CCISO 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

1. A CISO is asked to approve a temporary deviation from a security policy for a business unit that cannot meet the requirement this quarter. The CISO wants to ensure the deviation does not become permanent neglect and is governed properly. What is the best program process to apply?
   A. Exception Management
   B. Change Management
   C. Continuous Monitoring
   D. Audit Management

2. A security leader must explain security posture to senior executives in a way they can act on, focusing on business impact, trends, and decisions rather than raw technical dashboards. What practice best fits this need?
   A. Continuous Monitoring
   B. Executive Reporting
   C. Control Selection
   D. Vulnerability Management

3. A team has proven user identity using a strong method, but now must determine what specific actions that user can perform in a system. Which concept is being applied?
   A. Authentication
   B. Access Control
   C. Authorization
   D. Accountability

4. After a security incident, legal counsel issues a directive that overrides normal retention and deletion so potentially relevant information is preserved. What is this directive called?
   A. Data Retention
   B. Business Continuity Plan (BCP)
   C. Disaster Recovery Plan (DRP)
   D. Legal Hold

5. Leadership wants a clear statement of how much cyber risk the organization is willing to accept so control choices, exceptions, and investments can be justified in business terms. What is the most relevant concept?
   A. Cyber Risk Appetite
   B. Risk Treatment

C. Material Risk
D. Governance

6. Before selecting a critical vendor, the organization performs investigation and evaluation to support a defensible decision rather than relying on informal trust. What concept does this describe?
   A. Due Care
   B. Due Diligence
   C. Accountability
   D. Audit Evidence

7. A review finds that security teams are tracking "number of scans run" but leaders want metrics that signal increasing risk exposure and provide early warning triggers for decisions. What type of metric should be emphasized?
   A. Key Performance Indicator (KPI)
   B. Metrics and Measurement
   C. Key Risk Indicator (KRI)
   D. Control Objective

8. A control is being debated in a scenario, and the exam question focuses on the intended security outcome the control is supposed to achieve rather than the tool or feature set. What is that intended outcome called?
   A. Control Selection
   B. Audit Evidence
   C. Enterprise Risk Management (ERM)
   D. Control Objective

9. A security program uses multiple layers of safeguards so that if one control fails, a full compromise is less likely. What strategy does this describe?
   A. Defense in Depth
   B. Confidentiality
   C. Integrity
   D. Availability

10. During continuity planning, leaders need a foundational input that identifies critical processes, acceptable downtime, and the operational and financial impact of outages so recovery priorities align to the business. What is this called?
    A. Risk Assessment
    B. Business Impact Analysis (BIA)

C. Disaster Recovery Plan (DRP)
D. Business Continuity Plan (BCP)

---

1. Correct Answer: A. Exception Management
   Explanation: Exception management is the controlled process for approving, documenting, time-bounding, and reviewing deviations from policy or standards. It prevents an exception from becoming permanent neglect by requiring a risk owner, justification, and a defined review or expiration cycle.
2. Correct Answer: B. Executive Reporting
   Explanation: Executive reporting communicates security posture, risk, and program performance in a way senior leaders can act on. It emphasizes business impact, trends, and decisions rather than raw technical dashboards.
3. Correct Answer: C. Authorization
   Explanation: Authorization is the process of granting an authenticated identity specific permissions such as read, write, or admin access. It differs from authentication, which proves identity rather than defining allowed actions.
4. Correct Answer: D. Legal Hold
   Explanation: A legal hold is a directive to preserve potentially relevant information for litigation, investigation, or regulatory inquiry and it overrides normal deletion. It is used to protect evidence integrity and coordinate with legal before data is purged.
5. Correct Answer: A. Cyber Risk Appetite
   Explanation: Cyber risk appetite is the amount and type of security risk an organization is willing to accept in pursuit of its objectives. It provides the “why” behind control choices, exceptions, and investment decisions in a way leaders can approve and measure.
6. Correct Answer: B. Due Diligence
   Explanation: Due diligence is the investigation and evaluation performed before making a security decision such as selecting a vendor. It is the “show your homework” step that supports defensible choices rather than assumptions or informal trust.
7. Correct Answer: C. Key Risk Indicator (KRI)
   Explanation: A KRI signals increasing or decreasing risk exposure and is used for early warning and trend detection. It supports thresholds and triggers that prompt leadership decisions rather than counting activity.

