1.0 Configuration and Deployment

1.1 Given a scenario, analyze system requirements to ensure successful system deployment.

- **Appropriate commands, structure, tools, and automation/orchestration as needed**
- **Platforms and applications**
- **Interaction of cloud components and services**
  - Network components
  - Application components
  - Storage components
  - Compute components
  - Security components
- **Interaction of non-cloud components and services**
- **Baselines**
- **Target hosts**
- **Existing systems**
- **Cloud architecture**
- **Cloud elements/target objects**

1.2 Given a scenario, execute a provided deployment plan.

- **Apply the Change Management Process**
  - Approvals
  - Scheduling
- **Refer to documentation and follow standard operating procedures**
- **Execute workflow**
- **Configure automation and orchestration, where appropriate, for the system being deployed**
- **Use commands and tools as needed**
- **Document results**

1.3 Given a scenario, analyze system requirements to determine if a given testing plan is appropriate.

- **Underlying environment considerations included in the testing plan**
  - Shared components
    - Storage
    - Compute
    - Network
  - Production vs. development vs. QA
  - Sizing
  - Performance
  - High availability
  - Connectivity
  - Data integrity
  - Proper function
  - Replication
  - Load balancing
  - Automation/orchestration
- **Testing techniques**
  - Vulnerability testing
  - Penetration testing
  - Load testing

1.4 Given a scenario, analyze testing results to determine if the testing was successful in relation to given system requirements.

- **Consider success factor indicators of the testing environment**
  - Sizing
  - Performance
  - Availability
  - Connectivity
  - Data integrity
  - Proper functionality
- **Document results**
- **Baseline comparisons**
- **SLA comparisons**
- **Cloud performance fluctuation variables**

1.5 Given a scenario, analyze sizing, subnetting, and basic routing for a provided deployment of the virtual network.

- **Cloud deployment models**
  - Public
  - Private
  - Hybrid
  - Community
- **Network components**
- **Applicable port and protocol considerations when extending to the cloud**
- **Determine configuration for the applicable platform as it applies to the network**
  - VPN
  - IDS/IPS
  - DMZ
  - VXLAN
  - Address space required
  - Network segmentation and micro-segmentation
- **Determine if cloud resources are consistent with the SLA and/or change management requirements**

1.6 Given a scenario, analyze CPU and memory sizing for a provided deployment.

- **Available vs. proposed resources**
  - CPU
  - RAM
- **Memory technologies**
  - Bursting and ballooning
  - Overcommitment ratio
- **CPU technologies**
  - Hyperthreading
  - VT-x
  - Overcommitment ratio
- **Effect to HA/DR**
- **Performance considerations**
- **Cost considerations**
- **Energy savings**
- **Dedicated compute environment vs. shared compute environment**

1.7 Given a scenario, analyze the appropriate storage type and protection capability for a provided deployment.

- **Requested IOPS and read/write throughput**
- **Protection capabilities**
  - High availability
    - Failover zones
  - Storage replication
    - Regional
    - Multiregional
    - Synchronous and asynchronous
  - Storage mirroring
  - Cloning
  - Redundancy level/factor
- **Storage types**
  - NAS
  - DAS
  - SAN
  - Object storage
- **Access protocols**
- **Management differences**
- **Provisioning model**
  - Thick provisioned
  - Thin provisioned
  - Encryption requirements
  - Tokenization
- **Storage technologies**
  - Deduplication technologies
  - Compression technologies
- **Storage tiers**
- **Overcommitting storage**
- **Security configurations for applicable platforms**
  - ACLs
  - Obfuscation
  - Zoning
  - User/host authentication and authorization

1.8 Given a scenario, analyze characteristics of the workload (storage, network, compute) to ensure a successful migration.

- **Migration types**
  - P2V
  - V2V
  - V2P
  - P2P
  - Storage migrations
  - Online vs. offline migrations
- **Source and destination format of the workload**
  - Virtualization format
  - Application and data portability
- **Network connections and data transfer methodologies**
- **Standard operating procedures for the workload migration**
- **Environmental constraints**
  - Bandwidth
  - Working hour restrictions
  - Downtime impact
  - Peak timeframes
  - Legal restrictions
  - Follow-the-sun constraints/time zones

1.9 Given a scenario, apply elements required to extend the infrastructure into a given cloud solution.

- **Identity management elements**
  - Identification
  - Authentication
  - Authorization
    - Approvals
    - Access policy
  - Federation
    - Single sign-on
- **Appropriate protocols given requirements**
- **Element considerations to deploy infrastructure services such as:**
  - DNS
  - DHCP
  - Certificate services
  - Local agents
  - Antivirus
  - Load balancer
  - Multifactor authentication
  - Firewall
  - IPS/IDS