CCISO Exam Glossary

Find more at BareMetalCyber.com

1. **Access Control**
   Access control is the set of rules and mechanisms that determine who can access systems, data, and functions, and under what conditions. On the CCISO exam it often shows up as a governance-and-oversight decision about selecting appropriate control types and proving they work through evidence like access reviews and role definitions.

2. **Acceptable Use Policy (AUP)**
   An acceptable use policy defines what users may and may not do with organizational technology and data. On the exam, the key is linking policy language to enforceability and auditability, such as whether violations trigger defined actions and whether the policy maps to training, monitoring, and disciplinary processes.

3. **Accountability**
   Accountability means specific leaders and roles are answerable for security outcomes, not just tasks being assigned. On the CCISO exam, it commonly appears in scenarios about governance structure, clear ownership of risk decisions, and whether reporting lines and decision rights are defined and defensible.

4. **Audit Evidence**
   Audit evidence is the documented proof an auditor uses to judge whether a control exists, is designed well, and operates as intended. On the exam, the trap is choosing "good-sounding" activities instead of verifiable artifacts like signed approvals, logs, tickets, reports, or test results that support a conclusion.

5. **Audit Management**
   Audit management is the planning, execution, reporting, and follow-up cycle that ensures audits produce actionable, risk-based outcomes. On the CCISO exam, it shows up as decisions about scope, independence, reporting to stakeholders, and timely remediation tracking tied back to risk.

6. **Authentication**
   Authentication is the process of proving an identity is valid, such as through passwords, tokens, certificates, or multi-factor methods. On the exam, focus on matching authentication strength to risk and explaining what evidence demonstrates correct use (for example, MFA enforcement settings and access logs).

7. **Authorization**
   Authorization is the process of granting an authenticated identity specific permissions, such as read, write, admin, or system access. On the CCISO exam, it often appears as a least-privilege judgment call, where the right answer emphasizes role design, approval workflow, and periodic access review.

8. **Availability**
   Availability means systems and information are accessible and usable when needed, consistent with business requirements. On the exam, availability is usually tested through risk tradeoffs, resilience choices, and how continuity planning and metrics tie to business objectives rather than purely technical uptime claims.

9. **Business Continuity Plan (BCP)**
   A business continuity plan is the documented approach for sustaining critical business operations during and after disruption. On the CCISO exam, it shows up as program leadership: ensuring plans are owned, tested, updated, and aligned to business priorities and recovery requirements.

10. **Business Impact Analysis (BIA)**
    A business impact analysis identifies critical processes, acceptable downtime, and the operational and financial impact of outages. On the exam, BIA is a foundational input to risk decisions and continuity strategy, and a common confusion point is mixing it up with risk assessment or technical disaster recovery planning.

11. **Capability Maturity Model**
    A capability maturity model is a structured way to rate how well a process is defined, repeatable, measured, and improving over time. On the CCISO exam, it often shows up when judging whether a security program is “ad hoc” versus “managed,” and what evidence would prove sustained, repeatable performance.

12. **Change Management**
    Change management is the controlled process for requesting, approving, implementing, and reviewing changes to systems and configurations. On the exam, it appears as a governance and risk control that reduces outages and security drift, with emphasis on approvals, rollback planning, and traceable records.

13. **Chief Information Security Officer (CISO)**
    A CISO is the executive role accountable for leading the organization’s information security strategy, governance, and risk-based decisions. On the CCISO exam, the focus is less on hands-on technical work and more on leadership duties like aligning to business objectives, communicating risk, and setting program direction. E

14. **Confidentiality**
    Confidentiality means information is protected from unauthorized disclosure. On the CCISO exam, confidentiality is tested through decisions about data classification, access boundaries, and vendor or cloud arrangements where the key confusion is “private” data versus “properly controlled” data.

15. **Conflict of Interest**
    A conflict of interest is a situation where personal or organizational incentives could bias security decisions, oversight, or audit conclusions. On the exam, it typically appears in governance and audit scenarios where independence and objective reporting matter more than good intentions.

16. **Continuous Monitoring**
    Continuous monitoring is the ongoing measurement of control performance, risk indicators, and security posture over time. On the CCISO exam, it shows up as a program-management expectation: defining what gets measured, how often, who reviews it, and what actions follow when thresholds are breached.

17. **Control Objective**
    A control objective is the intended security outcome a control is supposed to achieve, such as preventing unauthorized access or detecting misuse. On the exam, it’s common to be given a scenario and asked to select the control that best meets the objective, not the one with the most features.

