SSCP 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 2

Bank 2 6

Bank 3 10

Bank 4 14

Bank 5 18

Bank 1

1. A user signs in successfully to a reporting portal, but the system blocks them from exporting a sensitive report because they lack the required permission. Which concept is being enforced at the export step?
   A. Authentication
   B. Authorization
   C. Accountability
   D. Availability

2. A security analyst wants a quick way to detect whether a critical file has been altered without relying on secrecy of the file contents. Which control concept best fits that goal?
   A. Cryptographic hash
   B. Decryption
   C. Cipher
   D. Encryption

3. Administrators need a tightly controlled, hardened entry point for managing systems in a sensitive internal network without opening broad administrative access from the outside. Which architectural component best matches this purpose?
   A. Demilitarized zone (DMZ)
   B. Firewall
   C. Access Control List (ACL)
   D. Bastion host

4. A security team implements centralized logging and alerting so they can identify suspicious activity quickly, even if it does not block the activity. What type of control is this best described as?
   A. Preventive control
   B. Corrective control
   C. Detective control
   D. Compensating control

5. A company is worried about sensitive data being emailed, uploaded, or copied to removable media without approval, and wants controls that can detect and help prevent those leaks. Which control category best fits?
   A. Data retention
   B. Encryption

C. Baseline
D. Data Loss Prevention (DLP)

6. A hurricane disrupts a region and leadership asks, “How do we keep critical operations running at an acceptable level during the disruption?” Which plan best addresses that need?
   A. Disaster recovery plan (DRP)
   B. Business continuity plan (BCP)
   C. Change management plan
   D. Configuration management plan

7. A policy needs to allow access only when a user’s device meets posture requirements, the request is from an approved location, and the time of day is within a defined window. Which access model best matches this requirement?
   A. Attribute-Based Access Control (ABAC)
   B. Access Control List (ACL)
   C. Data classification
   D. Audit trail

8. During an investigation, an analyst links authentication logs with network alerts to determine whether separate events form a single coordinated attack pattern. What is this activity called?
   A. Continuous monitoring
   B. Anomaly detection
   C. Event correlation
   D. Evidence handling

9. A critical application must remain available even if a primary component fails, and the environment is designed to switch to a redundant component when failure occurs. Which term best describes this capability?
   A. Exposure
   B. Defense in depth
   C. Corrective control
   D. Failover

10. Before approving a vendor relationship, an organization performs investigation and validation activities to support a defensible decision. Which governance concept best matches this work?
    A. Due care
    B. Due diligence

C. Accountability
D. Data owner

---

1. Correct Answer: B. Authorization
   Explanation: Authorization is the permission decision that happens after identity is verified. SSCP-style scenarios often hinge on separating “who you are” from “what you can do.”

2. Correct Answer: A. Cryptographic hash
   Explanation: A cryptographic hash supports integrity checking by producing a digest that changes when the underlying data changes. It is not encryption because it is not reversible, which is why it is used for tamper detection rather than secrecy.

3. Correct Answer: D. Bastion host
   Explanation: A bastion host is a hardened system used as a controlled administrative entry point at a boundary. The exam-relevant idea is reducing attack surface while supporting strong authentication and logging for access.

4. Correct Answer: C. Detective control
   Explanation: Detective controls identify that an event has occurred, such as through logging and alerting. They do not primarily prevent the event, but they enable faster response once suspicious activity is observed.

5. Correct Answer: D. Data Loss Prevention (DLP)
   Explanation: DLP controls detect and help prevent sensitive data from leaving approved boundaries through channels like email, web upload, or removable media. On the exam, DLP complements access control and encryption rather than replacing them.

6. Correct Answer: B. Business continuity plan (BCP)
   Explanation: A BCP focuses on how critical operations continue during and after a disruptive event. It is distinct from a DRP, which focuses more narrowly on restoring technology systems and data.

7. Correct Answer: A. Attribute-Based Access Control (ABAC)
   Explanation: ABAC makes access decisions based on attributes like device posture, location, time, and sensitivity context. SSCP questions use this to test dynamic, fine-grained policy needs beyond simple roles or static lists.

8. Correct Answer: C. Event correlation
   Explanation: Event correlation links related events across sources to identify patterns a single alert might not reveal. The exam angle is recognizing correlation as an analysis step that strengthens detection and investigation decisions.

9. Correct Answer: D. Failover
   Explanation: Failover is switching to a redundant system or component when the primary fails. SSCP ties this to availability goals and the ability to maintain service during component outages.

