CompTIA Cloud+ Certification Exam Objectives

EXAM NUMBER: CV0-005 V5

CompTIA Cloud+ CV0-005 V5 Certification Exam
Draft Exam Objectives Document Version 1.0

About the Exam

The CompTIA Cloud+ CV0-005 V5 certification exam will certify that the successful candidate has the knowledge and skills required to:

- Understand cloud architecture and design concepts.
- Implement and maintain a secure cloud environment.
- Successfully provision and configure cloud resources.
- Demonstrate the ability to manage operations using observability, scaling, and automation throughout the cloud environment life cycle.
- Understand fundamental use of AI within cloud environments.
- Understand governance, risk, and compliance as it relates to cloud resources and technologies.
- Troubleshoot common issues related to cloud management.

This is equivalent to 4-5 years of hands-on experience as a cloud engineer with Network+, AutoOps+, and Security+ or equivalent knowledge.

These content examples are meant to clarify the exam objectives and should not be construed as a comprehensive list of all the content of this examination.

EXAM ACCREDITATION

The CompTIA Cloud+ exam is accredited by the ANSI National Accreditation Board (ANAB) to show compliance with the International Organization for Standardization (ISO) 17024 standard and, as such, undergoes regular reviews and updates to the exam objectives.

EXAM DEVELOPMENT

CompTIA exams result from subject matter expert workshops and industry-wide survey results regarding the skills and knowledge required of an IT professional.

CompTIA AUTHORIZED MATERIALS USE POLICY

CompTIA Certifications, LLC is not affiliated with and does not authorize, endorse, or condone utilizing any content provided by unauthorized third-party training sites (aka "brain dumps"). Individuals who utilize such materials in preparation for any CompTIA examination will have their certifications revoked and be suspended from future testing in accordance with the CompTIA Candidate Agreement. In an effort to more clearly communicate CompTIA's exam policies on use of unauthorized study materials, CompTIA directs all certification candidates to the CompTIA Certification Exam Policies. Please review all CompTIA policies before beginning the study process for any CompTIA exam. Candidates will be required to abide by the CompTIA Candidate Agreement. If a candidate has a question as to whether study materials are considered unauthorized (aka "brain dumps"), they should contact CompTIA at examsecurity@comptia.org to confirm.

PLEASE NOTE

The examples provided in bulleted list format are not exhaustive. Other examples of technologies, processes, or tasks pertaining to each objective may also be included on the exam, although not listed or covered in this objectives document. CompTIA is constantly reviewing the content of our exams and updating test questions to be sure our exams are current, and the security of the questions is protected. When necessary, we will publish updated exams based on existing exam objectives. Please know that all related exam preparation materials will still be valid.

TEST DETAILS

Required exam	Cloud+ CV0-005 V5
Number of questions	TBD
Types of questions	Multiple-choice and performance-based
Length of test	TBD
Recommended experience	4-5 years of hands-on experience as a cloud engineer with Network+, AutoOps+, and Security+ or equivalent knowledge
Passing score	TBD

EXAM OBJECTIVES (DOMAINS)

The table below lists the domains measured by this examination and the extent to which they are represented.

DOMAIN		PERCENTAGE OF EXAMINATION
1.0	Architecture and Design	TBD
2.0	Life-cycle Management	TBD
3.0	Operations	TBD
4.0	Security	TBD
5.0	Governance, Risk, and Compliance (GRC)	TBD
6.0	Artificial Intelligence (AI)	TBD
Total		**100%**

1.0 Architecture and Design

1.1 Given a set of business requirements, configure elements of an organizational structure.

- Common platform components
  - Security
  - Network
  - Identity
  - Policies
  - Access control
- Multi-account/subscriptions
  - Policies
  - Cross-account access
  - Main account
- Environment types
  - Non-production
  - Production
  - Sandbox
- Organizational hierarchy
- Logging strategies
  - Centralization
  - Aggregation
  - Isolation
- Role management
- Well-architected framework
- Account life cycle

