SSCP Exam Glossary

Find more at BareMetalCyber.com

1. **Accountability**
   Accountability means actions can be traced back to a specific person, device, or process through identity and logging. On the exam, it often appears as "what control helps prove who did what," and the best answer usually involves strong authentication plus reliable audit logging.

2. **Access Control List (ACL)**
   An ACL is a rule set that permits or denies traffic or access based on criteria like IP, port, protocol, user, or object. Exam questions commonly test where an ACL is applied and what it can and cannot do compared with roles, attributes, or segmentation.

3. **Advanced item types**
   Advanced item types are non-traditional question formats used alongside multiple choice to test applied judgment, not just recall. On the exam, the trap is treating them like trivia; the scoring usually rewards selecting the safest control choice given the scenario constraints.

4. **Anomaly**
   An anomaly is activity that deviates from a known baseline, such as unusual login times, spikes in errors, or unexpected configuration changes. SSCP questions use anomalies to test monitoring and analysis decisions: what to investigate first, what to escalate, and what evidence to capture.

5. **Asset management lifecycle**
   The asset management lifecycle is how hardware, software, and data are planned, acquired, inventoried, maintained, retained, and ultimately disposed of. On the exam, this shows up as scope and control coverage: if an asset is not inventoried or tracked to end-of-life, security controls and patching usually fail in predictable ways.

6. **Attribute-Based Access Control (ABAC)**
   ABAC is an access model that makes decisions based on attributes such as user role, device posture, location, time, and data sensitivity. SSCP items often test when ABAC is the best fit versus role-based access control, especially for dynamic environments and fine-grained policy.

7. **Authentication**
   Authentication is proving an identity claim, such as verifying a user is who they say they are. On the exam, the decision point is selecting the right method—single factor vs multifactor—and recognizing that authentication alone does not define what a user is allowed to do.

8. **Authorization**
   Authorization is granting permissions after identity is verified, defining what actions or resources are allowed. Exam scenarios frequently hinge on separating authentication from authorization so you pick the control that limits access appropriately, not just the control that logs someone in.

9. **Availability**
   Availability means systems and data remain accessible to authorized users when needed, including during failures or attacks. SSCP questions often frame availability as a tradeoff with security controls, testing whether redundancy, recovery objectives, and incident handling support the business requirement.

10. **Audit trail**
    An audit trail is a chronological record of events that supports reconstruction of actions, decisions, and changes. On the exam, it matters for investigations and compliance: strong audit trails must be complete enough to support timelines, attribution, and integrity checks.

11. **Baseline**
    A baseline is a known-good reference point for system configuration, performance, or security settings. On the SSCP exam it shows up in monitoring and change scenarios, where you must decide whether behavior is normal, suspicious, or the result of an approved change.

12. **Bastion host**
    A bastion host is a hardened system placed at a boundary to provide controlled administrative access into a more sensitive network. Exam questions often test why it exists, how it reduces attack surface, and what extra controls (like strong authentication and logging) make it defensible.

13. **Bring Your Own Device (BYOD)**
    BYOD is an organizational model that allows personally owned devices to access corporate resources. On the exam, the decision point is risk control: device posture,

data separation, remote wipe, and access restrictions that keep sensitive data protected even when the endpoint is not fully owned.

14. **Brute force attack**
    A brute force attack attempts many password or key combinations until one works, often using automation. SSCP questions typically focus on which controls blunt it fastest, such as multifactor authentication, account lockout and throttling, and monitoring for repeated failures.

15. **Business continuity plan (BCP)**
    A business continuity plan describes how critical operations continue during and after a disruptive event. On the exam, it commonly appears alongside disaster recovery, and you are tested on choosing actions that keep essential services available at an acceptable level.

16. **Business Impact Analysis (BIA)**
    A BIA identifies critical processes and quantifies the impact of outages, helping set priorities and recovery targets. SSCP items use BIA to test “what comes first” decisions, such as which system gets restored first and what downtime is acceptable.

17. **Certificate authority (CA)**
    A certificate authority issues and manages digital certificates that bind identities to public keys. On the exam, it often appears in trust and encryption scenarios, where you must recognize how certificates support authentication, secure communications, and non-repudiation.