8. Correct Answer: D. Control Objective
   Explanation: A control objective is the intended security outcome a control is supposed to achieve. Exam questions often test whether you can match the scenario's objective to the best control choice, not the most feature-rich option.

9. Correct Answer: A. Defense in Depth
   Explanation: Defense in depth uses multiple layers of controls so a single failure does not create a full compromise. It is a design principle that supports balanced preventive, detective, and corrective controls.

10. Correct Answer: B. Business Impact Analysis (BIA)
    Explanation: A BIA identifies critical processes, acceptable downtime, and the operational and financial impact of outages. It is a foundational input to continuity strategy and risk decisions and is commonly confused with risk assessment or technical recovery planning.

Bank 2

1. A new policy says certain datasets must be handled with stricter controls, but teams keep arguing about what category the data belongs in and which handling rules apply. The CISO wants a consistent, repeatable way to decide sensitivity and impact so controls can be chosen correctly. What concept best addresses this need?
   A. Encryption
   B. Data Retention
   C. Data Governance
   D. Data Classification

2. A security leader is asked to show that the security program is not just "busy," but is delivering real outcomes leadership can track over time. The leader chooses a small set of measures that reflect whether program activities are achieving intended performance results. What type of metric is being emphasized?
   A. Key Risk Indicator (KRI)
   B. Key Performance Indicator (KPI)
   C. Material Risk
   D. Risk Register

3. A business unit insists it has "secured privacy" because it deployed strong access controls and encryption, but it is still collecting and using personal data in ways that violate permitted-use rules. Which concept is most directly concerned with appropriate collection, use, and sharing based on law and policy?
   A. Data Privacy
   B. Confidentiality
   C. Integrity
   D. Availability

4. An auditor asks for proof that a control is operating as intended, not just that it exists on paper. The team responds with signed approvals, logs, and reports tied to specific dates and owners. What is the best term for this kind of proof?
   A. Audit Management
   B. Control Objective
   C. Audit Evidence
   D. Continuous Monitoring

5. Executives want security risk handled through the same decision process used for financial and operational risk, so security risk is expressed in business terms and

integrated into organization-wide risk oversight. What concept is being applied?
A. Governance
B. Enterprise Risk Management (ERM)
C. Risk Treatment
D. Risk Acceptance

6. A control gap is found during an internal review, and leadership wants a documented set of steps with owners and deadlines to remediate it, prioritize it by risk, and verify closure with evidence. What is the best artifact or process to produce?
A. Risk Register
B. Due Diligence
C. Acceptable Use Policy (AUP)
D. Corrective Action Plan (CAP)

7. A CISO needs to decide whether to avoid, mitigate, transfer, or accept a risk after reviewing likelihood and impact. The emphasis is choosing the most defensible option under business constraints and then tracking that choice. What concept is this?
A. Risk Treatment
B. Risk Assessment
C. Cyber Risk Appetite
D. Accountability

8. The security program has a policy, but leaders suspect the process is still inconsistent and "ad hoc," with outcomes varying by team. The CISO wants a structured way to rate whether the process is defined, repeatable, measured, and improving over time. What concept best fits?
A. Delegation of Authority
B. Change Management
C. Capability Maturity Model
D. Control Selection

9. A critical vulnerability scanning program reports high scan volume, but leadership wants a defensible approach that prioritizes what matters, remediates, and then verifies weaknesses are actually fixed. Which program area best describes that end-to-end cycle?
A. Audit Management
B. Continuous Monitoring

C. Executive Reporting
D. Vulnerability Management

10. A risk decision is being questioned months later, and the CISO needs a structured record that shows the risk, its rating, the owner, the chosen response, and current status. What should the CISO point to?
    A. Metrics and Measurement
    B. Risk Register
    C. Governance
    D. Conflict of Interest

---

1. Correct Answer: D. Data Classification
   Explanation: Data classification categorizes information based on sensitivity and impact so handling rules and controls can be applied consistently. It appears on the exam as the basis for deciding what protections are appropriate for different data.

2. Correct Answer: B. Key Performance Indicator (KPI)
   Explanation: A KPI reflects whether a program activity is achieving its intended performance outcome. It matters because the exam favors measures that drive action and show progress rather than raw technical counts.

