Certified Cloud Security Professional [CCSP] 5 Days

The CCSP exam tests your skills in six domains. The domains draw from a range of cloud security topics within the (ISC)² Common Body of Knowledge (CBK).

Here’s a closer look at the CCSP domains and how they’re weighted on the exam:

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

Architectural Concepts & Design Requirements – Cloud computing concepts & definitions based on the ISO/IEC 17788 standard; security concepts and principles relevant to secure cloud computing.

- Understand Cloud Computing Concepts
- Describe Cloud Reference Architecture
- Understand Security Concepts Relevant to Cloud Computing
- Understand Design Principles of Secure Cloud Computing
- Identify Trusted Cloud Services

Cloud Data Security – Concepts, principles, structures, and standards used to design, implement,monitor, and secure, operating systems, equipment, networks, applications, and those controls used to enforce various levels of confidentiality, integrity, and availability in cloud environments.

- Understand Cloud Data Lifecycle
- Design and Implement Cloud Data Storage Architectures
- Design and Apply Data Security Strategies
- Understand and Implement Data Discovery and Classification Technologies
- Design and Implement Relevant Jurisdictional Data Protections for Personally Identifiable Information (PII)
- Design and Implement Data Rights Management
- Plan and Implement Data Retention, Deletion, and Archiving Policies
- Design and Implement Auditability, Traceability and Accountability of Data Events

Cloud Platform & Infrastructure Security – Knowledge of the cloud infrastructure components,both the physical and virtual, existing threats, and mitigating and developing plans to deal with those threats.

- Comprehend Cloud Infrastructure Components
- Analyze Risks Associated to Cloud Infrastructure
- Design and Plan Security Controls
- Plan Disaster Recovery and Business Continuity Management

Cloud Application Security – Processes involved with cloud software assurance and validation; andthe use of verified secure software.

- Recognize the need for Training and Awareness in Application Security
- Understand Cloud Software Assurance and Validation
- Use Verified Secure Software
- Comprehend the Software Development Life-Cycle (SDLC) Process
- Apply the Secure Software Development Life-Cycle
- Comprehend the Specifics of Cloud Application Architecture
- Design Appropriate Identity and Access Management (IAM) Solutions

Operations – Identifying critical information and the execution of selected measures that eliminate or reduce adversary exploitation of it; requirements of cloud architecture to running and managing that infrastructure; definition of controls over hardware, media, and the operators with access privileges as well as the auditing and monitoring are the mechanisms, tools and facilities.

- Support the Planning Process for the Data Center Design
- Implement and Build Physical Infrastructure for Cloud Environment
- Run Physical Infrastructure for Cloud Environment
- Manage Physical Infrastructure for Cloud Environment
- Build Logical Infrastructure for Cloud Environment
- Run Logical Infrastructure for Cloud Environment
- Manage Logical Infrastructure for Cloud Environment
- Ensure Compliance with Regulations and Controls (e.g., ITIL, ISO/IEC 20000-1)
- Conduct Risk Assessment to Logical and Physical Infrastructure
- Understand the Collection, Acquisition and Preservation of Digital Evidence
- Manage Communication with Relevant Parties

Legal & Compliance – Addresses ethical behavior and compliance with regulatory frameworks. Includes investigative measures and techniques, gathering evidence (e.g., Legal Controls, eDiscovery, and Forensics); privacy issues and audit process and methodologies; implications of cloud environments in relation to enterprise risk management.

- Understand Legal Requirements and Unique Risks within the Cloud Environment
- Understand Privacy Issues, Including Jurisdictional Variation
- Understand Audit Process, Methodologies, and Required Adaption's for a Cloud Environment
- Understand Implications of Cloud to Enterprise Risk Management
- Understand Outsourcing and Cloud Contract Design
- Execute Vendor Management