1.2 Given a set of requirements, recommend the appropriate cloud resources.

- Requirements
  - Storage
  - Performance
  - Security
  - Cost
  - Availability
  - Compliance
  - Network
  - Compute
- Resources
  - Virtual machines
  - Containers
  - Serverless
  - Storage
  - Database
  - Network
  - Identity
  - Notification
  - Queueing
  - Monitoring

1.3 Given a set of requirements, implement reliable cloud architecture.

- Multicloud
- Multiregion
- Availability zones (AZs)
- High availability (HA)
- Disaster recovery (DR)
- Load balancing
- Resiliency
- Recovery time objective (RTO)/recovery point objective (RPO)
- Routing
- Connectivity
- Scaling
- Service mesh
- Resource placement
- Service availability
- Workload types
- Content delivery network (CDN)
- Health checks
- CAP theorem:
  - Consistency
  - Availability
  - Partition tolerance

1.4 Given a scenario, analyze design characteristics for cloud services integration.

- Workloads
- Queue systems
- Architectural patterns
- Databases
  - Vector
  - Relational
  - Non-relational
  - Time series
  - Graph
- Distribution
- Identity access
- Cache systems
- Orchestration
- Storage types
  - Persistent
  - Ephemeral
  - Object
  - Block
  - File
- Networking
- Encryption
- Sensitive data management
- Configuration management
- Application programming interface (API)
- Observability
- Log data
- Managed services
- Event streaming
- Protocols
- Notification services

1.5 Explain the financial aspects of cloud usage and management.

- Shared resources
- Cost allocation
- Tagging
- Consumption models
- Budget forecasting
- Cost granularity
- Soft limits
- Hard limits
- Financial controls
- Chargeback
- Vendor agreements
  - Support plans
  - Enterprise agreement
  - Reseller agreement
  - Managed service provider (MSP)
- Licensing models
  - Bring your own license (BYOL)
  - Subscription
- Scalability

2.0 Life-cycle Management

2.1 Explain the business aspects of life-cycle management.

- Uptime
- Service-level agreement (SLA)
- Vendor contracts
- Master service agreement (MSA)
- Change management
- Supplier management
- Artifacts
- Responsibility transition
- Merger and acquisition (M&A) transition
- Migration
- Licensing
- Workforce capability
- Forecasting

2.2 Given a scenario, use the appropriate techniques to provision cloud resources.

- Infrastructure as code (IaC)
  - Modules
- Templates
- Pipelines
- Configuration management
- Command line
- Software development kit (SDK)
- Web console-based
- Resources
- Landing zone
- Service catalog/marketplace
- Images
- Scripting
- Migration strategies
  - Replatform
  - Re-architect
  - Rehost
  - Retain
  - Retire
  - Refactor
- Stress testing
- Policy as Code

2.3 Given a scenario, use the appropriate techniques for maintaining cloud resources.

- Patch management
- Updates
- Upgrades
- Rollbacks
- Rollout techniques
  - Blue/green
  - Canary
  - Rolling
  - In-place
- Maintenance windows
- Environments
  - Production
  - Quality assurance (QA)
  - Staging
  - Development
  - Sandbox
- Desired state
- Baselines
- Resource policy
- Change management
- Peer review
- QA
  - Regression testing
  - Stress testing
- Runbooks
- Playbooks
- Standard operating procedure (SOP)
- Policy as Code
- Migration strategies

2.4 Explain considerations for decommissioning cloud resources.

- Final backup
- Data retention
- Hardware aging
- Firewall rules
- Access controls
- End-of-life (EOL)
- End-of-support (EOS)
- Deprecation
- Resource dependencies
- Policies
- Regulation
- Data destruction
- Orphaned resources
- Account termination
- Risk

2.5 Explain automation concepts for life-cycle management.

- Workflows
  - Visual
  - Agentic
  - Declarative
- Event-driven
- API integration
- Webhooks
- Rule-based
- Orchestration
- Playbooks
- State management

2.6 Given a scenario, troubleshoot life-cycle management issues.

- Drift
- Deployment
- Connectivity
- Patch management
- IaC
- Source code management (SCM)
- Upgrade
- Decommissioning errors
- Deletion prevention
- Blocking dependencies
- Misconfiguration
- Accidental deletion
- Peer review
- Resource availability
- Upstream dependencies
- Access controls
- Expired certificates
- Secrets rotation
- Corruption
- Lockout
- Account ownership
- Compatibility
- Regressions
- Performance degradation
- Pipeline failures
- Capability deficiency
- Technical debt
- Vendor lock-in
- Hard limits

