CRISC Exam Glossary

Find more at BareMetalCyber.com

1. **Acceptable risk**
   The amount of risk an organization is willing to tolerate without taking additional action. On the exam, this shows up when deciding whether a risk treatment is required or whether a documented acceptance (with the right approval) is the most appropriate response.

2. **Accountability**
   Clear ownership for risk decisions and control outcomes, meaning a named role is answerable for results. CRISC questions often test whether accountability is assigned to the right level (business owner versus technical team) and whether decisions are formally approved and traceable.

3. **Asset**
   Anything of value that must be protected or managed, such as data, systems, processes, people, or third-party services. On the exam, assets anchor risk scenarios, because likelihood and impact are assessed relative to what the asset supports and how it is used.

4. **Asset classification**
   A structured way to label assets (especially data) by sensitivity and criticality, so controls and handling requirements match the risk. Exam items commonly use classification to test whether the selected safeguards and reporting obligations make sense for the asset's importance.

5. **Asset inventory**
   A maintained record of assets, typically including what exists, where it is, who owns it, and how it connects to other systems. CRISC scenarios use weak inventories to create gaps in risk identification, control coverage, or monitoring, and the "best next step" is often improving visibility first.

6. **Asset owner**
   The person or role responsible for defining the asset's value, acceptable use, and risk tolerance, even if IT operates the technology. On the exam, this matters when choosing who should approve risk acceptance, sign off on control exceptions, or receive risk reports.

7. **Assurance**
   Confidence that controls are designed appropriately and operating effectively,

based on evidence rather than opinion. CRISC questions often frame assurance through testing results, metrics, or independent reviews that support a risk decision or a report to stakeholders.

8. **Attack surface**
   The set of ways a threat could interact with a system or process, such as exposed services, privileged accounts, integrations, and third-party connections. On CRISC, it helps shape risk scenarios and control selection, especially when evaluating how changes in technology increase likelihood.

9. **Baseline**
   A defined "normal" state used for comparison, such as normal access patterns, configuration standards, or expected performance ranges. Exam scenarios use baselines to test monitoring choices and to distinguish true emerging risk signals from routine variation.

10. **Business impact analysis (BIA)**
    A method to identify and quantify the consequences of disruption to business processes, including time sensitivity and downstream effects. On the exam, BIA logic supports impact estimates in risk assessments and strengthens decisions about prioritizing treatment plans and reporting severity.

11. **Business case**
    A documented justification for a proposed change, including expected benefits, costs, and key risks. On the exam, business cases matter because risk decisions should support business value, and weak cases often hide assumptions that inflate benefits or minimize impact.

12. **Business continuity plan (BCP)**
    A plan for keeping critical business processes running during and after a disruption. CRISC questions use BCP to test whether risk response choices protect the most time-sensitive processes and whether recovery expectations are evidence-based, not wishful.

13. **Business objective**
    A concrete outcome the organization is trying to achieve, such as revenue growth, regulatory compliance, or uptime targets. On the exam, objectives help determine risk appetite and priorities, because the "best" control or response is the one that protects what the business is actually trying to do.

14. **Business process**
    A repeatable set of activities that produces a business result, like order fulfillment or

payroll. CRISC scenarios often hinge on understanding the process flow so the correct risk is identified, the impact is realistic, and control ownership is assigned to the right place.

15. **Business process owner**
    The role accountable for how a business process performs, including its risk acceptance and control expectations. On the exam, this term shows up in governance and reporting decisions, especially when determining who should approve exceptions or receive risk updates.

16. **Business requirement**
    A stated need the solution must meet, such as confidentiality needs, auditability, or a service level. CRISC items use requirements to test whether a proposed control set is adequate, and whether tradeoffs are explicitly aligned to what must not fail.

17. **Business risk**
    The possibility that an event will prevent the organization from achieving its objectives. On CRISC, the key is linking technology risk to business outcomes, because the exam rewards answers that translate technical problems into measurable business impact.

18. **Business scenario**
    A short description of how the organization operates in a specific context, including constraints, dependencies, and assumptions. On the exam, scenarios help you frame likelihood and impact correctly and avoid “generic security” answers that do not fit the business reality.

19. **Business unit**
    A distinct organizational segment with its own goals, budget pressures, and operational needs. CRISC questions use business units to test governance, because risk ownership and reporting should match where decisions are made, not where the technology happens to sit.

20. **Business value**
    The benefit the organization gains from a process, system, or investment, such as revenue, efficiency, reliability, or compliance confidence. On the exam, business value guides prioritization, because the most appropriate risk response usually protects high-value outcomes with proportionate effort.

21. **Capability maturity**
    A measure of how well a process is defined, repeatable, and consistently performed over time. On the exam, maturity affects risk because low maturity increases

variability and control failure likelihood, and it influences whether “improve the process” is a better response than adding tools.

22. **Cause**
    The underlying reason a risk event could occur, such as weak access governance or unpatched dependencies. CRISC questions often separate cause from impact, and good answers target the cause with controls rather than only reacting to symptoms.

23. **Change management**
    A controlled process for requesting, assessing, approving, implementing, and documenting changes. On CRISC, change management is a frequent decision point because unmanaged change increases likelihood and reduces assurance, especially for production systems and regulated data.

24. **Compensating control**
    An alternative control used when the primary control cannot be implemented, intended to reduce risk to an acceptable level. Exam questions test whether the compensating control truly addresses the same risk and whether it is documented, approved, and measurable.

25. **Compliance**
    The state of meeting legal, regulatory, contractual, or internal policy requirements. On CRISC, compliance is often treated as a constraint on risk response, because some risks cannot be accepted if they would violate mandatory obligations.

