

## **PROGRAMMA CompTIA Cloud + (CV0-003)**

**40 ore**

### **Parts I: Cloud Architecture and Design**

- **Compare and contrast the different types of cloud models**
  - Deployment models
  - Service models
  - Advanced cloud services
  - Shared responsibility model
- **Explain the factors that contribute to capacity planning**
  - Requirements
  - Standard templates
  - Licensing
  - User density
  - System load
  - Trend analysis
  - Performance capacity planning
- **Explain the importance of high availability and scaling in cloud environments**
  - Hypervisors
  - Oversubscription
  - Regions and zones
  - Applications
  - Containers
  - Clusters
  - High availability of network functions
  - Avoid single points of failure

- Scalability
- **Given a scenario, analyze the solution design in support of the business requirements**
  - Requirement analysis
  - Environments
  - Testing techniques

## Parts II: Security

- **Given a scenario, configure identity and access management**
  - Identification and authorization
  - Directory services
  - Federation
  - Certificate management
  - Multifactor authentication (MFA)
  - Single sign-on (SSO)
- **Given a scenario, secure a network in a cloud environment**
  - Network segmentation
  - Protocols
  - Network services
  - Log and event monitoring
  - Network flows
  - Hardening and configuration changes
- **Given a scenario, apply the appropriate OS and application security controls**
  - Policies
  - User permissions
  - Antivirus/anti-malware/endpoint detection and response (EDR)
  - Host-based IDS (HIDS)/Host-based IPS (HIPS)
  - Hardened baselines
  - File integrity
  - Log and event monitoring
  - Configuration management
  - Builds

- Operating system (OS) upgrades
- Encryption
- Mandatory access control
- Software firewall
- **Given a scenario, apply data security and compliance controls in cloud environments**
  - Encryption
  - Integrity
  - Classification
  - Segmentation
  - Access control
  - Impact of laws and regulations
  - Records management
  - Data loss prevention (DLP)
  - Cloud access security broker (CASB)
- **Given a scenario, implement measures to meet security requirements**
  - Tools
  - Vulnerability assessment
  - Security patches
  - Risk register
  - Prioritization of patch application
  - Deactivate default accounts
  - Impacts of security tools on systems and services
  - Effects of cloud service models on security implementation