3.0 Operations

3.1 Given a scenario, use appropriate tools to interact with cloud resources.

- Command-line interface (CLI)
- SDK
- API
  - Endpoint
  - Client software
- Web console
- Model Context Protocol (MCP)
- Bastion host
- Cloud management platform (CMP) tool
- AI playground
- Integrated development environment (IDE)
- Formats
  - YAML Ain't Markup Language (YAML)
  - JavaScript Object Notation (JSON)

3.2 Given a scenario, analyze observability artifacts and monitoring resources.

- Resource usage
- Logs
- API
- Traces
- Service-level indicator (SLI)/service-level objective (SLO)
- Baselines
- Metrics
  - Infrastructure
  - Application
  - Service
  - Cost
  - Energy usage
  - Availability
- Dashboards
- Alerts
  - Webhooks
  - Notifications
  - Thresholds
  - Escalation
  - Prioritization
  - Severity
- Application performance monitoring (APM)
- Auditing
- Anomaly detection
- Workflow automation
- Health checks

3.3 Given a set of requirements, optimize cloud resources.

- Autoscaling
- Rightsizing
  - Memory
  - Disk
  - Compute
  - Graphics processing unit (GPU)
  - Network
- Storage tiers
- Serverless
  - Function as a service (FaaS)
- Cache systems
- Workflows
  - Event-driven
  - Schedule-based
- Load balancing
- Cluster management
- Containerization
  - Image size
  - Repository
  - Resource cap
- Financial operations (FinOps)
  - Budget
  - Cost
- Network
  - Ingress
  - Egress
  - IP addressing
- Policies
- Orphaned resource detection
- Edge computing

3.4 Given a set of business requirements, apply data protection and resiliency techniques.

- RTO
- RPO
- DR sites
  - Hot
  - Cold
  - Warm
- Archiving
- Versioning
- Replication
- Immutability
- Write once, read many (WORM)
- Litigation hold
- Backup and restore
- Retention management
- Compression
- Deduplication
- Data integrity

3.5 Given a scenario, troubleshoot cloud incidents.

- Service crash
- Resource availability
- Inadequate access
- Connectivity issues
- Misconfigurations
- Performance issues
  - Contention
  - Exhaustion
  - Resource limits
  - Latency
- Data corruption
- Backup failures
- Supply chain
  - Software
  - Hardware
  - Software as a service (SaaS)
- Patching issues
- Data breach
- Data leakage
- Shadow IT
- Baseline deviations

4.0 Security

4.1 Explain concepts related to securing physical devices.

- Threat detection and remediation
  - Device scanning
  - Device discovery
- Conditional access policies
- Operating system (OS) patching and updates
- Firmware updates
- Security groups
- Trusted Platform Module (TPM)
- Disk encryption
- Change tracking
- Disabling unnecessary ports
- Disabling unnecessary services
- Fault tolerance
- Hardware supply chain
- Benchmarks
  - Vendor-specific
  - Center for Internet Security (CIS)

4.2 Given a scenario, implement secure application principles.

- Firewalls
  - Web application firewall (WAF)
  - Next-generation firewall
- Software supply chain
- Software bill of materials (SBOM)
- Secrets management
- Secrets rotation
- Artifacts scanning
- Application updates
- Distributed denial of service (DDoS) protection
- Logging
- Security information and event management (SIEM) integrations
- Security orchestration, automation, and response (SOAR)
- API gateway
- MCP servers
- Session management
- Throttling
- Cloud security posture management (CSPM)
- Benchmarks
  - Vendor-specific
  - CIS