18. **Control Selection**
    Control selection is choosing specific safeguards that reduce risk to an acceptable level within business constraints. On the CCISO exam, the decision point is matching controls to threat likelihood and business impact, while considering feasibility, cost, and measurable effectiveness.

19. **Corrective Action Plan (CAP)**
    A corrective action plan is a documented set of steps, owners, and deadlines to remediate control gaps or audit findings. On the exam, the key is showing governance discipline: prioritizing by risk, tracking progress, validating closure with evidence, and preventing repeat findings.

20. **Cyber Risk Appetite**
    Cyber risk appetite is the amount and type of security risk an organization is willing to accept in pursuit of its objectives. On the CCISO exam, it often appears as the “why” behind control choices, exceptions, and investment decisions, and it should be expressed in a way leaders can approve and measure.

21. **Data Classification**
    Data classification is the process of categorizing information (for example, public, internal, confidential) based on sensitivity and impact. On the CCISO exam, it shows up as the foundation for selecting controls, setting handling rules, and justifying why certain data needs tighter access, encryption, or monitoring.

22. **Data Governance**
    Data governance is the set of decision rights, policies, and oversight practices that ensure data is managed consistently across the organization. On the CCISO exam, it commonly appears in scenarios where accountability is unclear, and the best answer ties ownership, standards, and reporting to measurable outcomes.

23. **Data Owner**
    A data owner is the role accountable for how a specific dataset is used, protected, shared, and retained, usually aligned to a business function. On the CCISO exam, this matters when deciding who approves access, who accepts risk, and whose sign-off makes an access or retention decision defensible.

24. **Data Privacy**
    Data privacy focuses on appropriate collection, use, sharing, and protection of personal or regulated information, based on law and policy. On the CCISO exam, it often appears as a governance decision where the confusion is mixing “privacy” (rights and permitted use) with “security” (controls and protection).

25. **Data Retention**
    Data retention defines how long information is kept and when it is securely disposed, based on legal, operational, and risk requirements. On the CCISO exam, it shows up in risk tradeoffs: retaining too long increases exposure, while deleting too early can violate legal hold, audit, or business needs.

26. **Defense in Depth**
    Defense in depth is a strategy that uses multiple layers of controls so a single failure does not create a full compromise. On the CCISO exam, it’s tested as a design principle and investment rationale, especially when selecting balanced preventive, detective, and corrective controls.

27. **Delegation of Authority**
    Delegation of authority is the formal assignment of decision-making power to specific roles, with clear limits and accountability. On the CCISO exam, it appears when evaluating whether security approvals and exceptions are made by the right level of leadership and documented in a repeatable way.

28. **Disaster Recovery Plan (DRP)**
    A disaster recovery plan is the documented approach for restoring systems and technology services after a disruption. On the CCISO exam, the key is aligning recovery activities to business requirements and proving readiness through testing, recovery objectives, and evidence of lessons learned.

29. **Due Care**
    Due care is acting with the level of prudence a reasonable organization would use to protect information and manage risk. On the CCISO exam, it often appears in governance and liability contexts, where the best answers reflect consistent, documented, and risk-based decision-making.

30. **Due Diligence**
    Due diligence is the investigation and evaluation performed before making a security decision, such as selecting a vendor or approving a major change. On the CCISO exam, it's frequently tested as "show your homework," meaning risk assessment, validation, and documented review rather than assumptions or informal trust.

31. **Encryption**
    Encryption is the use of cryptography to transform data so only authorized parties can read it with the correct key. On the CCISO exam, it appears as a control choice tied to data classification and threat models, and the common trap is assuming encryption alone solves access control, key management, or misuse.

32. **Enterprise Risk Management (ERM)**
    Enterprise risk management is the organization-wide approach to identifying, assessing, treating, and reporting risks across all functions, not just security. On the CCISO exam, ERM matters because security risk must be expressed in business terms and integrated into the same decision process leaders use for financial, operational, and compliance risk.

33. **Exception Management**
    Exception management is the controlled process for approving, documenting, time-bounding, and reviewing deviations from policy or standards. On the CCISO exam, the decision point is ensuring exceptions have clear justification, compensating controls, an owner who accepts risk, and a defined expiration or review cycle.

34. **Executive Reporting**
    Executive reporting is the practice of communicating security posture, risk, and program performance in a way senior leaders can act on. On the CCISO exam, it's

tested as clarity and relevance: metrics should connect to business impact, trends, and decisions, not raw technical dashboards.

