CCSP Exam Glossary

Find more at BareMetalCyber.com

1. **ABAC (Attribute-Based Access Control)**
   ABAC is an access-control approach that grants or denies access based on attributes such as user role, device posture, location, data sensitivity, and time. On the exam, ABAC often appears as the “best fit” when role-only rules are too coarse and the scenario needs policy decisions tied to data classification and cloud context.

2. **Accountability**
   Accountability is the ability to tie actions and outcomes to a specific identity or responsible party, including service accounts and delegated administrators. It matters because cloud security decisions frequently hinge on proving who did what, where it was recorded, and whether the evidence can stand up to audit or investigation.

3. **Advanced Item Types**
   Advanced item types are non-traditional question formats that may require multiple selections or structured interaction rather than a single best answer. They matter because they can test whether you can apply controls and evidence logic across several conditions, not just recall a definition. ISC2

4. **Anonymization**
   Anonymization is the process of transforming data so individuals can no longer be identified, even when combined with other datasets. On the exam, it commonly shows up as a privacy or regulatory decision point, where the key is understanding when anonymization reduces compliance scope versus when it still leaves re-identification risk.

5. **API Security**
   API security is the set of controls that protect application programming interfaces from misuse, data exposure, and unauthorized access, including strong authentication, authorization, input validation, and rate limiting. It matters because cloud applications often expose APIs as primary interfaces, and exam scenarios frequently test whether you prioritize identity, secrets handling, and logging as the real control boundaries.

6. **Archiving**
   Archiving is the long-term preservation of data for business, legal, or regulatory reasons, usually with controlled access and integrity protections. It matters on the exam because retention and deletion choices must match stated requirements, and "archive" is not the same as "backup" or "delete."

7. **Asset Inventory**
   An asset inventory is an up-to-date record of cloud resources and related components, such as workloads, identities, storage locations, and third-party services. On the exam, this often appears as a prerequisite for risk assessment, monitoring coverage, and proving scope in shared-responsibility scenarios.

8. **Assurance Report**
   An assurance report is independent evidence about a provider's controls, such as SOC reports or ISO certifications, used to support risk and compliance decisions. It matters because exam questions often ask what evidence is credible, what it covers, and what gaps still require customer-side controls or contract clauses.

9. **Auditability**
   Auditability is the ability to reconstruct events and control performance using reliable records, such as logs, configuration history, and approvals. It matters because CCSP scenarios frequently reward answers that are not only "secure," but also provable with traceable evidence across cloud layers.

10. **Authentication**
    Authentication is verifying an identity claim (user, workload, or service) before granting access. On the exam, authentication decisions often separate "good" from "best" answers when the scenario involves federation, privileged access, service accounts, or multi-factor requirements.

11. **Authorization**
    Authorization is deciding what an authenticated identity is allowed to do, such as which data it can read or which admin action it can perform. On the exam, the common trap is confusing authentication with authorization, and missing least privilege as the decision driver when roles or policies are too broad.

12. **Availability**
    Availability is ensuring systems and data are accessible when needed, including resilience against outages and disruptions. It shows up as tradeoffs between

redundancy, failover, and dependency design, and it is often tested alongside service level expectations and shared responsibility boundaries.

13. **Backup**
A backup is a point-in-time copy of data used for recovery after loss, corruption, or ransomware-style events. On the exam, “backup” is rarely the whole answer; the scenario often expects restore testing, defined recovery targets, and clarity on what is backed up versus what is rebuilt.

14. **BC/DR (Business Continuity / Disaster Recovery)**
BC/DR is the planning and capability to continue operations and recover services after disruptive events. It matters because cloud designs can fail if dependencies, regions, or identity systems are not included in recovery planning, and exam questions often ask for the most realistic recovery evidence.

15. **BYOK (Bring Your Own Key)**
BYOK is a key management model where the customer supplies and controls encryption keys used by the cloud service. On the exam, it often appears as a control choice for sensitive data, with the key decision being who can decrypt, how keys are rotated, and what logs prove key use.

16. **CASB (Cloud Access Security Broker)**
A CASB is a security control layer that helps enforce policy for cloud service use, commonly providing visibility, data protection controls, and governance for sanctioned and unsanctioned cloud apps. It matters because questions frequently test when to use a CASB for data loss prevention and access control versus relying only on native cloud controls.