4.3 Given a scenario, implement data security principles.

- Transport Layer Security (TLS)/Mutual Transport Layer Security (mTLS)
- Data-at-rest encryption
- Data-in-transit encryption
- Data security posture management (DSPM)
- Data loss prevention (DLP)
  - Pattern recognition
- Data detection
  - Personally identifiable information (PII)
  - Sensitive personally identifiable information (SPII)
  - Payment Card Industry Data Security Standard (PCI DSS)
- Secure web gateway
- Data categorization and classification
- Cloud access security broker (CASB)
- Authorization
- Data life-cycle management
  - Data destruction
  - Data retention
  - Record management
- Obfuscation
  - Data masking
  - Tokenization
- Immutability

4.4 Given a scenario, apply identity and access management (IAM).

- Least privilege
- Conditional access policy
- Authentication methods
  - Single sign-on (SSO)
  - Identity federation
  - Security Assertions Markup Language (SAML)
  - Open Authentication (OAuth)
  - Multifactor authentication (MFA)
  - Secure Shell (SSH) keys
- Authorization methods
  - Role-based access control
  - Attribute-based access control (ABAC)
  - Access control lists (ACLs)
  - Just-in-time (JIT) access
  - Endpoint privilege management (EPM)
- Certificate management
- Identity provider (IdP)
- Privileged access management (PAM)
- Impersonation
- Service accounts

4.5 Given a scenario, troubleshoot common security issues within the cloud networking environment.

- Lateral movement
- Incorrect zoning
- Overly permissive access
- Insecure public access
- Incorrect subnet allocation
- Expired network device certificates
- DDoS attacks
- Performance-related indicators
  - Maximum transmission unit (MTU) misconfiguration
  - Resource spike
  - Incorrect Domain Name System (DNS) resolution
  - DNS flooding
  - Latency
- Insecure protocols
  - Deprecated protocols
- Insecure ciphers
- Indicators of compromise (IOCs)
- Data scraping
- Non-encrypted traffic

5.0 Governance, Risk, and Compliance (GRC)

5.1 Explain the purpose of governance practices.

- Policy
- Process definition
- Tag management
- Account management
- Data sanitization
- Change management
- Project management methodologies
- Software development life cycle (SDLC)
- Financial controls
- Data disclosure
- Data classification

5.2 Explain the aspects of risk management.

- Risk register
  - Accepted risk
  - Risk remediation
  - Classification
  - Score
  - Likelihood
  - Impact
  - Ownership
- Supply chain management
- Strategies
  - Mitigation
  - Acceptance
  - Transference
  - Deference
- Business impact analysis (BIA)
- Responsible, Accountable, Consulted, Informed (RACI) matrix
- Frameworks

5.3 Explain the function of compliance in a cloud environment.

- Audits
- Frameworks and industry standards
  - General Data Protection Regulation (GDPR)
  - PCI DSS
  - System and Organization Controls 2 (SOC 2)
  - PII
  - SPII
  - International Organization for Standardization (ISO)
  - National Institute of Standards and Technology (NIST)
  - Cloud Security Alliance (CSA)
- Data residency compliance
- Data sovereignty
- Export controls
- Security controls
- Process controls
- Reporting
- Sustainability certification
- Benchmarks
  - Vendor-specific
  - Industry-specific
  - CIS

6.0 Artificial Intelligence (AI)

6.1 Explain aspects of AI life-cycle management.

- Context engineering
- Prompt-driven development
- AI-assisted prototyping
- Retrieval-augmented generation (RAG) management
- Agentic workflows
- Model management
- AI orchestration
- Function/tool calling

6.2 Explain artificial intelligence for IT operations (AIOps) use cases.

- Pattern recognition
- Log intelligence
- Crash analysis
- Scaling predictability
- Artifact creation/updates
- Debugging summary
- Remediation
- Process orchestration
- Creating and deploying services
- Automated response
- Human-in-the-loop (HITL)
- Gathering statistics and metrics
- Reporting

6.3 Given a scenario, analyze the results of an AI security review.

- Code review
- Root cause analysis (RCA)
- Log review
  - Anomaly detection
- Common Vulnerabilities and Exposures (CVE)
- Excessive permissions
- Remediation actions/recommendations
- Recognizing hallucinations

