures

- Storage types (e.g., long-term, ephemeral, raw storage)
- Threats to storage types

2.3 Design and apply data security technologies and strategies

- Encryption and key management
- Hashing
- Data obfuscation (e.g., masking, anonymization)
- Tokenization
- Data loss prevention (DLP)
- Keys, secrets and certificates management

2.4 Implement data discovery

- Structured data
- Unstructured data
- Semi-structured data
- Data location

2.5 Plan and implement data classification

- Data classification policies
- Data mapping
- Data labeling

2.6 Design and implement Information Rights Management (IRM)

- Objectives (e.g., data rights, provisioning, access models)
- Appropriate tools (e.g., issuing and revocation 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
- Legal hold

2.8 Design and implement auditability, traceability and accountability of data events

- Definition of event sources and requirement of event attributes (e.g., identity, Internet Protocol (IP) address, geolocation)
- Logging, storage and analysis of data events
- Chain of custody and non-repudiation

Domain 3: Cloud Platform and Infrastructure Security

3.1 Comprehend cloud infrastructure and platform components

- Physical environment
- Network and communications
- Compute
- Virtualization
- Storage
- Management plane

3.2 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)
- Design resilient

3.3 Analyze risks associated with cloud infrastructure and platforms

- Risk assessment (e.g., identification, analysis)
- Cloud vulnerabilities, threats and attacks
- Risk mitigation strategies

3.4 Plan and implementation of security controls

- Physical and environmental protection (e.g., on-premises)
- System, storage and communication protection
- Identification, authentication and authorization in cloud environments
- Audit mechanisms (e.g., log collection, correlation, packet capture)

3.5 Plan business continuity (BC) and disaster recovery (DR)

- Business continuity (BC) / disaster recovery (DR) strategy
- Business requirements (e.g., Recovery Time Objective (RTO), Recovery Point Objective (RPO), recovery service level)
- Creation, implementation and testing of plan

Domain 4: Cloud Application Security

4.1 Advocate training and awareness for application security

- Cloud development basics
- Common pitfalls
- Common cloud vulnerabilities (e.g., Open Web Application Security Project (OWASP) Top-10, SANS Top-25)

4.2 Describe the Secure Software Development Life Cycle (SDLC) process

- Business requirements
- Phases and methodologies (e.g., design, code, test, maintain, waterfall vs. agile)

4.3 Apply the Secure Software Development Life Cycle (SDLC)

- Cloud-specific risks
- Threat modeling (e.g., Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege (STRIDE), Disaster, Reproducibility, Exploitability, Affected Users, and Discoverability (DREAD), Architecture, Threats, Attack Surfaces, and Mitigations (ATASM), Process for Attack Simulation and Threat Analysis (PASTA))
- Avoid common vulnerabilities during development
- Secure coding (e.g., Open Web Application Security Project (OWASP) Application Security Verification Standard (ASVS), Software Assurance Forum for Excellence in Code (SAFECode))
- Software configuration management and versioning

4.4 Apply cloud software assurance and validation

- Functional and non-functional testing
- Security testing methodologies (e.g., blackbox, whitebox, static, dynamic, Software Composition Analysis (SCA), interactive application security testing (IAST))
- Quality assurance (QA)
- Abuse case testing

4.5 Use verified secure software

- Securing application programming interfaces (API)
- Supply-chain management (e.g., vendor assessment)
- Third-party software management (e.g., licensing)
- Validated open-source software

4.6 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 (e.g., microservices, containers)

4.7 Design appropriate identity and access management (IAM) solutions

- Federated identity
- Identity providers (IdP)
- Single sign-on (SSO)
- Multi-factor authentication (MFA)
- Cloud access security broker (CASB)
- Secrets management

Domain 5: Cloud Security Operations

5.1 Build and implement physical and logical infrastructure for cloud environment

- Hardware specific security configuration requirements (e.g., hardware security module (HSM) and Trusted Platform Module (TPM))
- Installation and configuration of management tools
- Virtual hardware specific security configuration requirements (e.g., network, storage, memory, central processing unit (CPU), Hypervisor type 1 and 2)
- Installation of guest operating system (OS) virtualization toolsets

5.2 Operate and maintain physical and logical infrastructure for cloud environment

- Access controls for local and remote access (e.g., Remote Desktop Protocol (RDP), secure terminal access, Secure Shell (SSH), console-based access mechanisms, jumpboxes, virtual client)
- Secure network configuration (e.g., virtual local area networks (VLAN), Transport Layer Security (TLS), Dynamic Host Configuration Protocol (DHCP), Domain Name System Security Extensions (DNSSEC), virtual private network (VPN))
- Network security controls (e.g., firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), honeypots, vulnerability assessments, network security groups, bastion host)
- Operating system (OS) hardening through the application of baselines, monitoring and remediation (e.g., Windows, Linux, VMware)
- Patch management
- Infrastructure as Code (IaC) strategy
- Availability of clustered hosts (e.g., distributed resource scheduling, dynamic optimization, storage clusters, maintenance mode, high availability (HA))
- Availability of guest operating system (OS)
- 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
- Management plane (e.g., scheduling, orchestration, maintenance)

5.3 Implement operational controls and standards (e.g., Information Technology Infrastructure Library (ITIL), International Organization for Standardization/International Electrotechnical Commission (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

5.4 Support digital forensics

- Forensic data collection methodologies
- Evidence management
- Collect, acquire, and preserve digital evidence

5.5 Manage communication with relevant parties

- Vendors
- Customers
- Partners
- Regulators
- Other stakeholders

5.6 Manage security operations

- Security operations center (SOC)
- Intelligent monitoring of security controls (e.g., firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), honeypots, network security groups, artificial intelligence (AI))
- Log capture and analysis (e.g., security information and event management (SIEM), log management)
- Incident management
- Vulnerability assessments

Domain 6: Legal, Risk and Compliance

6.1 Articulate legal requirements and unique risks within the cloud environment

- 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

6.2 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))
- Privacy Impact Assessments (PIA)

6.3 Understand audit process, methodologies, and required adaptations for a cloud environment

- 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 Engagements (ISAE))
- Restrictions of audit scope statements (e.g., Statement on Standards for Attestation Engagements (SSAE), International Standard on Assurance Engagements (ISAE))
- Gap analysis (e.g., control analysis, baselines)
- Audit planning
- Internal information security management system
- 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), Health Information Technology for Economic and Clinical Health (HITECH) Act, Payment Card Industry (PCI))
- Impact of distributed information technology (IT) model (e.g., diverse geographical locations and crossing over legal jurisdictions)

6.4 Understand implications of cloud to enterprise risk management

- Assess providers risk management programs (e.g., controls, methodologies, policies, risk profile, risk appetite)
- Difference between data owner/controller vs. data custodian/processor
- Regulatory transparency requirements (e.g., breach notification, Sarbanes-Oxley (SOX), General Data Protection Regulation (GDPR))
- Risk treatment (i.e., avoid, mitigate, transfer, share, acceptance)
- Different risk frameworks
- Metrics for risk management
- Assessment of risk environment (e.g., service, vendor, infrastructure, business)

6.5 Understand outsourcing and cloud contract design

- Business requirements (e.g., service-level agreement (SLA), master service agreement (MSA), statement of work (SOW))
- Vendor management (e.g., vendor assessments, vendor lock-in risks, vendor viability, escrow)
- 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)

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/certifications/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/Register-for-Exam.

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