CCSP®

Certified Cloud Security Professional

ISC2 Certification

Certification **Exam Outline**

Effective Date: August 1, 2026

ISC2™

About CCSP

ISC2 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.

The topics included in the CCSP Exam Outline 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, full-time experience in information technology (IT). Three years must be in cybersecurity, and one year must be in one or more of the six domains of the current CCSP Exam Outline. Earning a post-secondary degree (bachelors or masters) in computer science, IT or related fields may satisfy up to one year of the required experience. Earning CSA's CCSK certificate can be substituted for one year of experience. Only one year of experience can be waived. An active CISSP credential may be substituted for the entire CCSP experience requirement. Part-time work and internships may also count towards the experience requirement.

A candidate that doesn't have the required experience to become a CCSP may become an Associate of ISC2 by successfully passing the CCSP examination. The Associate of ISC2 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 the ANSI National Accreditation Board (ANAB) ISO/IEC Standard 17024.

Job Task Analysis (JTA)

ISC2 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 CAT Examination Information

The CCSP exam uses Computerized Adaptive Testing (CAT) for all English, Simplified Chinese, German, Japanese exams. You can learn more about CCSP CAT at www.isc2.org/certifications/computerized-adaptive-testing.

Length of exam	3 hours
Number of items	100 - 150
Item format	Multiple choice and advanced item types
Passing grade	700 out of 1000 points
Exam availability	English, Chinese, German, Japanese
Testing center	Pearson VUE Testing Center

CCSP CAT Examination Weights

Domains	Average Weight
1. Cloud Concepts, Architecture and Design	17%
2. Cloud Data Security	20%
3. Cloud Platform and Infrastructure Security	17%
4. Cloud Application Security	16%
5. Cloud Security Operations	17%
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 (CSP), cloud service partner, cloud service broker, regulator)
- Essential 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)

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)
- Virtualization security (e.g., hypervisor security, container security, ephemeral computing, serverless technology, isolation)
- Common cloud threats
- Security hygiene (e.g., patching, baselining, immutable architecture, hardening)

1.4 Understand design principles of secure cloud computing

- Cloud secure data lifecycle
- Cloud-based Business Continuity (BC) and Disaster Recovery (DR) planning
- Business Impact Analysis (BIA) (e.g., Cost-Benefit Analysis (CBA), 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, secure by design)
- DevOps security

1.5 Evaluate Cloud Service Providers (CSP)

- Verification against criteria
- System/subsystem product certifications (e.g., Common Criteria (CC), Federal Information Processing Standard (FIPS) 140-2)

1.6 Comprehend Artificial Intelligence (AI)/Machine Learning (ML)

- Cloud threat detection and analysis
- Data source validation and verification
- Security Orchestration, Automation And Response (SOAR)
- Ethical concerns
- Regulatory requirements

Domain 2: Cloud Data Security

2.1 Describe cloud data concepts

- Cloud data lifecycle phases
- Data dispersion
- Data flows

2.2 Design and implement cloud data storage architectures

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

2.3 Design and apply data security technologies and strategies

- Encryption and key management
- Hashing (e.g., data integrity, non-repudiation)
- 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 and tagging

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 (e.g., authorized access, deletion prevention)

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

2.9 Comprehend data protection of Artificial Intelligence (AI) and Machine Learning (ML) data

- Data set and model privacy
- Data set and model security (e.g., validation, verification)

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 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 resilience (e.g., power, Heating, Ventilation, and Air Conditioning (HVAC), connectivity)

3.3 Analyze risks associated with cloud infrastructure and platforms

- Risk assessment (e.g., identification, analysis)
- Cloud vulnerabilities, threats and attacks
- Risk treatment 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, Application Security Verification Standard (ASVS), Top 10 Application Programming Interface (API), Top 10 for Large Language Model Applications, 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 (e.g., shared technology issues, Cloud Service Provider (CSP) insider threats, lack of visibility and control, legal and jurisdiction issues)
- 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 (CM) and versioning

4.4 Apply cloud software assurance and validation

- Functional and non-functional testing (e.g., Continuous Integration And Continuous Delivery (CI/CD) processes)
- Security testing methodologies (e.g., blackbox, whitebox, Software Composition Analysis (SCA), Interactive Application Security Testing (IAST), Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST))
- Quality Assurance (QA)
- Abuse case testing

4.5 Use verified secure software

- Securing Application Programming Interfaces (API)
- Supply-chain management (e.g., vendor assessment, integrity, authenticity, licensing)
- Third-party software management
- Validated open-source software

4.6 Comprehend and apply 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, load balancer)
- Cryptography
- Sandboxing
- Application virtualization and orchestration (e.g., microservices, containers, docker, Kubernetes)

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, key, and certificate 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))
- Secure by default
- Installation and configuration of management plane 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, Single Sign-On (SSO))
- 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, segmentation)
- Operating System (OS) hardening through the application of baselines, monitoring and remediation (e.g., Windows, Linux, VMware)
- Patch management
- 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., National Institute Of Standards And Technology (NIST), International Organization For Standardization (ISO), Health Insurance Portability and Accountability Act (HIPPA), Control Objectives For Information And Related Technology (COBIT), Center For Internet Security (CIS) Controls, Comittee Of Sponsoring Organizations (COSO), 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 (CM)
- Service-level management
- Availability management
- Capacity management

5.4 Support digital forensics

- Forensic data collection methodologies
- Evidence management
- Collecting, acquiring, and preserving 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, threat intelligence)
- Incident Response (IR)
- Vulnerability assessments
- Penetration testing

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 and regulatory frameworks and guidelines
- eDiscovery (e.g., International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27050, Cloud Security Alliance (CSA) Guidance)
- Forensics requirements (e.g., Cloud Security Alliance (CSA), International Organization For Standardization/International Electrotechnical Commission (ISO/IEC) 27037:2012/27041:2015/ 27042:2015/ 27043:2015)

6.2 Understand privacy requirements

- 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., Family Educational Rights And Privacy Act (FERPA), The Personal Information Protection And Electronic Documents Act (PIPEDA), General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPPA), Digital Personal Data Protection Act)
- 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 processes, 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 risk and control self-assessment)
- 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), 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 roles (e.g., owner, controller, custodian, processor, stewards)
- Regulatory transparency requirements (e.g., breach notification, Sarbanes-Oxley (SOX), General Data Protection Regulation (GDPR))
- Risk treatment (e.g., avoid, mitigate, transfer, share, accept)
- 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, data ownership, security requirements)
- 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 CCSP Exam Outline and identifying areas of study that may need additional attention.

View the full list of supplementary references at ISC2.org/certifications/References.

Examination Policies and Procedures

ISC2 recommends that candidates review exam policies and procedures prior to registering for the examination. Read the comprehensive breakdown of this important information at ISC2.org/Register-for-Exam.

Legal Info

For any questions related to ISC2's legal policies, please contact the ISC2 Legal Department at legal@isc2.org.

Any Questions?

Contact ISC2 Candidate Services in your region:

Americas
Tel: +1.866.331.ISC2 (4722), press 1
Email: membersupport@isc2.org

Asia-Pacific
Tel: +(852) 5803-5662
Email: isc2asia@isc2.org

Europe, Middle East and Africa
Tel: +44 203-960-7800
Email: info-emea@isc2.org