CCSP Certification Test Bank

Welcome to the Bare Metal Cyber Audio Academy, an audio-first learning library built to help you pass certification exams through clear, practical instruction you can use anywhere. Each course is designed for busy learners who want structured coverage of the exam objectives, high-yield recall practice, and scenario-ready decision skills without needing slides, labs, or extra downloads. The handouts that come with each course are meant to reinforce what you hear, giving you quick reference material like question banks, key definitions, and review prompts you can use before a study session or right before exam day. The goal is simple: help you recognize what the exam is asking, select the best answer confidently, and avoid common traps. You can find the full catalog of courses, books, and resources at https://baremetalcyber.com/, where everything is organized to support steady progress from first listen to test-day readiness.

Find more for free at BareMetalCyber.com

Contents

Bank 1

1. A company is migrating a customer-facing web app to the cloud. The scenario states the team will use a managed application platform where the provider manages the operating system and runtime, while the customer manages the application code and data. What is the most important first step before selecting security controls?
   A. Confirm the cloud service model and the shared responsibility boundary
   B. Require a CASB for all users before go-live
   C. Tokenize all sensitive fields to remove compliance scope
   D. Set RTO and RPO targets before choosing any identity controls

2. During an incident investigation, an auditor asks how the team can prove who accessed a sensitive dataset and when. Which concept best describes the requirement to reconstruct events using reliable records?
   A. Anonymization
   B. Auditability
   C. Availability
   D. Data residency

3. A question describes a cloud workload where data must remain stored within a specific country's borders due to contractual and regulatory requirements. Which term best matches this constraint?
   A. Data classification
   B. Data lifecycle
   C. Data residency
   D. Data remanence

4. A cloud security engineer proposes "encrypt everything" as the complete solution for a highly sensitive dataset. Which follow-up question aligns best with CCSP decision logic?
   A. "What is the service's maximum item count on exam day?"
   B. "Do we have a current asset inventory for every workload?"
   C. "Which cloud deployment model is being used?"
   D. "Who owns the encryption keys, who can decrypt, and where is access recorded?"

5. A recovery plan states the business can tolerate losing up to fifteen minutes of transactional data after a disruptive event. Which metric is being described?
   A. RTO
   B. RPO

C. BC/DR
D. Integrity

6. A breach scenario requires evidence that can stand up in court, including who collected logs, where they were stored, and who accessed them. Which term best fits this evidence-handling requirement?
   A. Chain of custody
   B. Continuous monitoring
   C. Configuration baseline
   D. Corrective control

7. A team is choosing between two answers on a scenario question. One option describes a control but does not mention how it is proven; the other describes a control plus logs, configuration history, and approvals that demonstrate it works. Which option is the better exam-style choice?
   A. The control-only option, because it is simpler
   B. The control-plus-evidence option, because verifiable proof is prioritized
   C. Either option, because both are security controls
   D. The option that adds more tools, because cloud is complex

8. A vendor evaluation is underway before signing a contract for a third-party cloud service. The team is reviewing assurance reports and contract clauses like breach notification and right to audit before committing. What is this activity called?
   A. Due care
   B. Risk acceptance
   C. Due diligence
   D. Continuous monitoring

9. An organization deletes a sensitive dataset, but later learns that residual copies may still exist in snapshots or underlying storage blocks. Which concept best describes this risk?
   A. Data tokenization
   B. Multi-tenancy
   C. Data remanence
   D. Anonymization

10. A policy must allow access decisions that consider user role, device posture, location, and data sensitivity together, rather than role alone. Which access control approach best fits?
    A. ABAC (Attribute-Based Access Control)