10. Correct Answer: B. Due diligence
    Explanation: Due diligence is the investigation and validation performed before taking action or approving a decision. SSCP scenarios use it to test defensible governance choices supported by review notes or assessment evidence.

Bank 2

1. A team wants to reduce exposure if an internet-facing server is compromised by isolating it from the internal network while still allowing public access to the service. Which design choice best supports this goal?
   A. Place the server in a demilitarized zone (DMZ).
   B. Disable firewall rules to simplify access.
   C. Store sensitive internal databases on the same host as the public service.
   D. Remove segmentation and rely only on endpoint antivirus.

2. A security reviewer needs to prove which administrator made a specific configuration change and when it occurred. Which concept most directly supports this requirement?
   A. Confidentiality
   B. Accountability
   C. Encryption
   D. Availability

3. A system experiences unusual login attempts at odd hours that deviate from the typical pattern. The monitoring team wants to flag this deviation for investigation. What is the best term for this deviation?
   A. Baseline
   B. Anomaly
   C. Cipher
   D. Failover

4. A company's access policy must adjust dynamically based on user role, device posture, location, time, and data sensitivity. Which control approach best matches this requirement?
   A. Access Control List (ACL)
   B. Role-Based Access Control (RBAC)
   C. Attribute-Based Access Control (ABAC)
   D. Data retention

5. A security analyst is asked to reconstruct a sequence of events during an incident using reliable records that show actions and changes in chronological order. Which artifact type is most directly being used?
   A. Audit trail
   B. Data classification label

C. Business Impact Analysis (BIA)
D. Compensating control

6. An organization cannot implement its preferred safeguard due to a technical constraint, but still needs to reduce risk to a comparable level using an alternative safeguard that can be supported with evidence. What is this alternative safeguard called?
A. Corrective control
B. Compensating control
C. Preventive control
D. Configuration management

7. After a disruptive event, leadership needs technology systems restored within defined targets, focusing on recovering infrastructure and data. Which plan best addresses this?
A. Business continuity plan (BCP)
B. Data retention plan
C. Disaster recovery plan (DRP)
D. Change management plan

8. A security team uses alerts and logs to identify suspicious behavior, but these measures do not directly block the behavior. Which control type is this?
A. Detective control
B. Corrective control
C. Preventive control
D. Due care

9. A threat actor uses stolen username and password pairs from another breach to attempt logins across many services. What is this attack called?
A. Brute force attack
B. Credential stuffing
C. Exploit
D. Anomaly

10. A system must maintain availability by switching to a redundant component when the primary fails. Which capability does this describe?
A. Defense in depth
B. Baseline
C. Failover
D. Exposure

1. Correct Answer: A. Place the server in a demilitarized zone (DMZ).
   Explanation: A DMZ is a network segment designed to host public-facing services while isolating internal networks from direct exposure. SSCP scenarios use DMZ placement to test segmentation and blast-radius reduction decisions.

2. Correct Answer: B. Accountability
   Explanation: Accountability means actions can be traced back to a specific identity through mechanisms like authentication and logging. On the exam, it appears when questions ask what supports “who did what and when.”

3. Correct Answer: B. Anomaly
   Explanation: An anomaly is activity that deviates from a known baseline, such as unusual login times or unexpected behavior spikes. SSCP questions use anomalies to test monitoring and analysis decisions about what to investigate.

4. Correct Answer: C. Attribute-Based Access Control (ABAC)
   Explanation: ABAC makes access decisions using attributes like device posture, location, time, and sensitivity context. The exam tests ABAC as the best fit for dynamic and fine-grained policies compared with static lists or roles alone.

5. Correct Answer: A. Audit trail
   Explanation: An audit trail is a chronological record of events that supports reconstruction of actions and changes. SSCP items emphasize audit trails for investigations, compliance evidence, and integrity checks.

6. Correct Answer: B. Compensating control
   Explanation: A compensating control is an alternative safeguard used when a preferred control cannot be implemented, while still meeting the intent of the requirement. SSCP scenarios test whether the substitute actually reduces risk to an equivalent level and can be supported with evidence like logs or approvals.

7. Correct Answer: C. Disaster recovery plan (DRP)
   Explanation: A DRP focuses on restoring systems and data after a major disruption, centered on technology recovery. SSCP contrasts this with business continuity, which focuses on keeping critical operations running.

8. Correct Answer: A. Detective control
   Explanation: Detective controls identify that an event has occurred, such as logging and alerting. They are distinct from preventive controls, which aim to stop the event, and corrective controls, which reduce impact after detection.

