Certified Cloud Security Professional

Duration: 5 Days **Course Code: CCSP**

About this course

The CCSP shows you have the advanced technical skills and knowledge to design, manage and secure data, applications and infrastructure in the cloud using best practices, policies and procedures established by the cybersecurity experts at (ISC)².

Audience profile

The CCSP is ideal for IT and information security leaders responsible for applying best practices to cloud security architecture, design, operations and service orchestration, including those in the following positions:

- Enterprise Architect
- Security Administrator
- Systems Engineer
- Security Architect
- Security Consultant
- Security Engineer
- Security Manager
- Systems Architect

Course Outline

Module 1: Architectural Concepts and Design Requirements The goal of the Architectural Concepts and Design Requirements domain is to provide you with knowledge of the building blocks necessary to develop cloud-based systems. You will be introduced to cloud computing concepts regarding topics such as the customer, provider, partner, measured services, scalability, virtualization, storage, and networking. You will also be able to understand the cloud reference architecture based on activities defined by industry-standard documents. Lastly, you will gain knowledge in relevant security and design principles for cloud computing, including secure data lifecycle and cost-benefit analysis of cloud-based systems. Platform and the data handling aspects of the platform • 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	**Module 2: Cloud Data Security Lifecycle Domain** The goal of the Cloud Data Security domain is to provide you with knowledge of the types of controls necessary to administer various levels of confidentiality, integrity, and availability, regarding securing data in the cloud. You will gain knowledge on topics of data discovery and classification techniques; digital rights management; privacy of data; data retention, deletion, and archiving; data event logging, chain of custody and non-repudiation; and the strategic use of security information and event management. • 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
Module 3: Cloud Platform and Infrastructure Security The goal of the Cloud Platform and Infrastructure Security domain is to provide you with knowledge regarding both the physical and virtual components of the cloud infrastructure. You will gain knowledge	**Module 4: Cloud Application Security** The goal of the Cloud Application Security domain is to provide you with knowledge as it relates to cloud application security. Through an exploration of the software development lifecycle, you will gain an

regarding risk-management analysis, including tools and techniques necessary for maintaining a secure cloud infrastructure. In addition to risk analysis, you will gain an understanding of how to prepare and maintain business continuity and disaster recovery plans, including techniques and concepts for identifying critical systems and lost data recovery. Stepping stones to the cloud • Comprehend cloud infrastructure components • Analyze risks associated to cloud infrastructure • Design and plan security controls • Plan disaster recovery and business continuity management	understanding in utilizing secure software and understand the controls necessary for developing secure cloud environments and program interfaces. You will gain knowledge in identity and access management solutions for the cloud and the cloud application architecture. You'll also learn how to ensure data and application integrity, confidentiality, and availability through cloud software assurance and validation. • 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
Module 5: Operations The goal of the Operations domain is to explain the requirements needed to develop, plan, implement, run, and manage the physical and logical cloud infrastructure. You will gain an understanding of the necessary controls and resources, best practices in monitoring and auditing, and the importance of risk assessment in both the physical and logical cloud infrastructures. With an understanding of specific industry compliance and regulations, you will know how to protect resources, restrict access, and apply appropriate controls in the cloud environment. • 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	**Module 6: Legal and Compliance** The goal of the Legal and Compliance domain is to provide you with an understanding of how to approach the various legal and regulatory challenges unique to cloud environments. To achieve and maintain compliance it is important to understand the audit processes utilized within a cloud environment, including auditing controls, assurance issues, and the specific reporting attributes. You will gain an understanding of ethical behavior and required compliance within regulatory frameworks, which includes investigative techniques for crime analysis and evidence-gathering methods. Enterprise risk considerations and the impact of outsourcing for design and hosting are also explored. • Understand legal requirements and unique risks within the cloud environment • Understand privacy issues, including jurisdictional variation • Understand audit process, methodologies, and required adaptions for a cloud environment • Understand implications of cloud to enterprise risk management • Understand outsourcing and cloud contract design • Execute vendor management

Contacts us:

For more Information please contact us on;
KENYA - training.kenya@clclearningafrica.com +254 713027191
TANZANIA- training.tanzania@clclearningafrica.com +255 784444490
UGANDA - training.uganda@clclearningafrica.com +256 782011784
RWANDA - training.rwanda@clclearningafrica.com +250 780953100
UAE - training.emea@clclearningafrica.com +971 552959655