17. **CAT (Computerized Adaptive Testing)**
CAT is an exam delivery method where the test adapts to your performance by selecting subsequent questions based on prior answers. It matters because pacing and confidence matter, and you cannot rely on seeing a fixed number of questions or a predictable distribution of difficulty.

18. **Chain of Custody**
Chain of custody is the documented handling history of evidence, showing who collected it, where it was stored, who accessed it, and when. On the exam, it appears in incident response and legal scenarios where evidence must be defensible and tamper-evident.

19. **CIA Triad (Confidentiality, Integrity, Availability)**
The CIA triad is a foundational way to frame security goals: protect secrecy, prevent unauthorized change, and keep services accessible. It matters because many "best" answers are the ones that correctly prioritize which part of CIA is most at risk in the scenario.

20. **Cloud Deployment Model**
A cloud deployment model describes where and how cloud services are hosted and consumed, typically public, private, hybrid, or community. On the exam, picking the right model clarifies trust boundaries and compliance constraints, and it prevents wrong-first-step control choices.

21. **Cloud Service Model**
A cloud service model describes what the provider delivers and what the customer must secure, typically IaaS, PaaS, or SaaS. On the exam, correctly identifying the model is often the first step because it drives which controls you can configure and what evidence you can realistically produce.

22. **Compliance Mapping**
Compliance mapping is the process of linking security controls to legal, regulatory, and contractual requirements. It matters because CCSP questions often test whether you can show coverage without overclaiming, and whether you recognize gaps that require additional controls or compensating measures.

23. **Confidentiality**
Confidentiality is preventing unauthorized access to data, whether at rest, in transit, or in use. On the exam, confidentiality decisions commonly involve data classification, encryption choices, identity controls, and proving who can access or decrypt sensitive data.

24. **Configuration Baseline**
A configuration baseline is an approved, documented standard configuration for systems and services that can be measured against and maintained over time. It matters because cloud drift is common, and exam scenarios frequently reward answers that emphasize known-good settings plus monitoring and change approval evidence.

25. **Container**
A container is a lightweight packaging format that includes an application and its dependencies while sharing the host operating system kernel. On the exam,

container security shows up through image provenance, isolation limits, runtime permissions, and the risk of treating containers like fully isolated virtual machines.

26. **Continuous Monitoring**
    Continuous monitoring is the ongoing collection and review of security-relevant signals such as logs, alerts, configuration changes, and access events. It matters because CCSP scenarios often test whether you can detect and respond in time, and whether monitoring is complete across identities, network paths, and data stores.

27. **Control Objective**
    A control objective is the security outcome a control is meant to achieve, such as preventing unauthorized access or ensuring accurate audit logs. On the exam, control objectives help you pick the best answer when multiple tools are mentioned, because the right choice is the one that meets the objective with clear evidence.

28. **Corrective Control**
    A corrective control is a control that fixes or restores after an issue is detected, such as reverting a change or restoring data. It matters because exam questions often ask for the best sequence of controls, and corrective controls are usually not the first line of defense.

29. **Cryptographic Key Management**
    Cryptographic key management is the creation, storage, rotation, access control, and destruction of encryption keys. On the exam, the key decision is often not “use encryption,” but who controls the keys, how access is logged, and what happens when keys are compromised.

30. **Data Classification**
    Data classification is categorizing data by sensitivity and required protections, such as public, internal, confidential, or regulated. It matters because classification drives encryption requirements, access policies, retention rules, and residency decisions, and it is a frequent source of trick options that ignore stated sensitivity.

31. **Data Custodian**
    A data custodian is the party responsible for implementing and maintaining the controls that protect data, such as access controls, backups, and monitoring. On the exam, the custodian is often different from the data owner, and confusion here leads to wrong answers about who approves access and who provides evidence.

32. **Data Lifecycle**
    The data lifecycle is the full path data takes from creation and collection through storage, use, sharing, archiving, and destruction. It matters because many CCSP questions test whether controls cover every stage, not just encryption at rest or access at login.

33. **Data Owner**
    A data owner is the party accountable for the data's business use and protection requirements, including classification and acceptable risk decisions. On the exam, owners typically approve access and define handling rules, while technical teams implement controls and provide operational evidence.

34. **Data Remanence**
    Data remanence is residual data that remains after deletion, such as blocks in storage systems or snapshots that still contain sensitive content. It matters because cloud storage and backups can preserve copies in unexpected places, and exam scenarios often test secure disposal and verification.