B. Least privilege
C. Federation
D. Authentication

---

1. Correct Answer: A. Confirm the cloud service model and the shared responsibility boundary
   Explanation: CCSP-style decisions start by identifying IaaS, PaaS, or SaaS because control ownership and visibility depend on the service model. Without that boundary, control choices often become the wrong-first-step.
2. Correct Answer: B. Auditability
   Explanation: Auditability is the ability to reconstruct events and control performance using reliable records such as logs, configuration history, and approvals. CCSP scenarios commonly reward answers that are provable with traceable evidence.
3. Correct Answer: C. Data residency
   Explanation: Data residency is the requirement that data be stored and sometimes processed within a specific geographic or legal jurisdiction. CCSP questions often treat residency as a hard constraint that shapes control and architecture choices.
4. Correct Answer: D. “Who owns the encryption keys, who can decrypt, and where is access recorded?”
   Explanation: The CCSP framing treats encryption as incomplete without key ownership, decryption access, rotation, and logging that proves key use. The best answers clarify who can decrypt and how access is recorded for accountability and auditability.
5. Correct Answer: B. RPO
   Explanation: RPO is the maximum acceptable amount of data loss measured in time, such as losing up to fifteen minutes of transactions. It is commonly confused with RTO, which measures acceptable downtime.
6. Correct Answer: A. Chain of custody
   Explanation: Chain of custody is the documented history of evidence handling, including who collected it, where it was stored, who accessed it, and when. CCSP incident scenarios emphasize defensible, tamper-evident evidence handling.
7. Correct Answer: B. The control-plus-evidence option, because verifiable proof is prioritized

Explanation: CCSP questions frequently prioritize controls that are verifiable with evidence like logs, configurations, tickets, and approvals. When two controls seem plausible, the option with a clearer proof trail is typically the better answer.

8. Correct Answer: C. Due diligence
   Explanation: Due diligence is the up-front investigation and evaluation of a provider or service before committing, including assurance reports and contract clauses. CCSP scenarios distinguish this from due care, which is the ongoing protection and review after the decision.

9. Correct Answer: C. Data remanence
   Explanation: Data remanence is residual data that remains after deletion, including storage blocks and snapshots that can preserve sensitive content. CCSP questions use this to test secure disposal and verification thinking beyond “delete the data.”

10. Correct Answer: A. ABAC (Attribute-Based Access Control)
    Explanation: ABAC grants or denies access based on multiple attributes such as device posture, location, time, and data sensitivity, not just role. CCSP scenarios often use ABAC when role-only access control is too coarse for the stated conditions.

Bank 2

1. A company wants to reduce exposure of cardholder-related data in a cloud analytics platform by replacing sensitive values with non-sensitive substitutes, while keeping the ability to map back to the original values in a secured system. Which technique best matches this description?
   A. Anonymization
   B. Tokenization
   C. Encryption in transit
   D. Data residency

2. A cloud environment relies on a centralized corporate identity provider so employees can use single sign-on to access multiple cloud services. Which concept best describes this trust relationship?
   A. Federation
   B. Authorization
   C. Multi-tenancy
   D. Configuration baseline

3. A security review finds that a service account can modify storage policies, create new admin roles, and disable logging, even though it only needs read access to one dataset. Which control principle is most directly violated?
   A. Availability
   B. Least privilege
   C. Auditability
   D. Data lifecycle

4. A team is evaluating a new cloud provider and asks for independent evidence about the provider's control environment to support a compliance decision. Which artifact type best fits that request?
   A. Asset inventory
   B. Assurance report
   C. Configuration baseline
   D. Continuous monitoring dashboard

5. A scenario says the organization can tolerate a maximum of two hours of downtime for a critical application after a disruptive event. Which metric does this represent?
   A. RPO
   B. Integrity

C. RTO
D. Data classification

6. A cloud design requires that logs be centrally collected and protected against tampering so investigators can trust the timeline of events. Which security property is being emphasized most?
   A. Integrity
   B. Availability
   C. Anonymization
   D. Archiving

7. A cloud workload uses multiple customers on shared underlying infrastructure with logical isolation between tenants. Which term best describes this architecture characteristic?
   A. Multi-tenancy
   B. eDiscovery
   C. Due care
   D. Corrective control

8. A security team documents an approved standard for cloud resource configurations and then checks for drift over time. What is this standard called?
   A. Configuration baseline
   B. Compliance mapping
   C. Corrective control
   D. Advanced item type

9. A scenario describes selecting controls to prevent sensitive data from being uploaded to unsanctioned cloud apps and to enforce policy across cloud services. Which control category best aligns?
   A. BC/DR
   B. CASB
   C. HSM
   D. Chain of custody

10. An exam question focuses on verifying an identity claim before any permissions are evaluated. Which concept is being tested first?
    A. Authorization
    B. Authentication
    C. Accountability
    D. Auditability

1. Correct Answer: B. Tokenization
   Explanation: Tokenization replaces sensitive data elements with non-sensitive tokens while preserving a secure mapping to original values. It shows up as a way to reduce exposure and scope, with the key decision being whether reversal is possible and who controls the mapping.