9. Correct Answer: B. Credential stuffing
   Explanation: Credential stuffing uses stolen username and password pairs to attempt logins on other systems. SSCP highlights defenses such as multifactor authentication, rate limiting, and monitoring for abnormal login patterns.

10. Correct Answer: C. Failover
    Explanation: Failover is the switching to a redundant system or component when the primary fails. SSCP connects failover to availability requirements and resilience planning.

Bank 3

1. A new dataset is created that includes sensitive business information, and someone must be accountable for deciding its classification level and approving who can access it. Which role best fits that responsibility?
   A. Data owner
   B. Firewall administrator
   C. Endpoint security engineer
   D. Incident responder

2. Before selecting a new vendor, the organization performs investigation and validation activities to support a defensible decision. Which concept best describes this work?
   A. Due care
   B. Due diligence
   C. Accountability
   D. Data retention

3. A reviewer suspects unauthorized configuration drift and wants to determine whether current system settings deviate from an approved “known-good” reference point. What should they compare against first?
   A. Audit trail
   B. Event correlation results
   C. Baseline
   D. Compensating control

4. A team receives a software package and wants a reliable way to detect whether it was altered in transit, without relying on secrecy of the contents. Which concept best fits?
   A. Encryption
   B. Decryption
   C. Cipher
   D. Cryptographic hash

5. During an incident review, leadership asks for reliable information that supports conclusions about what happened and what controls were in place, such as logs, tickets, and approvals. What is this information called?
   A. Evidence
   B. Exposure

C. Availability
D. Data classification

6. An analyst is instructed to collect and analyze digital information in a disciplined way that preserves integrity and traceability so it can support an investigation. Which term best matches that activity?
A. Data retention
B. Forensics
C. Continuous monitoring
D. Change management

7. A critical service must stay available even if the primary component fails, and the design requires switching to a redundant component when that failure occurs. Which capability does this describe?
A. Exposure
B. Defense in depth
C. Failover
D. Bastion host

8. A security architect proposes multiple independent safeguards so that if one control fails, the environment still resists compromise and limits impact. Which principle is being applied?
A. Due care
B. Data retention
C. Change management
D. Defense in depth

9. A security team continuously collects and reviews logs and alerts so suspicious behavior can be detected and investigated quickly over time. What is this practice called?
A. Continuous monitoring
B. Corrective control
C. Decryption
D. Baseline

10. A login portal shows many automated guesses attempting different passwords until one works. What is the best term for this attack pattern?
A. Credential stuffing
B. Brute force attack

C. Exploit
D. Event correlation

---

1. Correct Answer: A. Data owner
Explanation: A data owner is accountable for a data set's classification, permitted use, and access approvals. This shows up as a responsibility-boundary decision where ownership sets rules and others implement or verify them.

2. Correct Answer: B. Due diligence
Explanation: Due diligence is the investigation and validation performed before approving a decision, such as selecting a vendor. It is different from due care, which is the ongoing reasonable protection steps taken after decisions are made.

3. Correct Answer: C. Baseline
Explanation: A baseline is a known-good reference point for configuration or behavior. Comparing current settings to the baseline is the fastest way to confirm whether drift occurred and whether it aligns with approved change records.

4. Correct Answer: D. Cryptographic hash
Explanation: A cryptographic hash produces a digest used to detect tampering because the digest changes when the data changes. It supports integrity checking and is not encryption because it is not reversible.

5. Correct Answer: A. Evidence
Explanation: Evidence is reliable information used to support conclusions, such as logs, screenshots, tickets, approvals, and configuration records. SSCP-style decisions often ask what proves a claim or what records an analyst should rely on before acting.

6. Correct Answer: B. Forensics
Explanation: Forensics is the disciplined collection and analysis of digital evidence while preserving integrity and traceability. It matters when the goal is reconstruction and proof rather than quick troubleshooting alone.

7. Correct Answer: C. Failover
Explanation: Failover is switching to a redundant system or component when the primary fails. It is directly tied to availability because it supports continued access to services during component outages.

8. Correct Answer: D. Defense in depth
   Explanation: Defense in depth uses multiple layers of safeguards so one control failure does not lead to full compromise. The exam-style decision point is recognizing that layered controls reduce attack success and limit blast radius.

9. Correct Answer: A. Continuous monitoring
   Explanation: Continuous monitoring is the ongoing collection and review of security-relevant signals like logs and alerts. It supports faster detection and investigation by establishing visibility over time rather than relying on one-time checks.

10. Correct Answer: B. Brute force attack
    Explanation: A brute force attack attempts many password combinations until one works, often using automation. It differs from credential stuffing, which specifically reuses stolen username and password pairs from other breaches.

