KORNERSTONE
a TRAINOCATE company

Training. Makes a differece.

Certified Cloud Security Professional, CCSP®

D1 - Architectural Concepts & Design Requirements

Domain 1 – Architectural Concepts & Design Requirements

Overview & Requirements

The Architectural Concepts & Design Requirements domain focuses on the building blocks of cloud based systems. The candidate will need to have an understanding of Cloud Computing concepts such as definitions based on the ISO/IEC 17788 standard, roles like the Cloud Service Customer, Provider, and Partner, characteristics such as multi-tenancy, measured services, and rapid elasticity and scalability, as well as building block technologies of the cloud such as virtualization, storage, and networking. The Cloud Reference Architecture will need to be described and understood by the candidate, with a focus on areas such as Cloud Computing Activities as described in ISO/IEC 17789, Clause 9, Cloud Service Capabilities, Categories, Deployment Models, and the Cross-Cutting Aspects of Cloud Platform architecture and design such as interoperability, portability, governance, service levels, and performance. In addition, candidates will need to demonstrate a clear understanding of the relevant security and design principles for Cloud Computing, such as cryptography, access control, virtualization security, functional security requirements like vendor lock-in and interoperability, what a secure data lifecycle is for cloud based data, and how to carry out a cost benefit analysis of cloud based systems. The ability to identify what a trusted cloud service is, and what role certification against criteria plays in that identification using standards such as the Common Criteria and FIPS 140-2 are also areas of focus for this domain.

Domain Objectives

After completing this domain, you will be able to:

- Define the various roles, characteristics, and technologies as they relate to cloud computing concepts
- Describe cloud computing concepts as they relate to cloud computing activities, capabilities, categories, models, and cross-cutting aspects
- Identify the design principles necessary for secure cloud computing
- Define the various design principles for the different types of cloud categories
- Describe the design principles for secure cloud computing
- Identify criteria specific to national, international, and industry for certifying trusted cloud services
- Identify criteria specific to the system and subsystem product certification

Key Areas of Knowledge

A. *Understand Cloud Computing Concepts*

- A.1 Cloud Computing Definitions (ISO/IEC 17788)
- A.2 Cloud Computing Roles (i.e., Cloud Service Customer, Cloud Service Provider, and Cloud Service Partner)
- A.3 Key Cloud Computing Characteristics (e.g., on-demand self-service, broad network access, multi-tenancy, rapid elasticity and scalability, resource pooling, measured service)
- A.4 Building Block Technologies (e.g., virtualization, storage, networking, databases)

B. *Describe Cloud Reference Architecture*

- B.1 Cloud Computing Activities (ISO/IEC 17789, Clause 9)
- B.2 Cloud Service Capabilities (i.e., application capability type, platform capability type, infrastructure capability types)
- B.3 Cloud Service Categories (e.g., SaaS, IaaS, PaaS, NaaS, CompaaS, DSaaS)
- B.4 Cloud Deployment Models (e.g., public, private, hybrid, community)
- B.5 Cloud Cross-Cutting Aspects (e.g., interoperability, portability, reversibility, availability, security, privacy, resiliency, performance, governance, maintenance and versioning, service levels and service level agreement, auditability, and regulatory)

C. *Understand Security Concepts Relevant to Cloud Computing*

- C.1 Cryptography (e.g. encryption, in motion, at rest, key management)
- C.2 Access Control
- C.3 Data and Media Sanitization (e.g., overwriting, cryptographic erase)

Key Areas of Knowledge

C.4 Network security

C.5 Virtualization Security (e.g., hypervisor security)

C.6 Common Threats

C.7 Security Considerations for different Cloud Categories (e.g., SaaS, PaaS, *aaS)

D. Understand Design Principles of Secure Cloud Computing

D.1 Cloud Secure Data Lifecycle

D.2 Cloud Based Business Continuity/Disaster Recovery Planning

D.3 Cost Benefit Analysis

D.4 Functional Security Requirements (e.g., portability, interoperability, vendor lock-in)

E. Identify Trusted Cloud Services

E.1 Certification Against Criteria

E.2 System/Subsystem Product Certifications (e.g., common criteria, FIPS 140-2)

Drivers for Cloud Adoption

1. Cost Management (Opex vs Capex), pay per use
2. Risk Reduction (for testing before commitment)
3. Scalability
4. Elasticity (rent model; consumption-based pricing)
5. Virtualization
6. Business agility – mobility
7. Collaboration & Innovation platform

*** SIMPLICITY, EXPANDABILITY, ELASTICITY ***

Security Issues In Cloud Services

- Risk (business, reputation)
- Distributed Multi-tenant Security Environment
- Privacy issues
  - data leak, spill, co-mingle
  - data stored on provider's premise
  - Data sovereignty
- Compliance (Legal, regulatory, territorial)

To consider for managing risks

- Strategic alignment
  - Effective board oversight
  - Integration of risk into strategy setting & business planning
- Cultural alignment
  - Strong corporate values and a focus on compliance
- Operational focus
  - Strong control environment