2. Correct Answer: A. Federation
   Explanation: Federation enables identities from one system to access resources in another through a defined trust relationship. It commonly appears in CCSP scenarios involving centralized identity, single sign-on, and consistent access control across cloud services.

3. Correct Answer: B. Least privilege
   Explanation: Least privilege means granting only the minimum access needed for a task and no more. CCSP scenarios often treat excessive permissions, especially for service accounts, as a root risk that leads to poor security outcomes.

4. Correct Answer: B. Assurance report
   Explanation: An assurance report is independent evidence about a provider's controls used to support risk and compliance decisions. CCSP questions often test whether you recognize what such reports cover and where customer-side controls are still needed.

5. Correct Answer: C. RTO
   Explanation: RTO is the maximum acceptable downtime before a service must be restored. It is frequently confused with RPO, which measures acceptable data loss rather than time to recover service.

6. Correct Answer: A. Integrity
   Explanation: Integrity ensures records and data have not been altered in an unauthorized or undetected way. CCSP scenarios commonly connect integrity to log trustworthiness, tamper resistance, and defensible incident timelines.

7. Correct Answer: A. Multi-tenancy
   Explanation: Multi-tenancy describes shared infrastructure serving multiple customers with logical isolation between tenants. It matters because CCSP questions use it to test isolation risks and what controls must be validated with evidence.

8. Correct Answer: A. Configuration baseline
   Explanation: A configuration baseline is an approved, documented standard configuration that can be measured against and maintained over time. It matters because cloud configuration drift is common and exam scenarios reward answers that emphasize standardized settings plus evidence of control.

9. Correct Answer: B. CASB
   Explanation: A CASB helps enforce security policies for cloud service use, including visibility and data protection controls across cloud apps. CCSP scenarios often pair CASB with data loss prevention and governance for sanctioned and unsanctioned services.

10. Correct Answer: B. Authentication
    Explanation: Authentication verifies an identity claim before access is granted. CCSP questions separate authentication from authorization, which is the later step that determines what the identity is allowed to do.

Bank 3

1. A cloud team says they have “done backups,” so disaster recovery is solved. During review, the assessor notes there is no proof that restores work or that dependencies are included. What is the best exam-style correction?
   A. Replace backups with anonymization to eliminate recovery needs
   B. Treat backup as sufficient if storage is encrypted
   C. Focus only on availability metrics, not testing
   D. Validate recovery with restore testing and evidence tied to RTO/RPO assumptions

2. A privacy requirement states data must be transformed so individuals cannot be identified, even when combined with other datasets. Which term best matches this requirement?
   A. Anonymization
   B. Tokenization
   C. Data remanence
   D. Archiving

3. An auditor asks for proof that a control is effective and traceable, including logs with reliable timestamps, configuration history, and approvals. Which concept best describes the ability to produce this proof?
   A. Availability
   B. Auditability
   C. Multi-tenancy
   D. Federation

4. A cloud provider offers a service for generating and storing cryptographic keys in a tamper-resistant way to support higher-assurance key protection. Which option best fits?
   A. CASB
   B. HSM
   C. BC/DR
   D. Compliance mapping

5. A scenario describes preventing sensitive data from leaving authorized boundaries, such as uploads to external sites or cloud storage. Which control category is being tested?
   A. DLP
   B. Chain of custody

C. Due diligence
D. Corrective control

6. A security architect must choose controls for a dataset. The best answer must cover create, store, use, share, archive, and destroy, not just storage encryption. Which concept is being emphasized?
   A. Data residency
   B. Data lifecycle
   C. Advanced item types
   D. Asset inventory

7. A compliance question asks the candidate to link specific security controls to legal and contractual requirements and identify coverage gaps without overclaiming. What activity is being described?
   A. Configuration baseline
   B. Compliance mapping
   C. Continuous monitoring
   D. Corrective control

8. A cloud security incident requires collecting logs and preserving evidence so it is defensible, including documenting who accessed the evidence and when. Which term best fits?
   A. Integrity
   B. Chain of custody
   C. Authorization
   D. Accountability

9. A team is asked to prove they can tie admin actions to a specific identity and responsible party, including service accounts and delegated administrators. Which concept best matches?
   A. Accountability
   B. Availability
   C. RPO
   D. Data tokenization

10. A company wants to move fast on a new cloud service and says it will “sort out security later.” Which concept represents the ongoing, reasonable actions expected after a decision is made to protect assets and meet obligations?
    A. Due diligence
    B. Due care