3. Correct Answer: A. Data Privacy
   Explanation: Data privacy focuses on appropriate collection, use, and sharing of personal or regulated information based on law and policy. It commonly appears as a decision point where privacy rights and permitted use are distinct from security controls.

4. Correct Answer: C. Audit Evidence
   Explanation: Audit evidence is the documented proof used to judge whether a control exists, is designed well, and operates as intended. The exam often rewards choices that cite verifiable artifacts like approvals, logs, tickets, and reports.

5. Correct Answer: B. Enterprise Risk Management (ERM)
   Explanation: ERM is the organization-wide approach to identifying, assessing, treating, and reporting risk across all functions. On the exam, it matters because security risk should be integrated into the same leadership process used for other business risks.

6. Correct Answer: D. Corrective Action Plan (CAP)
   Explanation: A CAP documents steps, owners, and deadlines to remediate findings

and track closure. It shows governance discipline by prioritizing by risk and validating remediation with evidence.

7. Correct Answer: A. Risk Treatment
   Explanation: Risk treatment is selecting and implementing a response such as avoid, mitigate, transfer, or accept. The exam tests whether the chosen treatment is defensible under constraints and tied to tracking and verification.

8. Correct Answer: C. Capability Maturity Model
   Explanation: A capability maturity model rates how well a process is defined, repeatable, measured, and improving. On the exam, it helps distinguish ad hoc activity from managed, evidence-backed program performance.

9. Correct Answer: D. Vulnerability Management
   Explanation: Vulnerability management is the continuous process of discovering, prioritizing, remediating, and verifying weaknesses. The exam emphasizes risk-based prioritization, remediation evidence, and verification over scan volume.

10. Correct Answer: B. Risk Register
    Explanation: A risk register records identified risks, their ratings, owners, treatments, and current status in a structured way. It matters on the exam because it provides traceability from discovery to decision, action, and reporting.

Bank 3

1. A security director is asked to oversee an internal audit of a program area that they personally designed and are being evaluated on for a bonus. The CISO wants to ensure the review is objective and defensible, not influenced by incentives. Which concept best describes the risk in this situation?
   A. Accountability
   B. Audit Evidence
   C. Conflict of Interest
   D. Executive Reporting

2. A business unit documents a known security risk and argues that treating it right now would cost more than the benefit, and leadership agrees it falls within the organization's stated limits. What is the best term for this decision when it is made formally and documented?
   A. Risk Acceptance
   B. Risk Assessment
   C. Risk Treatment
   D. Cyber Risk Appetite

3. A critical production system experienced an outage after an untracked configuration change, and leadership wants a process that requires request, approval, implementation records, and review so changes are controlled and traceable. What program control process best fits?
   A. Audit Management
   B. Exception Management
   C. Continuous Monitoring
   D. Change Management

4. A CISO asks for an ongoing way to measure whether key controls are performing over time, with defined review frequency and clear actions when thresholds are breached. What practice does this describe?
   A. Executive Reporting
   B. Continuous Monitoring
   C. Audit Evidence
   D. Control Objective

5. An organization keeps having unclear security approvals because no one knows who has the authority to grant exceptions, approve high-risk access, or accept residual risk. The CISO wants formal decision rights with clear limits and

accountability. What concept best addresses this?
A. Governance
B. Accountability
C. Delegation of Authority
D. Due Diligence

6. Phishing incidents are increasing and leaders want a measurable control that improves user behavior, is tailored by role, and produces evidence of effectiveness rather than a one-time email reminder. What program area best fits?
A. Security Awareness and Training
B. Acceptable Use Policy (AUP)
C. Access Control
D. Authentication

7. During an incident, teams argue about who escalates, who communicates, and how evidence is handled. Leadership wants a documented approach that defines detection, analysis, containment, recovery, communications, and continuous improvement through exercises. What artifact best fits?
A. Business Continuity Plan (BCP)
B. Disaster Recovery Plan (DRP)
C. Legal Hold
D. Incident Response Plan (IRP)

8. A regulator asks whether the organization acted with reasonable prudence in protecting information and making risk-based decisions, and the CISO needs to show consistent, documented choices rather than informal judgment. What concept is being evaluated?
A. Due Diligence
B. Due Care
C. Audit Management
D. Risk Register