Cloud Computing Functions

- Cloud administrator
- Cloud application architect
- Cloud architect (for private cloud to meet policies)
- Cloud data architect
- Cloud developer
- Cloud operator
- Cloud service manager
- Cloud storage administrator

IAAS

- Key components and characteristics
  - Scale
  - Converged IT & network capacity pool
  - Self-service, on-demand
  - High reliability and resilience (ref: datacenter)
- Benefits
  - Metered usage
  - Scale up and down as need
  - Reduced cost of ownership
  - “Green IT”

PAAS

- Key components and characteristics
- Key benefits

SAAS

- Key components and characteristics
- Key benefits

Cloud services security principles

- Define protections that enable trust in the cloud
- Develop cross-platform capabilities and patterns for proprietary and open-source providers
- Facilitate trusted and efficient access, administration, and resiliency to the customer/consumer
- Provide direction to secure information that is protected by regulations
- The architecture must facilitate proper and efficient identification, authentication, authorization, administration, and auditability
- Centralize security policy, maintenance operation, and oversight functions
- Access to information must be secure yet still easy to obtain
- Delegate or federate access control where appropriate
- Must be easy to adopt and consume, supporting the design of security patterns
- The architecture must be elastic, flexible, and resilient, supporting multi-tenant, multi-landlord platforms
- The architecture must address and support multiple levels of protection, including network, operating system, and application security needs

Cloud Technology Roadmap (per NIST)

- Interoperability
- Portability
- **Availability**
- **Security**
- **Privacy**
- **Resilience**
- Performance
- Governance & Regulatory
- SLA
- Auditability

Cloud Architecture Security Components

- Network Infrastructure & Perimeter Security
- Crytography
  - Data security, data-in-motion, SSL, privacy etc
- Access control
  - Authentication, directory services, IDM, user provisioning
- Data & Media Sanitization
  - Vendor lock-in
  - Cryptographic erasure
- Virtualization security (ref SDN)

Cloud security – common threats

- Data breach
- Data loss
- Account, session or sevice hijacking
- Insecure API
- Denial of Service (DDOS) / outage
- Malicious (or careless, unqualified) insiders
- Abuse of cloud services
- Insufficient due diligence
- Shared technology vulnerabilities
  - (data spillage / co-mingle, multi-tenancy)

IAAS Security

PAAS Security

SAAS Security

- Application & Development Security

Cloud Data Life cycle

KORNERSTONE
a TRAINOCATE company

Business Continuity & Disaster Recovery

Cloud BCP/DRM critical success factors – SLA requirements

1. Clearly state and ensure the SLA addresses which components of business continuity/disaster recovery are covered and to what degree they are covered.
   a. Penalties/compensation for loss of service
   b. Recovery Time Objectives (RTO)/Recovery Point Objectives (RPO)
   c. Loss of integrity or confidentiality (are these both covered)
   d. Points of contact and escalation processes
   e. Where failover to ensure continuity is utilized, does this maintain compliance and ensure the same or greater level of security controls?
   f. When changes are made that could impact the availability of services, that these are communicated in a timely manner
   g. Data ownership, data custodians, and data processing responsibilities are clearly defined within the SL
   h. Where third parties and key supply chain are required to ensure that availability of services is maintained, that the equivalent or greater levels of security are met, as per the SLA agreed between customer and provider

2. **Understanding your responsibilities vs. the cloud provider's responsibilities.**
   a. Customer responsibilities
   b. Cloud provider responsibilities
   c. Understand any interdependencies/third parties (supply chain risks)
   d. Order of restoration (priority) – who/what gets priority?
   e. Appropriate frameworks/certifications held by the facility, services, and processes
   f. Right to audit/regular assessments of continuity capabilities
   g. Communications of any issues/limited services
   h. Is there a need for backups to be held on-site/off-site/with another cloud provider?

Important SLA Components

Finally, regarding Disaster Recovery, a similar approach should be taken by the cloud customer to ensure the following are fully understood and acted upon, prior to signing relevant SLAs and contracts:

- **Single Points of Failure should not exist**
- **Migration to alternate provider(s) should be possible within the agreed upon RTO**
- **Whether all components will be supported by alternate cloud providers in the event of a failover** or on-site/on-premise services would be required
- **Automated controls should be enabled to allow customers to verify data integrity**
- **Where data backups are included, incremental backups should allow the user to select the desired settings**, including desired coverage, frequency, and ease of use for recovery point restoration options
- **Continuous monitoring of relevant control points**

Cost-Benefit Analysis & TCO

Cloud Security Certification & Standards

- ISO-27001
  - ISO-27011 (telco), 27017 (cloud), 27040 (storage), 22301 (BCP)
- SOC I*, II, III (SSAE, formerly SAS70)
- NIST SP 800-53
- PCI-DSS**
- CSA STAR, CCM
- CCSK, CCSP
- CC (EAL, ISO-15408, FIPS 140-2)

*Financial Report
**Card Payments