C. Data remanence
D. Authentication

---

1. Correct Answer: D. Validate recovery with restore testing and evidence tied to RTO/RPO assumptions
   Explanation: Backup is not the same as recovery readiness, and CCSP decision logic expects evidence that restores work and dependencies are accounted for. RTO and RPO targets drive what "good recovery" means, and proof should match those assumptions.
2. Correct Answer: A. Anonymization
   Explanation: Anonymization transforms data so individuals cannot be identified, even when combined with other datasets. CCSP scenarios use this to test privacy-driven decisions and re-identification risk awareness.
3. Correct Answer: B. Auditability
   Explanation: Auditability is the ability to reconstruct events and control performance using reliable records such as logs, configuration history, and approvals. CCSP questions often reward answers that emphasize verifiable proof and traceability.
4. Correct Answer: B. HSM
   Explanation: An HSM is designed to generate, store, and use cryptographic keys in a tamper-resistant way. CCSP scenarios use HSM choices to test higher-assurance key protection and provable key-handling controls.
5. Correct Answer: A. DLP
   Explanation: DLP focuses on detecting and preventing sensitive data from leaving authorized boundaries. CCSP questions commonly test whether you connect DLP to classification and policy enforcement rather than treating it as a generic tool.
6. Correct Answer: B. Data lifecycle
   Explanation: The data lifecycle covers creation through destruction, and CCSP scenarios often test whether controls apply across all stages. Answers that focus only on encryption at rest typically miss lifecycle stages like sharing, retention, and disposal.
7. Correct Answer: B. Compliance mapping
   Explanation: Compliance mapping links security controls to legal, regulatory, and contractual requirements. CCSP scenarios test whether you can demonstrate

coverage without overclaiming and recognize gaps that need additional controls or evidence.

8. Correct Answer: B. Chain of custody
   Explanation: Chain of custody is the documented handling history of evidence, including who collected it, where it was stored, and who accessed it and when. CCSP incident scenarios emphasize defensible, tamper-evident evidence handling.

9. Correct Answer: A. Accountability
   Explanation: Accountability ties actions and outcomes to a specific identity or responsible party. CCSP questions often connect accountability to audit trails, admin activity logging, and evidence that can stand up to review.

10. Correct Answer: B. Due care
    Explanation: Due care is the ongoing reasonable actions taken to protect assets and meet obligations after decisions are made. CCSP scenarios distinguish due care from due diligence, which is the pre-contract or pre-commit evaluation phase.

Bank 4

1. A scenario states the cloud provider manages the underlying infrastructure for a SaaS application, but the customer remains responsible for configuring access, managing users, and controlling how sensitive data is shared. Which concept best explains why the customer still has meaningful security duties?
   A. Shared responsibility model
   B. Data remanence
   C. Advanced item types
   D. Configuration baseline

2. An incident response review finds that logs exist, but they cannot be trusted because they may have been altered and there is no reliable way to verify they are unchanged. Which security property is the primary concern?
   A. Availability
   B. Integrity
   C. Authentication
   D. Anonymization

3. A cloud access policy must allow a contractor to access a dataset only from managed devices, from an approved region, during business hours, and only if the dataset is classified as internal. Which access control approach best matches this requirement?
   A. ABAC
   B. Federation
   C. Authentication
   D. Multi-tenancy

4. A team is selecting between two answers about cloud logging. One option says “enable logging,” while another says “centralize logs, protect integrity, and ensure they support reconstruction of user and admin actions.” Which option is the best exam-style choice and why?
   A. “Enable logging,” because it is the simplest control
   B. “Enable logging,” because advanced item types require short answers
   C. “Centralize and protect logs,” because it supports auditability and defensible evidence
   D. Either option, because logging is always equivalent in cloud scenarios

5. A provider contract review asks for an independent report about the provider’s controls, but the scenario also warns that such reports do not automatically prove

the customer's configuration is correct. What is the best concept to cite for the provider evidence?
A. Assurance report
B. Configuration baseline
C. Asset inventory
D. Data lifecycle

6. A cloud storage service is used to retain records for legal requirements. The scenario focuses on long-term preservation with controlled access and integrity protections, not quick restore for outages. Which term best fits?
A. Backup
B. Archiving
C. RPO
D. Tokenization

