INFOSECTRAIN

CCSP

CERTIFIED CLOUD SECURITY PROFESSIONAL

CERTIFICATION TRAINING

CCSP Program Overview

The CCSP is a globally renowned certification that validates the certification holder's advanced skills and abilities to design, manage, and protect data, and applications in a cloud environment while adhering to the established practices, policies, and procedures.

CCSP certification course at InfosecTrain aims to provide an in-depth understanding of cloud computing concepts, cloud reference architecture, and cloud computing security concepts. The participants learn to safeguard the critical data assets in a cloud environment and exhibit their competency in implementing cloud security architecture.

Learn by Practice

Experience Immersive Learning with highly interactive sessions and hands-on labs

Take Regular Assessments

Bridge knowledge-gaps with our free mock exams and high intensity skill assessments

Earn CPEs

Complete your CPE target by getting CPEs and accessing our library of most trending courses

CCSP Course Highlights

48-Hour Instructor-led Training	**Online Test** Simulations
Instructors with **18+ Years Experience**	Full Coverage **6-Domains**

100% Satisfaction Guarantee
Not satisfied with your training on Day 1?
You can get a refund or enroll in a different course.

Access Recorded Sessions
Revisit your lectures, revise your concepts, and retain your knowledge From anywhere, whenever you want

Extended Post Training Support
Get extended support even after you finish your training. We're here for you until you reach your certification goals.

Who Should **Attend**

Cloud Security Analysts	Cloud Engineers	Cloud Architects
IT Security Managers	Compliance Analysts	Operations Managers

Pre-Requisites

The candidates who are enrolling for this course must have five years of working experience in information security and CCSP CBK domains. All those who fail to fulfill the eligibility criteria can take the exam to become an associate of (ISC)2 and can start working towards getting the experience to get the desired certification.

Note

- CCSP® is a registered mark of The International Information Systems Security Certification Consortium ((ISC)2).
- We are not an authorized training partner of (ISC)2.

About the **CCSP** Exam

Exam Name	Certified Cloud Security Professional (CCSP)
Exam Duration	**180 Minutes**
Number of questions	**125**
Exam format	Multiple Choice Questions
Passing Score	**700** out of **1000**
Language	English, Chinese, German and Japanese
Testing center	Pearson VUE Testing Center

Our Expert **Instructors**

PRABH NAIR   **18+ Years Of Experience**

**CISSP-ISSAP | CGRC | CCSP | CSSLP | CCISO | CISM | CISA | CRISC | CGEIT | CIPM
CIPPE | CDPSE**

18+ years of IT industry experience, specializing in Information Security. Expertise spans Vulnerability Assessment & Penetration Testing, Application Security, IT Governance, Risk & Compliance, and Security Solutions. Led global Information Security operations for a US-based IT Service Provider with a presence in the US, Canada, India, and Sri Lanka. Delivered services to 250+ organizations across 25+ countries through diverse assignments.

KRISH   **18+ Years Of Experience**

**Cloud Audit | CCSP | CCSK | CCAK | AWS CS-S | AWS CAN–S | AWS CSA-P | AWS CDE-P
MCT | CCAK | Azure Adv. Architect & Security | GCP PCA | GCP PCSE | CEH | RHCE**

18+ years of experience in deploying, migrating, auditing, and securing public cloud platforms such as AWS, GCP, and Azure. Recognized as a Microsoft Certified Trainer, with over 1000 professionals trained globally, including Fortune 500 employees. Extensive expertise as an Enterprise Cloud Security Architect, GRC Specialist, and Cloud Migration Strategist, serving 60+ enterprises worldwide. Active contributor as a Technical Writer and Subject Matter Expert for global publications and organizations.

KK SINGH   18+ Years Of Experience

C|CISO | CISSP | CCSP | CISM | CRISC | CISA | CCSK | CCAK | CDPSE | CEH | RHCSA GRCA | GRCP | CPP | PSP | PCI | AZ-900 | GDPR

With 18+ years of experience, KK is a seasoned Cyber Security Professional with a stellar record in developing and executing cybersecurity strategies for global organizations. He is an expert dedicated to safeguarding sensitive data and ensuring the integrity and availability of critical systems. He has extensive experience in the evolving cybersecurity landscape, excelling in areas such as risk management, incident response, security architecture, and both network and cloud security. His expertise also covers identity and access management, digital transformation security, DevSecOps, and compliance with standards like GDPR and ISO 27001. Equipped with advanced knowledge in blockchain, AI/ML security, and frameworks like Archer GRC, he is committed to staying ahead of emerging threats and delivering comprehensive protection for today's complex digital environment. Holding certifications such as C|CISO, CISSP, CCSP, CISM, CRISC, CISA, CCSK, CCAK, CDPSE, CEH, RHCSA, GRCA, GRCP, CPP, PSP, and PCI, KK is a recognized Cloud & Cybersecurity Strategist and a prominent CyberSec Leader, Speaker, and Mentor. He is committed to staying ahead of emerging threats and ensuring robust protection in today's complex digital world.

SUJAY   15+ Years Of Experience

CSOA | CCSP | CISSP | ISO 27001 Lead Auditor | ITIL v3

Nearly 15+ years of experience as a seasoned, technically inclined and highly empowered IT professional with strong emphasis on understanding business vision, requirements, effective communication and team building to deliver robust IT solutions and services. Sujay delivers power-packed training sessions on certification courses like CISSP, CCSP, AWS Architect, Cloud Architecture, Information Security Awareness. His sessions are highly interactive, maintaining a very high success rate throughout his courses.

Happy Learners Across the World

Vetrivel Boovaragasamy

United Arab Emirates

The trainer provided very interactive and really good sessions. Enjoyed the course a lot.

Rahul M Durugkar

Germany

The trainer's skills are excellent in cloud platforms. He guided and supported us with all queries and answers in time. Thanks, Infosec Train, will meet again in the next training session.

Lubin Abdul Khader

United Arab Emirates

Excellent training with highly professional communication from the support team (prompt delivery of all recordings). Would highly recommend InfosecTrain. Thanks a ton.

Anish Ayyappan

India

I found the training to be highly valuable and wanted to express my gratitude for the comprehensive and well-structured program. The concepts were explained in an easy to understand language. The trainer made all efforts to make sure we had our concentration on his sessions and kept us engaged.

CCSP Domains

- **Domain 1:** Cloud Concepts, Architecture and Design **(17%)**

- **Domain 2:** Cloud Data Security **(20%)**

- **Domain 3:** Cloud Platform and Infrastructure Security **(17%)**

- **Domain 4:** Cloud Application Security **(17%)**

- **Domain 5:** Cloud Security Operations **(16%)**

- **Domain 6:** Legal, Risk and Compliance **(13%)**

Domain 1
Cloud Concepts, Architecture and Design (17%)

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 (20%)

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(17%)

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 (17%)

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))

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 (16%)

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 (13%)

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., NorthAmerican 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)

INFOSECTRAIN

www.infosectrain.com I sales@infosectrain.com