9. A CISO must choose safeguards that reduce risk to an acceptable level while considering feasibility, cost, and measurable effectiveness. The scenario emphasizes matching safeguards to likelihood and impact rather than picking the most feature-rich tool. What concept is being applied?
A. Control Objective
B. Defense in Depth
C. Control Selection
D. Metrics and Measurement

10. A user has proven their identity successfully, but the system must now grant that user only the permissions appropriate to their role, consistent with least privilege and periodic review. Which concept is responsible for granting those specific permissions?
    A. Authorization
    B. Authentication
    C. Access Control
    D. Accountability

---

1. Correct Answer: C. Conflict of Interest
   Explanation: A conflict of interest exists when personal or organizational incentives could bias oversight, audit conclusions, or security decisions. The exam expects independence and objective reporting, especially when the reviewer benefits from a favorable outcome.
2. Correct Answer: A. Risk Acceptance
   Explanation: Risk acceptance is the formal decision to live with a known risk when it falls within appetite or when treatment costs outweigh benefits. The exam emphasizes documented rationale, a named risk owner, and a defined review cadence.
3. Correct Answer: D. Change Management
   Explanation: Change management controls how changes are requested, approved, implemented, and reviewed to reduce outages and security drift. The exam looks for traceable records, approvals, and rollback or review discipline rather than informal changes.
4. Correct Answer: B. Continuous Monitoring
   Explanation: Continuous monitoring is the ongoing measurement of control performance and risk indicators over time. It appears on the exam as defining what is measured, how often it is reviewed, and what actions follow when thresholds are exceeded.
5. Correct Answer: C. Delegation of Authority
   Explanation: Delegation of authority formally assigns decision-making power to roles with clear limits and accountability. The exam tests whether approvals and risk decisions are made by the right level of leadership and documented in a repeatable way.

6. Correct Answer: A. Security Awareness and Training
   Explanation: Security awareness and training is a measurable program designed to build user understanding and behaviors that reduce human-driven risk. The exam favors role-based depth and evidence of effectiveness over one-time communications.

7. Correct Answer: D. Incident Response Plan (IRP)
   Explanation: An incident response plan defines how the organization detects, analyzes, contains, eradicates, and recovers from incidents, including escalation and communications. The exam emphasizes defined roles, exercises, and improvement rather than improvised coordination.

8. Correct Answer: B. Due Care
   Explanation: Due care is acting with the level of prudence a reasonable organization would use to protect information and manage risk. The exam ties it to consistent, documented, risk-based decisions that can be defended later.

9. Correct Answer: C. Control Selection
   Explanation: Control selection is choosing safeguards that reduce risk to an acceptable level while considering constraints like cost and feasibility. The exam often tests matching controls to likelihood and impact with measurable effectiveness, not picking the flashiest option.

10. Correct Answer: A. Authorization
    Explanation: Authorization grants an authenticated identity specific permissions such as read, write, or admin access. The exam distinguishes it from authentication, which proves identity rather than defining allowed actions.

Bank 4

1. A CISO is building a program dashboard for the board and wants measures that provide early warning when risk exposure is rising, with thresholds that trigger leadership decisions. Which metric type best fits?
   A. Key Performance Indicator (KPI)
   B. Key Risk Indicator (KRI)
   C. Metrics and Measurement
   D. Control Objective

2. During continuity planning, leadership wants to ensure critical business operations can continue during a disruption, not just restore technology systems. Which plan is the best match?
   A. Disaster Recovery Plan (DRP)
   B. Incident Response Plan (IRP)
   C. Business Impact Analysis (BIA)
   D. Business Continuity Plan (BCP)

3. A team proposes deploying encryption for sensitive data, but the CISO points out that leadership still needs rules about who can access what and under which conditions. What control category is the CISO emphasizing?
   A. Access Control
   B. Data Retention
   C. Integrity
   D. Availability

4. An organization has multiple business units defining security requirements differently for the same type of data, creating inconsistency and confusion. The CISO wants clear decision rights, policies, and oversight so data is managed consistently across the enterprise. What concept best fits?
   A. Data Classification
   B. Executive Reporting
   C. Data Governance
   D. Risk Register

5. A risk review identifies a significant risk, and leaders need to decide whether to avoid, mitigate, transfer, or accept it and then track the chosen approach. What process is being performed?
   A. Risk Treatment
   B. Risk Assessment

