CCSP-Certified Cloud Security Professional - Certification Preparation

Duration: 5 Days   Course Code: GK2364

Overview:

The CCSP - Certified Cloud Security Professional - certificate gives you international recognition as a security professional from ISC2. This course prepares you for the CCSP exam of ISC2.As powerful as cloud computing is for the organization, understanding its information security risks and mitigation strategies is critical. Legacy approaches are inadequate, and organizations need competent, experienced professionals equipped with the right cloud security knowledge and skills to be successful. They need CCSPs.

Backed by the two leading non-profits focused on cloud and information security, the Cloud Security Alliance (CSA) and (ISC)², the CCSP credential denotes professionals with deep-seated knowledge and competency derived from hands-on experience with cyber, information, software and cloud computing infrastructure security. CCSPs help you achieve the highest standard for cloud security expertise and enable your organization to benefit from the power of cloud computing while keeping sensitive data secure.

Target Audience:

The CCSP credential is designed for experienced information security professionals with at least five years of full-time IT experience, including three years of information security and at least one year of cloud security experience. The CCSP credential is suitable for mid-level to advanced professionals involved with IT architecture, web and cloud security engineering, information security, governance, risk and compliance, and even IT auditing.

CCSP is most appropriate for those whose day-to-day responsibilities involve procuring, securing and managing cloud environments or purchased cloud services. In other words, CCSPs are heavily involved with the cloud. Many CCSPs will be responsible for cloud security architecture, design, operations, and/or service orchestration.

Example job functions include, but are not limited to: Enterprise ArchitectSecurity AdministratorSystems EngineerSecurity ArchitectSecurity ConsultantSecurity EngineerSecurity ManagerSystems Architect

Objectives:

- CCSP is a global credential born from the expertise of the two industry-leading stewards of information systems and cloud computing security, (ISC)² and CSA. The CCSP credential is appropriate and applicable to cloud security in a global environment. This is especially important given the legal, regulatory and compliance concerns that come with multi-jurisdictional housing of personally identifiable information (PII).

- For those who qualify, the CCSP exam will test their competence in the six CCSP domains of the (ISC)² Common Body of Knowledge (CBK), which cover:

- Architectural Concepts & Design Requirements

- Cloud Data Security

- Cloud Platform & Infrastructure Security

- Cloud Application Security

- Operations

- Legal & Compliance

Prerequisites:

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.

You can learn more about CCSP experience requirements and

Testing and Certification

This exam is not included in the course price and can be ordered separately.

- Exam: 3 hours
- Number of items: 125
- Item format: Multiple choice
- Passing grade: 700 out of 1000 points
- Exam availability English
- Testing center: Pearson VUE Testing Center

how to account for part-time work and internships at
https://www.isc2.org/Certifications/CCSP/experience-requirements

- CISSP - CISSP-Certified Information Systems Security Professional - Certification Preparation

Content:

Domain 1: Architectural Concepts and Design Requirements

- 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

Domain 2: Cloud Data Security

- Understand Cloud Data Lifecycle (CSA Guidance)
- 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

Domain 3: Cloud Platform and Infrastructure Security

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

Domain 4: Cloud Application Security

- 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

Domain 5: Operations

- 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 Assesment to Logical and Physical Infrastructure
- Understand the Collection, Acquisition and Preservation of Digital Evidence
- Manage Communication with Relevant Parties

Domain 6: Legal and Compliance

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

Further Information:

For More information, or to book your course, please call us on 0800/84.009

info@globalknowledge.be

www.globalknowledge.com/en-be/