Cloud Computing

Candidates for this certification have a foundational knowledge the characteristics of cloud solutions, including the advantages they offer to stakeholders and their cost structure. Candidates are able to distinguish between various cloud offerings and architectures, including virtual machines, containers, data storage options, and identify when each is appropriate to meet a business need. Candidates understand the phases in the cloud development lifecycle. Candidates understand the importance and of governance and security when developing and deploying a cloud solution. The exam is vendor-neutral, although candidates should understand, at least at a fundamental level, the terminology used by both Azure and AWS. Candidates at least 150 hours of instruction or hands-on experience developing and deploying cloud solutions.

To be successful on the test, the candidate is also expected to have the following prerequisite knowledge and skills:
- 8th grade reading skills
- An understanding of how communication occurs on a network
- Digital literacy skills, including the ability to research, create content, and solve problems using technology
- Computational thinking skills, including the ability to decompose a problem into smaller parts and solve problems through automation

Although not required, the following skills will help a candidate learn about cloud computing more easily:
- Familiarity with at least one programming or scripting language
- Familiarity with data storage technologies, including relational databases
- Familiarity with TCP/IP
- Familiarity with common network security controls

1. Cloud Concepts

1.1 Explain cloud advantages to stakeholders

- Describe cloud infrastructure
- Distinguish between IaaS, PaaS, and SaaS
- Explain how cloud facilitates building applications faster and more cost-effectively than traditional models

1.2 Explain cost to stakeholders

- Identify the use case (new development or transition of existing product or service)
- Identify the resources that will be required to construct the service or product using cloud-hosted components (including compute, data, and network costs)
- Describe support plan that will be required to meet performance, availability, scalability, and reliability (PASR) criteria
- Consider factors that determine return on investment

1.3 Explain performance to stakeholders

- Identify performance criteria
- Consider which solutions meet the performance criteria
- Assess cost and availability of technical expertise

INFORMATION TECHNOLOGY SPECIALIST

1.4 Explain reliability to stakeholders

- Identify reliability criteria, including network speeds
- Consider which solutions meet the criteria
- Understand service-level agreement (SLA) of the cloud provider
- Consider disaster-recovery and backup plans (including backup redundancy or replication factor)

1.5 Explain availability to stakeholders

- Identify the use case (new development or transition of existing product or service)
- Identify any upstream or downstream SLAs that will govern availability requirements
- Establish availability metrics
- Assess the SLA offered by the cloud-hosted solution

1.6 Explain scalability to stakeholders

- Identify the use case (new development or transition of existing product or service)
- Understand that rules can be set to adjust resources based on need

1.7 Recommend off-the-shelf (OTS) or custom solutions as needed

- Identify the use case (new development or transition of existing product or service)
- Evaluate if an existing OTS offering meets performance, availability, scalability, and reliability needs
- Evaluate the technical effort needed for a custom solution
- Evaluate whether a custom solution can exceed OTS solution on PASR criteria

2. Developing cloud architecture

2.1 Choose between public, private, and hybrid cloud implementations

- Identify the security and privacy requirements for the solution (focusing on networking options that each provides)
- Consider limits imposed by tenancy in various cloud implementations

2.2 Draw an architectural diagram (show data flows)

- Break down the proposed solution into compute, data, and networking components
- Produce logical groupings for the components
- Mark data flows between components (including the protocol)
- Identify system and component boundaries (including responsibility model)

2.3 Define requirements

- Decide whether to virtualize server, network, storage, and desktop
- Be aware of design patterns like microservices and serverless
- Consider networking infrastructure, storage devices, memory, and end-user devices required

INFORMATION TECHNOLOGY
SPECIALIST

2.4 Identify how services communicate through application programming interfaces (APIs)

- Identifying services with which the application needs to integrate
- Interact with a service using an API

2.5 Create virtual machines

- Determine the operating system for the virtual machines
- Choose the appropriate size for the virtual machines
- Decide on geographic setting for the virtual machines (latency, legal requirements)
- Configure options (e.g., time limitations, scaling, backups) for the virtual machines

2.6 Identify data storage requirements

- Distinguish between structured and unstructured data
- Determine amount of storage needed
- Consider location of storage
- Consider storage security

3. Implementing the cloud development life cycle

3.1 Create content in virtual environments

- Understand that a source-code management system needs to be set up
- Install and configure the prerequisite packages in the virtual environment
- Save changes and keep track of the codes in a source code management system (such as Github)

3.2 Perform testing

- Provide different test cases, test scenarios, and test scripts
- Run the tests and report the bugs iteratively

3.3 Structure the overall cloud-based solution

- Integrate systems and applications within the selected environment
- Integrate systems and applications with legacy systems
- Integrate systems and applications with third-party applications
- Distinguish between containers and virtual machines
- Know when to choose containers over virtual machines

3.4 Deploy application

- Decide on the strategy to deploy a new application, replacing a previous one
- Understand version control
- Identify cloud-hosted solutions to create code and data pipelines (e.g., cloud-native CI/CD offerings and workflow automation like GitHub Actions)
- Identify existing CI/CD practices

INFORMATION TECHNOLOGY SPECIALIST

4. Deploy the application

4.1 Manage operational costs
- Understand usage-based pricing
- Scale up and scale down to meet demand cost-effectively

4.2 Develop business continuity and disaster recovery policy
- Identify potential risks and disaster scenarios
- Establish on-premise vs offsite backup strategy

4.3 Provide support to users
- Identify protection and security policies for external and internal users
- Provide application and hardware support for internal users
- Provide training tools for internal and external users

4.4 Monitor cloud systems
- Log events
- Monitor hardware and software (e.g., interpret graphs and dashboards)
- Understand notifications or alerts for provisioning backup

5. Understanding cloud governance

5.1 Comply with privacy and regulatory requirements
- Identify relevant privacy requirements based on geographical and domain constraints (e.g. BIPA, HIPAA, PDP, FERPA, COPPA, GDPR, CCPA, etc.) as well as organization-specific policies
- Identify cloud-provider compliance for these privacy regulations
- Assess types of data managed within the environment
- Assess location and storage of data
- Be aware of NIST and ISO frameworks and standards

5.2 Comply with ethical guidelines
- Consider the impact of bias, lack of transparency, and lack of accountability
- Explain potential bias and transparency challenges with prebuilt services

5.3 Managing cloud security
- Understand options and concepts for identity verification and authentication, including digital identity and multifactor authentication
- Understand access policies and authorizations (e.g., options for access; vendor-provided roles vs. custom roles and permissions; and access hygiene, including least privilege access, removal of access when not needed and disabling accounts)
- Understand the importance of data security and encryption
- Understand options to protect against unauthorized access in cloud environments (including intrusion detection and prevention, firewalls)