C. Cyber Risk Appetite
D. Due Care

6. An internal audit finds a control gap, and leadership wants a documented set of remediation steps with owners and deadlines, prioritized by risk, and validated at closure with evidence. What should be created?
   A. Risk Register
   B. Audit Evidence
   C. Change Management
   D. Corrective Action Plan (CAP)

7. A vendor will handle sensitive organizational data, and the CISO wants a lifecycle approach that evaluates the vendor before contract, sets requirements, and monitors compliance over time. What program area best matches?
   A. Data Owner
   B. Third-Party Risk Management (TPRM)
   C. Confidentiality
   D. Security Awareness and Training

8. A leadership team wants to decide which risks matter most by estimating likelihood and impact, rather than jumping straight to buying tools. What activity best fits that step?
   A. Control Selection
   B. Risk Acceptance
   C. Risk Assessment
   D. Enterprise Risk Management (ERM)

9. Investigators need to prove that event records were not altered after an incident, and leadership wants controls that support tamper evidence and trustworthy records. Which security property is most directly involved?
   A. Confidentiality
   B. Availability
   C. Encryption
   D. Integrity

10. A CISO needs a record that shows each identified risk, its rating, the named owner, the chosen response, and current status so decisions can be defended later. What artifact is most appropriate?
    A. Audit Management
    B. Risk Register

C. Acceptable Use Policy (AUP)
D. Delegation of Authority

---

1. Correct Answer: B. Key Risk Indicator (KRI)
   Explanation: A KRI signals increasing or decreasing risk exposure and is used for early warning and trend detection. It supports thresholds and triggers that prompt leadership decisions rather than measuring activity volume.
2. Correct Answer: D. Business Continuity Plan (BCP)
   Explanation: A BCP focuses on sustaining critical business operations during and after disruption. It is distinct from disaster recovery, which centers on restoring technology services.
3. Correct Answer: A. Access Control
   Explanation: Access control determines who can access systems, data, and functions and under what conditions. It commonly appears as a governance decision about selecting appropriate controls and proving they work through reviews and role definitions.
4. Correct Answer: C. Data Governance
   Explanation: Data governance sets decision rights, policies, and oversight to ensure data is managed consistently across the organization. It often appears when accountability is unclear and consistent standards and reporting are needed.
5. Correct Answer: A. Risk Treatment
   Explanation: Risk treatment is selecting and implementing a response such as avoid, mitigate, transfer, or accept. The exam emphasizes choosing a defensible option under business constraints and tracking that decision.
6. Correct Answer: D. Corrective Action Plan (CAP)
   Explanation: A CAP is a documented set of steps, owners, and deadlines to remediate findings and track progress. It supports governance by prioritizing by risk and validating closure with evidence.
7. Correct Answer: B. Third-Party Risk Management (TPRM)
   Explanation: TPRM evaluates, contracts, monitors, and responds to risks introduced by vendors and service providers. It is tested as governance across the supplier lifecycle, not a one-time review.
8. Correct Answer: C. Risk Assessment
   Explanation: Risk assessment identifies threats, vulnerabilities, likelihood, and

impact to determine risk level and treatment options. It is often the expected first step before selecting controls or tools.

9. Correct Answer: D. Integrity
   Explanation: Integrity means information remains accurate, complete, and protected from unauthorized modification or destruction. It appears in scenarios about tamper evidence, trustworthy logs, and controlled change.

10. Correct Answer: B. Risk Register
    Explanation: A risk register records identified risks, their ratings, owners, treatments, and current status in a structured way. It provides traceability from discovery to decision, action, and reporting.

Bank 5

1. A CISO is asked to approve new security spending, but leadership wants to see that the choices align to the organization's stated tolerance for cyber risk and are expressed in business terms that can be approved and measured. What concept should anchor the justification?
   A. Cyber Risk Appetite
   B. Risk Assessment
   C. Control Objective
   D. Audit Management

2. During an incident investigation, responders want to preserve potentially relevant data and stop normal deletion routines while legal and compliance teams evaluate next steps. What action best fits this requirement?
   A. Update the Data Retention schedule
   B. Issue a Legal Hold
   C. Activate the Business Continuity Plan (BCP)
   D. Start the Business Impact Analysis (BIA)

