KORNERSTONE
a TRAINOCATE company

Training. Makes a differece.

Certified Cloud Security Professional, CCSP®

D5 - Operations

Domain 5 - Operations

Operations - Domain Objectives

- Describe the specifications necessary for the physical, logical, and environmental design of the data center
- Identify the requirements to build and implement the physical cloud infrastructure
- Define the process for running the physical infrastructure based on access, security, and availability configurations
- Define the process for managing the physical infrastructure with regard to access, monitoring, security controls, analysis, and maintenance
- Identify the requirements to build and implement the logical cloud infrastructure
- Define the process for running the logical infrastructure based on access, security, and availability configurations
- Define the process for managing the logical infrastructure with regard to access, monitoring, security controls, analysis, and maintenance
- Identify the necessary regulations and controls to ensure compliance for the operation and management of the cloud infrastructure
- Describe the process of conducting a risk assessment of the physical and logical infrastructure
- Describe the process for the collection, acquisition, and preservation

Operations - Domain Agenda

MODULE	NAME
1	Support the Planning Process for the Data Center Design
2	Implement and Build Physical Infrastructure for Cloud Environment
3	Run Physical Infrastructure for Cloud Environment
4	Manage Physical Infrastructure for Cloud Environment
5	Build Logical Infrastructure for Cloud Environment
6	Run Logical Infrastructure for Cloud Environment
7	Manage Logical Infrastructure for Cloud Environment
8	Ensure Compliance with Regulations and Controls
9	Conduct Risk Assessment to Logical and Physical Infrastructure
10	Understand the Collection, Acquisition and Preservation of Digital Evidence
11	Manage Communications with Relevant Parties

Planning Process for Data Center Design

- Modern Data Centers and Cloud Service Offerings
- Factors that Impact Data Center Design
  - Location
  - type of intended service (_aaS)
- Additional considerations
  - automating service enablement
  - consolidation of monitoring capabilities
  - reducing mean time to repair (MTTR)
  - mean time between failure (MTBF)

Planning Process for Data Center Design

- Logical Design
  - multi-tenancy
  - cloud management plane
  - virtualization technology
  - communications access
  - secure communication
  - secure storage
  - backup and disaster recovery
- Other considerations
- Logical design levels
- Service models (_aaS)

Physical Design Considerations

- Protect against environmental threats of the location
  - Flood, earthquake, storm
- Access to resources or supplies during disaster to ensure continued operation
  - Water, power, food, telecoms, accessibility, other amenities
- Physical access control
  - Fence, wall, gate, electronic surveillance
  - Ingress and egress access control points, identity and access authorization
  - Audit trail, logs, monitoring
- Buy or Build
- Datacenter Design Standards
  - Tier I, II, III, IV (Uptime Institute)
  - Fault Tolerant; Redundancy; Concurrently Maintainable

Environmental Design

Data Center Classification

Tiered Model Summary

	Tier I	Tier II	Tier III	Tier IV
Active Capacity Components to Support the IT Load	N	N+1	N+1	N After any Failure
Distribution Paths	1	1	1 Active and 1 Alternate	2 Simultaneously Active
Concurrently Maintainable	No	No	Yes	Yes
Fault Tolerance	No	No	No	Yes
Compartmentalization	No	No	No	Yes
Continuous Cooling	No	No	No	Yes

Physical Infrastructure for Cloud Environment

- Secure Configuration of Hardware-specific Requirements
- Installation & configuration of virtualization management tools for the host

Run Physical Infrastructure for Cloud Environment

- Configure network access for cloud hosting
- Securing network configurations
- O/S hardening via application baseline
- Availability of hosts – standalone, clustered

Manage Physical Infrastructure for Cloud Environment

- Cloud infra – who uses, why, how it works, benefits.
- Configure access control for remote access
  - Service models (_aaS), deployment models (public, private, hybrid, comm)
  - RDP (remote desktop protocol)

- O/S baseline compliance – monitoring & remediation
- Patch management
- Performance monitoring
- Hardware monitoring
- Back-up and restore of host config
- Implementation of network security controls
- Log Capture
- Management Plan

Logical Infra for Cloud Environment

BUILD

- Logical & physical design
- Secure configuration of hardware-specific requirements

RUN

- Secure network configuration
- Availability of Guest O/S

Logical Infra for Cloud Environment

MANAGE

Ensure Compliance with Regulation & Controls

- Compliance Considerations
- ITSM
- Config management
- Change management
- Incident management
- Problem management
- Release & Deployment management
- Service Level management
- Availability management
- Capacity management
- Continuity management
- Continual Service Improvement mgmt.
- Information Security management

KORNERSTONE
Training. Makes a difference.

Conduct Risk Assessment to Physical and Logical Infrastructure

- Risk assessment
- Loss expectancy
- Risk monitoring

Collection and preservation of Digital Evidence

- Cloud Forensic Challenges
  - Control over data
  - Multi-tenancy
  - Data volatility
  - Evidence acquisition

- Proper methodologies for Forensic collection of (cloud) data
- Evidence management

Managing communications with relevant parties

The "5 W's and the H" of communication are:

- **Who:** Who is the target of the communication?
- **What:** What is the communication designed to achieve?
- **When:** When is the communication best delivered/most likely to reach its intended target(s)?
- **Where:** Where is the communication pathway best managed from?
- **Why:** Why is the communication being initiated in the first place?
- **How:** How is the communication being transmitted and how is it being received?

Managing communications with relevant parties

- Vendors (suppliers)
- Customers
- Partners (eg. marketing, solution offering)
- Regulators (government)
  - Compliance regimes
- Other stakeholders