Bank 4

1. A team needs to reduce the chance that sensitive data is disclosed to unauthorized parties when stored on a device. Which security objective is most directly being protected?
   A. Availability
   B. Confidentiality
   C. Accountability
   D. Failover

2. A security control is intended to reduce impact after a problem has been detected, such as restoring service or fixing the issue that caused the weakness. What type of control is this?
   A. Corrective control
   B. Detective control
   C. Compensating control
   D. Access Control List (ACL)

3. A security engineer wants to enforce a set of rules that permits or denies traffic based on criteria such as IP address, port, and protocol. Which mechanism best matches this?
   A. Data classification
   B. Attribute-Based Access Control (ABAC)
   C. Access Control List (ACL)
   D. Audit trail

4. An investigator wants to link authentication logs with network alerts so that separate signals can be evaluated together to identify an attack pattern. What is this activity called?
   A. Evidence preservation
   B. Event correlation
   C. Decryption
   D. Data retention

5. A company wants to minimize how reachable and susceptible a system is by reducing attack surface through segmentation, hardening, and access control. Which term best describes the risk factor being reduced?
   A. Exposure
   B. Cipher

C. Availability
D. Due diligence

6. A security control provides boundary enforcement by applying traffic rules between networks or zones. Which control is being described?
A. Baseline
B. Bastion host
C. Firewall
D. Business Impact Analysis (BIA)

7. A team identifies a deviation from normal behavior and needs to decide what to investigate first and what records to capture. Which concept most directly describes the deviation?
A. Baseline
B. Anomaly
C. Encryption
D. Data owner

8. A company allows personally owned devices to access corporate resources, increasing the need for posture checks and data separation. Which model is being used?
A. Disaster recovery plan (DRP)
B. Business continuity plan (BCP)
C. Bring Your Own Device (BYOD)
D. Continuous monitoring

9. A control transforms plaintext into ciphertext so only authorized parties with the correct key can read it. Which concept is being described?
A. Cryptographic hash
B. Encryption
C. Audit trail
D. Due care

10. A hardened entry point is used to provide controlled administrative access into a sensitive network while limiting exposure and improving logging and authentication controls. Which component best matches this description?
A. Bastion host
B. Data Loss Prevention (DLP)
C. Data retention
D. Credential stuffing

1. Correct Answer: B. Confidentiality
   Explanation: Confidentiality means information is only accessible to authorized people, systems, and processes. SSCP-style items frame it as preventing disclosure and typically point to access control and encryption choices.

2. Correct Answer: A. Corrective control
   Explanation: Corrective controls reduce impact after an issue occurs, such as restoring from backup or applying a fix. The exam commonly tests the difference between corrective actions and detective controls that only identify events.

3. Correct Answer: C. Access Control List (ACL)
   Explanation: An ACL is a rule set that permits or denies traffic or access based on criteria like IP, port, and protocol. SSCP questions often test what an ACL can enforce and where it is applied.

4. Correct Answer: B. Event correlation
   Explanation: Event correlation links related events across multiple sources to identify patterns that single alerts may not reveal. It is used to strengthen monitoring and investigation decisions by combining signals.

5. Correct Answer: A. Exposure
   Explanation: Exposure is the degree to which an asset is reachable or susceptible given its configuration and access paths. SSCP scenarios connect reducing exposure with reducing attack surface using segmentation, hardening, and access control.

6. Correct Answer: C. Firewall
   Explanation: A firewall enforces traffic rules between networks or zones and supports segmentation. SSCP questions test firewall placement and purpose, recognizing it complements but does not replace other controls.

7. Correct Answer: B. Anomaly
   Explanation: An anomaly is behavior that deviates from a known baseline, such as unusual login patterns or unexpected changes. SSCP uses anomalies to test what to investigate and what evidence to capture.

8. Correct Answer: C. Bring Your Own Device (BYOD)
   Explanation: BYOD allows personally owned devices to access corporate resources and introduces added risk controls like posture checks and data separation. SSCP

questions use BYOD to test endpoint and access decisions when devices are not fully owned.

9. Correct Answer: B. Encryption
Explanation: Encryption transforms readable data into ciphertext so only parties with the correct key can read it. The exam tests selecting encryption for confidentiality and recognizing that key handling determines real protection.

10. Correct Answer: A. Bastion host
Explanation: A bastion host is a hardened system used as a controlled administrative entry point at a boundary. SSCP scenarios use it to test reduced attack surface alongside strong authentication and audit logging.