26. **Confidentiality**
    Protecting information from unauthorized access or disclosure. CRISC items use confidentiality to connect controls to business impact, such as reputation damage, legal exposure, or loss of competitive advantage when sensitive data is exposed.

27. **Control**
    A safeguard or process that reduces risk by preventing, detecting, or correcting unwanted outcomes. On the exam, you are frequently asked to evaluate whether a control is appropriate, effective, and aligned to the risk scenario rather than simply “more security.”

28. **Control deficiency**
    A weakness in design or operation that prevents a control from achieving its intended purpose. CRISC questions test how you respond: determine the risk implication, document it, communicate to the right stakeholders, and decide whether remediation or an exception is warranted.

29. **Control objective**
    The intended outcome a control is supposed to achieve, stated in business-relevant terms. On CRISC, control objectives help you choose the right control type and avoid confusing a control activity (what is done) with the outcome it must produce.

30. **Control owner**
    The role responsible for ensuring a specific control exists, is maintained, and performs as expected. Exam scenarios use this term to test governance and accountability, because the correct owner is often a business or process owner, not automatically IT or security.

31. **Corrective control**
    A control that fixes an issue after it has been detected, such as restoring systems, removing malicious changes, or closing a policy gap. On the exam, corrective controls are commonly contrasted with preventive and detective controls, and you may need to pick the best mix for the scenario.

32. **COSO**
    A widely used internal control framework (from the Committee of Sponsoring Organizations of the Treadway Commission) often referenced in governance and assurance contexts. CRISC questions may use COSO to test how control frameworks support consistent risk and control language across the organization.

33. **Coverage**
    How completely controls or assessments address the relevant scope, such as all critical assets, all high-risk processes, or all required control objectives. On CRISC, “coverage gaps” are a common trap, because a control can look strong but still fail if it ignores key systems, users, or third parties.

34. **Criteria**
    The standards or requirements used to judge whether something is acceptable, such as policy requirements, risk appetite thresholds, or control test expectations. Exam items use criteria to test whether conclusions are justified by agreed measures rather than personal preference.

35. **Criticality**
    The degree to which an asset or process is essential to mission or business objectives, especially during disruption. On the exam, criticality drives prioritization, because the correct response often focuses on what must recover first and what failure would cost most.

36. **Data owner**
    The role accountable for how data is used, protected, and shared, including classification and retention expectations. CRISC scenarios use data owners to test approval paths for access, exceptions, and risk acceptance tied to sensitive information.

37. **Detective control**
    A control that identifies events or conditions after they occur, such as monitoring, alerts, reconciliations, or audit logs. On CRISC, detective controls are often evaluated based on timeliness and actionability, because detection without response does not reduce impact.

38. **Detection time**
    The time between the start of an adverse event and when it is discovered. On the exam, detection time influences impact and response selection, because shorter detection reduces loss and can change whether a risk is acceptable.

39. **Due care**
    The level of prudence and attention expected from a reasonable organization in similar circumstances. CRISC questions use due care to test governance decisions, especially where failing to act on known risks could create legal, regulatory, or fiduciary exposure.

40. **Due diligence**
    The investigation and analysis performed before making a decision, such as evaluating a vendor, a technology change, or a risk treatment option. On CRISC, due diligence often appears as the “right next step” before acceptance or implementation, because the exam values evidence-based decisions.

41. **Enterprise risk management (ERM)**
    A coordinated approach for identifying, assessing, responding to, and reporting risk across the organization. On the exam, ERM matters because CRISC risk decisions should fit into an enterprise view, not a siloed “IT-only” perspective.

42. **Exposure**
    The condition of being subject to loss due to a threat, vulnerability, and asset relationship, often described as the extent of potential harm. CRISC questions use exposure to test whether you can explain risk in business terms and prioritize what creates the largest meaningful loss.

43. **Governance**
    The structures and decision rights that ensure risk and control activities support

business objectives and accountability. On CRISC, governance shows up as “who decides what,” “who approves,” and “who receives reporting,” with an emphasis on traceability and alignment to risk appetite.

44. **Inherent risk**
    The level of risk that exists before any controls are applied. On the exam, inherent risk is contrasted with residual risk to test whether controls are actually reducing risk and whether the remaining exposure is acceptable.

45. **Integrity**
    Protecting information and processing from unauthorized modification, ensuring accuracy and completeness. CRISC items use integrity in scenarios like financial reporting, configuration baselines, and transaction processing where silent changes can be more damaging than downtime.

46. **Issue management**
    The process for logging, prioritizing, assigning, tracking, and closing control gaps or risk-related findings. On the exam, issue management matters because unresolved findings increase residual risk and weak tracking breaks assurance and reporting credibility.

47. **Key risk indicator (KRI)**
    A metric designed to signal changes in risk exposure, ideally early enough to trigger action. CRISC questions test whether a chosen KRI is predictive and tied to a specific risk scenario, not just a generic performance metric.

48. **Likelihood**
    The probability that a risk event will occur within a defined timeframe, based on evidence and assumptions. On CRISC, likelihood choices are often tested through scenario cues like control strength, threat activity, process maturity, and frequency of change.

49. **Residual risk**
    The risk remaining after controls and risk responses are applied. On the exam, residual risk is the key decision point for acceptance versus further treatment, and it must be compared against risk appetite and documented approval criteria.

50. **Risk appetite**
    The overall amount of risk an organization is willing to pursue or retain to achieve objectives. CRISC questions frequently test risk appetite as the governing constraint, because it drives thresholds, prioritization, escalation, and whether acceptance is allowed.