7. A question describes selecting security controls but warns that some answers assume an on-prem approach that does not fit the cloud service being used. What is the most likely "wrong-first-step" that leads to this mistake?
A. Skipping identification of the cloud service model and trust boundary
B. Setting RTO and RPO before selecting any controls
C. Using DLP for sensitive data
D. Using a configuration baseline to manage drift

8. A security team wants to reduce risk by ensuring keys are well protected, but they also need a clear record of who can decrypt and where those actions are logged. Which topic is being tested most directly?
A. Data tokenization
B. Cryptographic key management
C. Multi-tenancy
D. eDiscovery

9. A cloud program decision requires linking a control to a specific requirement and documenting what evidence proves compliance without overclaiming. Which activity best matches?
A. Compliance mapping
B. Corrective control
C. Advanced item types
D. Authorization

10. A team is asked to list all cloud resources in scope so they can assess risk and verify monitoring coverage. Which term best describes this foundational record?
    A. Data residency
    B. Asset inventory
    C. RTO
    D. Due care

---

1. Correct Answer: A. Shared responsibility model
   Explanation: The shared responsibility model explains how security and compliance duties are divided between the provider and the customer based on the service model. CCSP scenarios often test whether you recognize that customers still own identity, configuration, and data-use responsibilities even in SaaS.

2. Correct Answer: B. Integrity
   Explanation: Integrity is the assurance that data and records have not been altered in an unauthorized or undetected way. CCSP scenarios frequently connect integrity to trustworthy logs and defensible incident timelines.

3. Correct Answer: A. ABAC
   Explanation: ABAC makes access decisions using multiple attributes such as device posture, location, time, and data sensitivity. CCSP questions use ABAC when role-only rules are insufficient to enforce scenario constraints.

4. Correct Answer: C. “Centralize and protect logs,” because it supports auditability and defensible evidence
   Explanation: CCSP-style answers prioritize auditability, meaning the ability to reconstruct events using reliable records. Centralized, integrity-protected logs better support traceable evidence than a generic “enable logging” statement.

5. Correct Answer: A. Assurance report
   Explanation: An assurance report is independent evidence about a provider’s controls used to support compliance and risk decisions. CCSP scenarios also expect recognition that provider reports do not automatically prove customer-side configuration is correct.

6. Correct Answer: B. Archiving
   Explanation: Archiving focuses on long-term preservation of records with controlled access and integrity protections. CCSP questions often distinguish archiving from backup, which is oriented toward operational recovery.

7. Correct Answer: A. Skipping identification of the cloud service model and trust boundary
   Explanation: CCSP decision logic begins with identifying the service model and shared responsibility boundary because it determines control ownership and visibility. Skipping that step leads to on-prem assumptions and wrong control selection.

8. Correct Answer: B. Cryptographic key management
   Explanation: Cryptographic key management covers key creation, storage, access control, rotation, and destruction, along with auditability of key use. CCSP questions commonly test key ownership, decryption access, and where actions are recorded as the real decision points.

9. Correct Answer: A. Compliance mapping
   Explanation: Compliance mapping links specific controls to legal, regulatory, and contractual requirements and helps identify gaps. CCSP scenarios reward answers that pair controls with clear evidence and avoid overclaiming.

10. Correct Answer: B. Asset inventory
    Explanation: An asset inventory is an up-to-date record of cloud resources and related components needed for scope, risk assessment, and monitoring coverage. CCSP questions often treat inventory as a prerequisite for proving what is in scope and what is protected.

Bank 5

1. A security team proposes a control that prevents unauthorized reading of stored cloud data, but the scenario also requires minimizing who can decrypt and proving access in logs. Which paired focus best matches the exam's expected reasoning?
   A. Confidentiality plus auditability
   B. Availability plus archiving
   C. Integrity plus tokenization
   D. Multi-tenancy plus eDiscovery

2. A company uses a managed key service but wants to supply its own keys to retain stronger control over decryption capability. Which key management model best fits?
   A. ABAC
   B. BYOK
   C. DLP
   D. CASB

3. A scenario says, "The best answer must be provable," and references logs, approvals, and configuration history as proof. Which term captures this exam preference most directly?
   A. Authorization
   B. Accountability
   C. Auditability
   D. Advanced item types

4. A cloud provider selection includes reviewing independent evidence about the provider's controls and validating contract clauses before committing. Which term best describes this up-front evaluation work?
   A. Due care
   B. Due diligence
   C. Continuous monitoring
   D. Corrective control