6.4 Given a scenario, securely integrate AI components with cloud workloads.

- MCP
  - Servers
  - Proxy
  - Location
  - Isolation
- Large language model (LLM)
  - Location
  - Types
  - Routing
  - Discovery
  - Isolation
- AI agent configuration
- Prompt injection controls
- Authorization
- Identification
- Impersonation
- Guardrails
- Execution path filters
- Role-based access control
- Agent2Agent (A2A) protocol
- Deterministic rules
- Permission boundaries
- HITL intervention
- In-line DLP
- Hallucination detection
- Sandbox
- Data sanitization
- Context engineering

6.5 Explain the use of AI in GRC.

- Agentic checks
  - Data
  - Regulation
  - Compliance
  - AI subscriptions
- Governance
  - Responsible use of AI
  - Guardrails
  - HITL
  - Context engineering
- Provider routing
- Vulnerability assessment
- Patch management
- Risk assessment
- Risk remediation

CompTIA Cloud+ Acronym List

The following is a list of acronyms that appear on the CompTIA Cloud+ CV0-005 V5 certification exam. Candidates are encouraged to review the complete list and attain a working knowledge of all listed acronyms as part of a comprehensive exam preparation program.

ACRONYM	DEFINITION
A2A	Agent2Agent
ABAC	attribute-based access control
ACL	access control list
AI	artificial intelligence
API	application programming interface
APM	application performance monitoring
AZ	availability zone
BIA	business impact analysis
BYOL	bring your own license
CAP	consistency, availability, and partition tolerance
CASB	cloud access security broker
CDN	content delivery network
CIS	Center for Internet Security
CLI	command-line interface
CMP	cloud management platform
CSA	Cloud Security Alliance
CSPM	cloud security posture management
CVE	Common Vulnerabilities and Exposures
DDoS	distributed denial of service
DLP	data loss prevention
DNS	Domain Name System
DR	disaster recovery
DSPM	data security posture management
EOL	end-of-life
EOS	end-of-support
EPM	endpoint privilege management
FaaS	function as a service
GDPR	General Data Protection Regulation
GPU	graphics processing unit
GRC	governance, risk, and compliance
HA	high availability
HITL	human-in-the-loop
IaC	infrastructure as code
IDE	integrated development environment
IdP	identity provider
IOC	indicator of compromise

ACRONYM	DEFINITION
ISO	International Organization for Standardization
JIT	just-in-time
JSON	JavaScript Object Notation
LLM	large language model
M&A	merger and acquisition
MCP	Model Context Protocol
MFA	multifactor authentication
MSA	master service agreement
MSP	managed service provider
mTLS	Mutual Transport Layer Security
MTU	maximum transmission unit
NIST	National Institute of Standards and Technology
OS	operating system
PAM	privileged access management
PCI DSS	Payment Card Industry Data Security Standard
PII	personally identifiable information
QA	quality assurance
RACI	Responsible, Accountable, Consulted, Informed
RAG	retrieval-augmented generation
RCA	root cause analysis
RPO	recovery point objective
RTO	recovery time objective
SaaS	software as a service
SAML	Security Assertions Markup Language
SBOM	software bill of materials
SCM	source code management
SDK	software development kit
SDLC	software development life cycle
SIEM	security information and event management
SLA	service-level agreement
SLI	service-level indicator
SLO	service-level objective
SOAR	security orchestration, automation, and response
SOC 2	System and Organization Controls 2
SOP	standard operating procedure
SPII	sensitive personally identifiable information
SSH	Secure Shell
SSO	single sign-on
TLS	Transport Layer Security
TPM	Trusted Platform Module
WAF	web application firewall
WORM	write once, read many
YAML	YAML Ain’t Markup Language

CompTIA Cloud+ Hardware and Software List

CompTIA has included this sample list of hardware and software to assist candidates as they prepare for the Cloud+ CV0-005 V5 certification exam. This list may also be helpful for training companies that wish to create a lab component for their training offering. The bulleted lists below each topic are sample lists and are not exhaustive.

SOFTWARE

- Automation tools
- Client (and server) OS
- Various web browsers
- Container orchestration platform
- IDE
- CLI

OTHER

- Internet access
- Access to SaaS, platform as a service (PaaS), or infrastructure as a service (IaaS) environments
- Remote access to cloud service providers
- Observability tools
- Access to an AI platform