18. **Change management**
    Change management is the controlled process for requesting, approving, implementing, and documenting changes to systems. SSCP questions use it to test governance and accountability, especially when “unplanned” changes lead to incidents or weaken security controls.

19. **Cipher**
    A cipher is the algorithm used to perform encryption or decryption, such as a symmetric or asymmetric method. On the exam, the key is choosing a cipher and mode appropriate to the use case and recognizing weak choices that fail confidentiality or integrity goals.

20. **Compensating control**
    A compensating control is an alternative safeguard used when the 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 is supportable with evidence like logs, approvals, or monitoring results.

21. **Confidentiality**
    Confidentiality means information is only accessible to authorized people, systems, and processes. On the SSCP exam it often appears as “prevent disclosure,” where the best answer usually involves access controls plus encryption or data handling rules.

22. **Configuration management**
    Configuration management is the discipline of defining, maintaining, and tracking approved system settings over time. Exam questions use it to test control of change, repeatability, and the ability to spot unauthorized drift using records like baselines, change tickets, and configuration snapshots.

23. **Continuous monitoring**
    Continuous monitoring is the ongoing collection and review of security-relevant signals such as logs, alerts, and posture data. On the exam, it shows up as deciding what to watch, what thresholds matter, and how monitoring supports faster detection and response.

24. **Control**
    A control is a safeguard that reduces risk by preventing, detecting, or correcting unwanted events. SSCP questions frequently test choosing the most effective control type for the scenario instead of picking a control that sounds “strong” but does not address the actual risk.

25. **Corrective control**
    A corrective control reduces impact after an issue occurs, such as restoring from backup or applying a fix to remove a known weakness. On the exam, the common confusion is mixing corrective controls with preventive or detective controls; the clue is that corrective actions happen after detection.

26. **Credential**
    A credential is proof used to authenticate an identity claim, such as a password, token, certificate, or biometric factor. SSCP items test how credentials are stored,

protected, and revoked because weak credential handling usually becomes the fastest path to compromise.

27. **Credential stuffing**
    Credential stuffing is using stolen username and password pairs from one breach to attempt logins on other systems. On the exam, it often points to defenses like multifactor authentication, rate limiting, monitoring for unusual login patterns, and blocking known compromised credentials.

28. **Cryptographic hash**
    A cryptographic hash is a one-way function that produces a fixed-length digest used for integrity checking. SSCP questions typically use hashing to test integrity and tamper detection, and the key distinction is that hashing is not encryption because it is not reversible.

29. **Cryptography**
    Cryptography is the use of mathematical methods to provide confidentiality, integrity, authentication, and sometimes non-repudiation. On the SSCP exam, it shows up as selecting the right tool for the goal, such as encrypting for confidentiality versus hashing for integrity.

30. **Data classification**
    Data classification is assigning sensitivity levels to data so handling rules match business risk, such as public, internal, confidential, or restricted. SSCP scenarios use classification to test which safeguards apply, like encryption requirements, access restrictions, retention, and secure disposal.

31. **Data Loss Prevention (DLP)**
    Data Loss Prevention is a set of controls that detect and help prevent sensitive data from leaving approved boundaries, such as by email, web upload, or removable media. On the SSCP exam, it shows up as choosing controls that reduce data exfiltration risk, and the common confusion is assuming DLP replaces encryption or access control rather than complementing them.

32. **Data owner**
    A data owner is the person or role accountable for a data set’s classification, permitted use, and access approvals. Exam questions often test responsibility boundaries, where the owner sets rules while administrators implement technical controls and auditors verify evidence like approval records.

33. **Data retention**
    Data retention is keeping information for a defined period to meet business, legal, and risk requirements, then disposing of it properly. On the exam, retention shows up as a governance decision point, where keeping data too long increases exposure while deleting too early can violate requirements.

34. **Decryption**
    Decryption is converting ciphertext back into readable plaintext using the correct key and algorithm. SSCP items use decryption to test practical understanding of where keys live, who should have access, and what happens when key management is weak.