5. An incident response plan requires preserving evidence so it is defensible, including documenting who handled the evidence, where it was stored, and when it was accessed. Which concept best fits?
   A. Integrity
   B. Chain of custody
   C. Data classification
   D. Compliance mapping

6. A scenario presents two answers for access design. One relies only on “role = admin,” while the other uses role plus device posture, location, time, and data sensitivity. Which approach best fits the scenario and why?
   A. Authentication, because identity verification is sufficient
   B. Federation, because single sign-on replaces fine-grained policy
   C. ABAC, because it supports attribute-based conditions beyond roles
   D. Least privilege, because it is the same as ABAC

7. A cloud team says the provider “handles security,” so customer-side monitoring is unnecessary. Which statement best reflects the exam’s expected correction?
   A. Monitoring is optional if encryption is enabled
   B. The customer still needs due care, including monitoring and evidence of control effectiveness
   C. Monitoring is only required for private cloud deployments
   D. Monitoring is replaced by assurance reports

8. A company must keep data within a specific jurisdiction, and the best answer must respect that constraint before proposing technical controls. Which term best matches the constraint?
   A. Data lifecycle
   B. Data residency
   C. Data tokenization
   D. Data remanence

9. A security reviewer finds that cloud resources are not consistently tracked, making it unclear what is in scope, what is monitored, and what evidence is available. What foundational artifact is missing?
   A. Configuration baseline
   B. Asset inventory
   C. Assurance report
   D. Archiving plan

10. A question describes a shared cloud platform serving multiple customers with logical isolation, and the risk discussion centers on isolation assurance and evidence expectations. Which term best fits?
    A. Multi-tenancy
    B. Authorization
    C. RTO
    D. Anonymization

1. Correct Answer: A. Confidentiality plus auditability
   Explanation: Confidentiality addresses preventing unauthorized access to sensitive data, while auditability ensures access and control performance can be reconstructed using reliable records. CCSP scenarios often treat “secure” as incomplete unless access and decryption actions can also be proven with evidence.

2. Correct Answer: B. BYOK
   Explanation: BYOK means the customer supplies and controls the encryption keys used by the cloud service. CCSP questions use BYOK to test key ownership, decryption control, and the evidence trail around key use and access.

3. Correct Answer: C. Auditability
   Explanation: Auditability is the ability to reconstruct events and control performance using reliable records such as logs, configuration history, and approvals. CCSP scenarios often prioritize answers that are verifiable with a clear proof trail.

4. Correct Answer: B. Due diligence
   Explanation: Due diligence is the up-front investigation and evaluation of a provider or service before committing, including reviewing assurance evidence and contract clauses. CCSP questions distinguish this from due care, which is ongoing after the decision is made.

5. Correct Answer: B. Chain of custody
   Explanation: Chain of custody documents the handling history of evidence, including who collected it, where it was stored, who accessed it, and when. CCSP incident scenarios emphasize defensible evidence handling rather than just having logs available.

6. Correct Answer: C. ABAC, because it supports attribute-based conditions beyond roles
   Explanation: ABAC grants or denies access using multiple attributes such as device posture, location, time, and data sensitivity. CCSP scenarios often present ABAC as the better fit when role-only authorization is too coarse for stated conditions.

7. Correct Answer: B. The customer still needs due care, including monitoring and evidence of control effectiveness
   Explanation: Due care is the ongoing reasonable actions taken to protect assets and meet obligations after decisions are made. CCSP scenarios frequently correct the

misconception that a provider's responsibilities eliminate the customer's need to monitor and produce evidence.

8. Correct Answer: B. Data residency
   Explanation: Data residency requires data to be stored and sometimes processed within a specific geographic or legal jurisdiction. CCSP questions treat residency as a constraint that must be honored before selecting or proposing controls.

9. Correct Answer: B. Asset inventory
   Explanation: An asset inventory is the up-to-date record of cloud resources needed to define scope, assess risk, and verify monitoring coverage. CCSP scenarios often treat inventory as a prerequisite for evidence, governance, and reliable security decisions.

10. Correct Answer: A. Multi-tenancy
    Explanation: Multi-tenancy describes shared infrastructure serving multiple customers with logical isolation between tenants. CCSP scenarios use it to test isolation risks and what evidence is needed to justify trust in that isolation.