Bank 5

1. A security team needs to prove that a specific user performed an action on a system by tying events to identity and reliable logs. Which concept is most directly being achieved?
   A. Accountability
   B. Availability
   C. Encryption
   D. Data retention

2. A company needs to keep certain records for a defined period to meet business and legal requirements, then dispose of them properly to reduce risk. Which concept best matches this practice?
   A. Data classification
   B. Data retention
   C. Business Impact Analysis (BIA)
   D. Event correlation

3. A team wants to keep critical operations running at an acceptable level during a major disruption, even before all technology systems are fully restored. Which plan best fits?
   A. Business continuity plan (BCP)
   B. Disaster recovery plan (DRP)
   C. Change management plan
   D. Configuration management plan

4. A security analyst is asked to determine which business processes and systems are most critical and to quantify the impact of outages to set recovery priorities. What is this analysis called?
   A. Baseline
   B. Business Impact Analysis (BIA)
   C. Due care
   D. Encryption

5. A team is deciding what to monitor over time and how to use logs and alerts to support faster detection and investigation. Which practice is being described?
   A. Forensics
   B. Continuous monitoring
   C. Corrective control
   D. Decryption

6. A control is selected specifically because it identifies that suspicious activity has occurred, but it does not directly prevent the activity. Which control type is this?
   A. Detective control
   B. Corrective control
   C. Compensating control
   D. Preventive control

7. An organization wants to verify whether a file has been altered and also ensure that a record of events can support reconstruction and integrity checking during an investigation. Which paired concept combination best fits?
   A. Data owner and due diligence
   B. Baseline and BYOD
   C. Cryptographic hash and audit trail
   D. Failover and firewall

8. A team uses an alternative safeguard because the preferred safeguard cannot be implemented, but they still need to meet the intent of the requirement and support it with logs and approvals. What is this called?
   A. Corrective control
   B. Compensating control
   C. Detective control
   D. Defense in depth

9. A security team wants to prevent sensitive data from leaving approved boundaries through email, web upload, or removable media, including detection and prevention actions. Which control category best fits?
   A. Data retention
   B. Data Loss Prevention (DLP)
   C. Baseline
   D. Decryption

10. A team needs a hardened system at a boundary that provides controlled administrative access into a sensitive network without broadly exposing internal systems. Which component is this?
    A. Firewall
    B. Demilitarized zone (DMZ)
    C. Bastion host
    D. Access Control List (ACL)

1. Correct Answer: A. Accountability
   Explanation: Accountability means actions can be traced back to a specific person, device, or process through identity and logging. SSCP questions use it when scenarios ask what proves “who did what and when.”

2. Correct Answer: B. Data retention
   Explanation: Data retention is keeping information for a defined period to meet business, legal, and risk requirements, then disposing of it properly. SSCP uses it as a governance decision point where over-retention increases exposure.

3. Correct Answer: A. Business continuity plan (BCP)
   Explanation: A BCP focuses on continuing critical operations during and after disruption. SSCP distinguishes it from disaster recovery, which focuses on restoring technology systems and data.

4. Correct Answer: B. Business Impact Analysis (BIA)
   Explanation: A BIA identifies critical processes and quantifies outage impacts to set priorities and recovery targets. SSCP scenarios use it to test “what comes first” recovery decisions.

5. Correct Answer: B. Continuous monitoring
   Explanation: Continuous monitoring is ongoing collection and review of security signals like logs and alerts. It supports faster detection and investigation by establishing visibility over time.

6. Correct Answer: A. Detective control
   Explanation: Detective controls identify that an event has occurred, such as through logging and alerting. They differ from preventive controls that aim to stop an event and corrective controls that reduce impact afterward.

7. Correct Answer: C. Cryptographic hash and audit trail
   Explanation: A cryptographic hash supports integrity checking by revealing tampering when the digest changes. An audit trail provides a chronological record of events to reconstruct actions and support investigations.

8. Correct Answer: B. Compensating control
   Explanation: A compensating control is an alternative safeguard used when a preferred control cannot be implemented while still meeting the intent of the requirement. SSCP scenarios test whether it reduces risk to a comparable level and can be supported with evidence.

9. Correct Answer: B. Data Loss Prevention (DLP)
   Explanation: DLP detects and helps prevent sensitive data from leaving approved boundaries through common channels. SSCP treats it as complementary to access control and encryption, not a replacement.

10. Correct Answer: C. Bastion host
    Explanation: A bastion host is a hardened entry point used to provide controlled administrative access at a boundary. SSCP questions often connect it to reduced attack surface, strong authentication, and audit logging.