35. **Governance**
    Governance is the structure of oversight, decision rights, policies, and accountability that directs and controls the security program. On the CCISO exam, governance shows up as “who decides what” and “how it is enforced,” including committees, charters, reporting lines, and documented authority.

36. **Incident Response Plan (IRP)**
    An incident response plan defines how the organization detects, analyzes, contains, eradicates, and recovers from security incidents. On the CCISO exam, it’s typically tested through leadership choices: roles, escalation, communications, evidence handling, and ensuring the plan is exercised and improved.

37. **Information Security Program**
    An information security program is the coordinated set of policies, processes, people, and controls that manage security risk over time. On the CCISO exam, the emphasis is program leadership: alignment to business goals, measurable objectives, funding priorities, and repeatable governance rather than isolated technical projects.

38. **Integrity**
    Integrity means information remains accurate, complete, and protected from unauthorized modification or destruction. On the CCISO exam, integrity appears in scenarios about logging, change control, transaction accuracy, and tamper evidence, with a common confusion between “data quality” and “security integrity controls.”

39. **Key Performance Indicator (KPI)**
    A key performance indicator is a metric that reflects whether a program activity is achieving its intended performance outcome. On the CCISO exam, KPIs are tested as management tools: selecting measures that drive action, demonstrate progress, and avoid vanity metrics that look good but do not reduce risk.

40. **Key Risk Indicator (KRI)**
    A key risk indicator is a metric that signals increasing or decreasing risk exposure, often used for early warning and trend detection. On the CCISO exam, KRIs matter because leadership needs triggers and thresholds that prompt decisions, such as rising critical vulnerabilities, incident rates, or control failures.

41. **Legal Hold**
    A legal hold is a directive to preserve potentially relevant information for litigation, investigation, or regulatory inquiry, overriding normal retention and deletion. On the CCISO exam, it shows up in governance and incident contexts where the right answer protects evidence integrity and coordinates with legal before systems are altered or data is purged.

42. **Material Risk**
    Material risk is a risk significant enough to influence business decisions, financial outcomes, regulatory exposure, or stakeholder confidence. On the CCISO exam, it appears as a reporting and prioritization concept: leaders focus on what could change the business, not what is merely interesting from a technical standpoint.

43. **Metrics and Measurement**
    Metrics and measurement are the methods for quantifying security performance, control effectiveness, and risk trends over time. On the CCISO exam, the key is selecting measures that support decisions and accountability, with common confusion between activity counts (busy work) and outcome measures (risk reduction).

44. **Risk Acceptance**
    Risk acceptance is the formal decision to live with a known risk when it falls within appetite or when treatment costs outweigh benefits. On the CCISO exam, it is tested through governance discipline: documented rationale, named risk owner, defined scope, and a review cadence so acceptance does not become permanent neglect.

45. **Risk Assessment**
    Risk assessment is the process of identifying threats, vulnerabilities, likelihood, and impact to determine risk level and treatment options. On the CCISO exam, it often appears as the “first move” in program decisions, and the trap is skipping assessment and jumping straight to tools or controls.

46. **Risk Register**
    A risk register is a structured record of identified risks, their ratings, owners, treatments, and current status. On the CCISO exam, it shows up as proof of program maturity because it creates traceability from discovery to decision, funding, remediation, and residual risk reporting.

47. **Risk Treatment**
    Risk treatment is selecting and implementing a response to risk, typically avoid,

mitigate, transfer, or accept. On the CCISO exam, it is tested as choosing the most defensible option given business constraints, and showing how treatment decisions are tracked and verified.

48. **Security Awareness and Training**
    Security awareness and training is the program that builds user understanding and behaviors that reduce human-driven risk. On the CCISO exam, it appears as a measurable control: audience targeting, role-based depth, testing effectiveness, and evidence that training supports policy and reduces incidents.

49. **Third-Party Risk Management (TPRM)**
    Third-party risk management is the process for evaluating, contracting, monitoring, and responding to risks introduced by vendors and service providers. On the CCISO exam, it's tested as governance and lifecycle control: due diligence, contract requirements, ongoing oversight, and what to do when a supplier fails expectations.

50. **Vulnerability Management**
    Vulnerability management is the continuous process of discovering, prioritizing, remediating, and verifying weaknesses in systems and applications. On the CCISO exam, it often shows up as a prioritization and accountability scenario where risk-based triage, remediation evidence, and exception handling matter more than raw scan volume.