35. **Defense in depth**
    Defense in depth is layering multiple independent safeguards so one control failure does not cause a full compromise. On the exam, it appears in architecture questions where the best answer is usually a combination of segmentation, access control, monitoring, and hardening rather than a single “magic” tool.

36. **Detective control**
    A detective control identifies that an event has occurred, such as logging, alerting, intrusion detection, or file integrity monitoring. SSCP questions often test whether a choice actually detects versus prevents, and the scenario usually expects you to pair detection with response steps.

37. **Disaster recovery plan (DRP)**
    A disaster recovery plan describes how to restore systems and data after a major disruption, focusing on technology recovery. On the exam, DRP is frequently contrasted with business continuity, and you are tested on selecting steps that restore critical services within agreed recovery targets.

38. **Demilitarized zone (DMZ)**
    A demilitarized zone is a network segment that hosts public-facing services while isolating internal networks from direct exposure. SSCP scenarios use DMZs to test segmentation choices, rule placement, and how to limit blast radius when an internet-exposed system is attacked.

39. **Due care**
    Due care is taking reasonable, prudent steps to protect assets, consistent with the organization’s obligations and risk profile. On the exam, it shows up as governance

language that supports defensible decisions, often tied to having policies, standards, and documented controls in place.

40. **Due diligence**
    Due diligence is the investigation and validation performed before making a decision, such as assessing a vendor, selecting a control, or approving an exception. SSCP questions commonly test that diligence happens before action, and that evidence like assessments, questionnaires, or review notes supports the decision.

41. **Encryption**
    Encryption transforms readable data into ciphertext so only authorized parties with the correct key can read it. On the SSCP exam, it shows up as choosing the right protection for data at rest versus data in transit, and recognizing that weak key handling can undo strong algorithms.

42. **Endpoint Detection and Response (EDR)**
    EDR is a set of endpoint tools and processes that collect telemetry, detect suspicious behavior, and support investigation and containment on hosts. Exam scenarios often test what EDR is best at (visibility and response) versus what it is not (a complete substitute for patching, least privilege, or network controls).

43. **Endpoint security**
    Endpoint security is the protective control set applied to devices like workstations, servers, and mobile endpoints, including hardening, patching, anti-malware, and device control. On the exam, the decision point is usually selecting controls that reduce the most likely compromise path for that endpoint type while preserving required business use.

44. **Evidence**
    Evidence is the reliable information used to support conclusions about what happened and what controls were in place, such as logs, screenshots, tickets, approvals, and configuration records. On the SSCP exam, evidence matters because many questions ask what proves a claim or what data an analyst needs before escalating or remediating.

45. **Event correlation**
    Event correlation links related security events across sources to identify patterns that a single alert would not reveal. SSCP questions use correlation to test

monitoring maturity, such as combining authentication logs with network alerts to distinguish false positives from a real incident.

46. **Exploit**
    An exploit is a technique or code that takes advantage of a vulnerability to cause unintended behavior, such as gaining execution or elevating privileges. On the exam, the confusion often lies in mixing up vulnerability, threat, and exploit; the exploit is the action that turns a weakness into impact.

47. **Exposure**
    Exposure is the degree to which an asset is reachable or susceptible, given its configuration, access paths, and protections. SSCP scenarios use exposure to test risk thinking, where reducing attack surface through segmentation, hardening, or access control is often the fastest win.

48. **Failover**
    Failover is the automatic or manual switching to a redundant system or component when the primary fails. On the SSCP exam, it appears under availability and recovery, where you must match failover design to the stated uptime need and recognize dependencies that can still create single points of failure.

49. **Firewall**
    A firewall enforces traffic rules between networks or zones, typically based on addresses, ports, protocols, and sometimes applications or identities. SSCP questions often test placement and purpose: firewalls support segmentation and policy enforcement, but they do not fix weak authentication or insecure applications by themselves.

50. **Forensics**
    Forensics is the disciplined collection and analysis of digital evidence to understand events while preserving integrity and traceability. On the SSCP exam, it shows up in incident response choices, including when to capture volatile data, how to preserve logs, and how to avoid contaminating evidence during investigation.