3. A program review finds that a security process is defined in writing, executed consistently, measured, and shows evidence of ongoing improvement over time. Which concept is most directly used to describe that progression?
   A. Delegation of Authority
   B. Capability Maturity Model
   C. Defense in Depth
   D. Control Selection

4. A security manager proves identity using strong methods, but a later control failure allows that same user to access functions outside their job role. Which control area most directly failed?
   A. Authentication
   B. Encryption
   C. Authorization
   D. Confidentiality

5. Leaders want a structured record that ties each risk to a named owner, shows the chosen response, and tracks status so decisions can be reviewed and defended later. Which artifact best meets this need?
   A. Risk Register
   B. Corrective Action Plan (CAP)

C. Executive Reporting
D. Metrics and Measurement

6. An executive team demands a concise view of security posture that highlights business impact and trends, not raw technical dashboards. Which practice is being requested?
   A. Continuous Monitoring
   B. Executive Reporting
   C. Audit Evidence
   D. Access Control

7. A security policy allows deviations, but leadership wants every deviation to have a documented justification, a risk owner who accepts it, compensating controls if needed, and a clear expiration or review date. Which program process best fits?
   A. Risk Treatment
   B. Exception Management
   C. Change Management
   D. Audit Management

8. A team claims it is “compliant” because it runs vulnerability scans weekly, but leadership wants proof that weaknesses are prioritized by risk, fixed, and verified as remediated. Which program area best describes the complete lifecycle?
   A. Vulnerability Management
   B. Continuous Monitoring
   C. Audit Management
   D. Control Objective

9. A privacy office challenges a business unit that is collecting and using personal data in ways that violate permitted-use rules, even though the unit deployed strong security controls. Which concept is most directly at issue?
   A. Confidentiality
   B. Integrity
   C. Data Privacy
   D. Availability

10. An auditor asks for proof that a control is operating as intended, and the team provides signed approvals, logs, tickets, and reports tied to specific dates and owners. What is the best term for these artifacts?
    A. Control Objective
    B. Audit Evidence

C. Governance
D. Due Care

---

1. Correct Answer: A. Cyber Risk Appetite
   Explanation: Cyber risk appetite is the amount and type of security risk an organization is willing to accept in pursuit of its objectives. It provides the rationale leaders use to approve and measure control choices, exceptions, and investments.

2. Correct Answer: B. Issue a Legal Hold
   Explanation: A legal hold is a directive to preserve potentially relevant information for litigation, investigation, or regulatory inquiry and it overrides normal deletion. It protects evidence integrity and coordinates preservation while legal review proceeds.

3. Correct Answer: B. Capability Maturity Model
   Explanation: A capability maturity model rates how well a process is defined, repeatable, measured, and improving over time. It is used to distinguish ad hoc activity from managed, evidence-backed program performance.

4. Correct Answer: C. Authorization
   Explanation: Authorization grants an authenticated identity specific permissions appropriate to role and least privilege. It differs from authentication, which proves identity rather than controlling what actions are allowed.

5. Correct Answer: A. Risk Register
   Explanation: A risk register records identified risks, their ratings, owners, treatments, and current status in a structured way. It provides traceability from discovery to decision, action, and reporting.

6. Correct Answer: B. Executive Reporting
   Explanation: Executive reporting communicates security posture, risk, and program performance in a way senior leaders can act on. It emphasizes business impact, trends, and decisions rather than raw technical details.

7. Correct Answer: B. Exception Management
   Explanation: Exception management governs deviations from policy through documentation, time-bounding, and review. It prevents exceptions from becoming permanent neglect by requiring a risk owner, justification, and defined expiration or review cycle.

8. Correct Answer: A. Vulnerability Management
   Explanation: Vulnerability management is the continuous process of discovering, prioritizing, remediating, and verifying weaknesses. The exam emphasizes risk-based prioritization and remediation evidence over scan volume alone.

9. Correct Answer: C. Data Privacy
   Explanation: Data privacy concerns appropriate collection, use, and sharing of personal or regulated information based on law and policy. It is distinct from security controls, which protect data but do not automatically make use permissible.

10. Correct Answer: B. Audit Evidence
    Explanation: Audit evidence is the documented proof used to judge whether a control exists, is designed well, and operates as intended. The exam rewards selecting verifiable artifacts such as approvals, logs, tickets, and reports over informal statements.