35. **Data Residency**
    Data residency is the requirement that data be stored and sometimes processed within specific geographic or legal jurisdictions. It matters because CCSP questions frequently include regulatory or contractual constraints, and the "best" answer usually respects residency while maintaining security and auditability.

36. **Data Tokenization**
    Tokenization replaces sensitive data elements with non-sensitive tokens while keeping the original values protected in a secure mapping system. On the exam, tokenization often appears as a way to reduce exposure and scope, but the key decision is whether tokens can be reversed and who controls the mapping.

37. **DLP (Data Loss Prevention)**
    DLP is a set of controls that detect and prevent sensitive data from leaving authorized boundaries, such as via email, web uploads, or cloud sharing. On the exam, DLP is often paired with classification and CASB concepts, and the trap is choosing DLP without defining what "sensitive" means in the scenario.

38. **Due Diligence**
    Due diligence is the up-front investigation and evaluation of a provider, service, or control choice before committing to it. It matters because CCSP scenarios test

whether you can select services responsibly using evidence, contract terms, and assurance reports rather than assumptions.

39. **Due Care**
Due care is the ongoing reasonable actions taken to protect assets and meet obligations after decisions are made. On the exam, due care shows up as continuous monitoring, periodic reviews, access recertification, and maintaining evidence that controls remain effective.

40. **eDiscovery**
eDiscovery is the process of identifying, preserving, collecting, and producing electronically stored information for legal proceedings. It matters because cloud storage, retention, and chain-of-custody requirements can conflict with routine operations, and exam questions often test defensible retention and evidence handling.

41. **Encryption**
Encryption is the use of cryptography to protect data confidentiality by making it unreadable without the correct key. On the exam, the best answer usually goes beyond “encrypt it” and addresses key ownership, access to decrypt, rotation, and logging that proves how encryption is used.

42. **Federation**
Federation is a trust relationship that allows identities from one system to access resources in another using shared authentication and authorization signals. It matters because many CCSP scenarios rely on centralized identity, single sign-on, and consistent access control, and the trap is missing how federation changes accountability and evidence needs.

43. **HSM (Hardware Security Module)**
An HSM is a dedicated device or service designed to generate, store, and use cryptographic keys in a tamper-resistant way. On the exam, HSMs often appear as a higher-assurance option for key protection, and the decision point is whether the scenario needs stronger key isolation, compliance alignment, or provable key-handling controls.

44. **IAM (Identity and Access Management)**
IAM is the set of processes and technical controls that manage identities, authentication, authorization, and access lifecycle. It matters because cloud security failures frequently start with overly broad permissions, weak service

accounts, and missing admin logging, so exam questions often treat IAM as the root control layer.

45. **Integrity**
    Integrity is the assurance that data and systems are accurate and have not been altered in an unauthorized or undetected way. On the exam, integrity is often tested through logging integrity, change control evidence, cryptographic hashes, and detection of tampering rather than simple access control alone.

46. **Key Rotation**
    Key rotation is the periodic replacement of cryptographic keys to reduce exposure if a key is compromised or overused. It matters because exam scenarios often test whether rotation is defined, automated where feasible, and supported by evidence such as policies, logs, and change approvals.

47. **Least Privilege**
    Least privilege is granting only the minimum access needed to perform a task, for the shortest necessary time. It matters because CCSP questions frequently include “convenient” answers that give broad permissions, and the best choice usually tightens roles, scopes, and auditability.

48. **Multi-Tenancy**
    Multi-tenancy is an architecture where multiple customers share the same underlying infrastructure while remaining logically isolated. On the exam, multi-tenancy drives risk decisions about isolation, side-channel concerns, logging, and which controls must be validated with provider evidence versus customer configuration.

49. **RPO (Recovery Point Objective)**
    RPO is the maximum acceptable amount of data loss measured in time, such as losing up to fifteen minutes of transactions. It matters because exam questions often require selecting backup and replication strategies that match RPO, not just “do backups,” and because RPO is commonly confused with RTO.

50. **RTO (Recovery Time Objective)**
    RTO is the maximum acceptable downtime before a service must be restored, measured in time such as two hours. It matters because CCSP scenarios test whether you can align availability design, failover, and operational readiness to an RTO target, and because RTO is often mixed up with RPO in answer choices.