CRISC 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 risk manager is asked to justify why a new control initiative should be prioritized this quarter. Which governance input best anchors the justification to what the organization is trying to accomplish?
   A. Organizational Strategy, Goals, and Objectives
   B. Organizational Culture
   C. Policies and Standards
   D. Business Processes

2. During a review, multiple teams claim that “someone else” is accountable for approving a key governance decision. Which objective area is most directly implicated by this confusion?
   A. Organizational Strategy, Goals, and Objectives
   B. Organizational Structure, Roles and Responsibilities
   C. Business Processes
   D. Organizational Assets

3. A policy exists, but teams routinely bypass it because “speed matters more,” and leaders rarely reinforce expected behavior. Which objective area best matches the root issue?
   A. Policies and Standards
   B. Organizational Structure, Roles and Responsibilities
   C. Organizational Culture
   D. Organizational Assets

4. A new governance requirement is drafted, but different departments implement it in inconsistent ways because no common internal benchmark exists for “what good looks like.” Which objective area should be strengthened first?
   A. Organizational Strategy, Goals, and Objectives
   B. Business Processes
   C. Organizational Culture
   D. Policies and Standards

5. An executive asks for a governance summary that shows how day-to-day work supports the organization’s long-term direction. Which objective area most directly provides that long-term direction?
   A. Organizational Strategy, Goals, and Objectives
   B. Business Processes

C. Organizational Assets
D. Organizational Structure, Roles and Responsibilities

6. A governance review finds that work is getting done, but it is unclear who is expected to do what, when handoffs occur, and who makes final decisions. Which objective area best addresses the need to clarify decision-making and accountability?
A. Organizational Culture
B. Organizational Structure, Roles and Responsibilities
C. Policies and Standards
D. Organizational Assets

7. A governance team notices that two groups perform the same activity in different ways, producing inconsistent results and confusion across handoffs. Which objective area most directly focuses on defining and stabilizing how work is performed?
A. Organizational Culture
B. Organizational Structure, Roles and Responsibilities
C. Business Processes
D. Organizational Strategy, Goals, and Objectives

8. A governance initiative depends on knowing what the organization has, where it is used, and what it supports, but stakeholders cannot clearly describe what resources exist. Which objective area is most directly missing?
A. Policies and Standards
B. Organizational Culture
C. Business Processes
D. Organizational Assets

9. A policy update is proposed that would add effort to several teams. Which governance check best ensures the policy supports what the organization is trying to achieve, rather than creating work for its own sake?
A. Organizational Strategy, Goals, and Objectives
B. Organizational Assets
C. Organizational Culture
D. Organizational Structure, Roles and Responsibilities

10. A new standard is published internally, but teams interpret it differently because it does not translate into consistent day-to-day steps and handoffs. Which objective area most directly needs attention to make execution consistent?
A. Organizational Assets

B. Organizational Culture
C. Organizational Structure, Roles and Responsibilities
D. Business Processes

---

1. Correct Answer: A. Organizational Strategy, Goals, and Objectives
   Explanation: This objective area defines what the organization is trying to accomplish and provides the most direct anchor for prioritization. It is the clearest basis for explaining why a governance initiative matters in terms of direction and outcomes.

2. Correct Answer: B. Organizational Structure, Roles and Responsibilities
   Explanation: Confusion about who approves and who is accountable points directly to roles and responsibilities not being defined or understood. This objective area focuses on clarifying structure and ownership so decisions are assigned and executed.

3. Correct Answer: C. Organizational Culture
   Explanation: Bypassing a policy because of shared norms and leadership behavior reflects culture, not simply the existence of written rules. This objective area covers the expectations and behaviors that determine whether governance is followed in practice.

4. Correct Answer: D. Policies and Standards
   Explanation: Inconsistent implementation across departments indicates a lack of common policies and standards to guide what "consistent" means. Strengthening this area creates shared definitions and expectations for how governance requirements should be applied.

5. Correct Answer: A. Organizational Strategy, Goals, and Objectives
   Explanation: Strategy, goals, and objectives express the organization's long-term direction and desired outcomes. This objective area is what day-to-day governance should connect back to for coherence and purpose.

6. Correct Answer: B. Organizational Structure, Roles and Responsibilities
   Explanation: The scenario describes unclear decision rights, ownership, and accountability, which is a roles-and-responsibilities problem. This objective area is the primary place to clarify who does what and who decides.

7. Correct Answer: C. Business Processes
   Explanation: Different groups performing the same activity in inconsistent ways

indicates the underlying process is not defined or consistently followed. This objective area focuses on how work flows, including handoffs and repeatable execution.

8. Correct Answer: D. Organizational Assets
   Explanation: Not knowing what resources exist and what they support is a direct gap in understanding organizational assets. This objective area addresses identifying and managing the assets the organization relies on.

9. Correct Answer: A. Organizational Strategy, Goals, and Objectives
   Explanation: Checking alignment to strategy, goals, and objectives ensures governance artifacts like policies support the organization's intended direction. This avoids changes that add effort without supporting organizational outcomes.

10. Correct Answer: D. Business Processes
    Explanation: A standard that does not translate into consistent execution indicates the process layer is not defined clearly enough for repeatable day-to-day work. This objective area addresses the operationalization of expectations through consistent steps and handoffs.

Bank 2

1. An organization has multiple teams assessing risk in different ways, producing conflicting conclusions for the same initiative. Which governance concept best addresses the need for a consistent approach across the organization?
   A. Three Lines of Defense
   B. Enterprise Risk Management and Risk Management Framework
   C. Risk Profile
   D. Organizational Culture

2. A risk manager is asked to explain how risk decisions in one business unit will be made comparable to risk decisions in another unit. Which concept most directly provides the structure for consistent risk decision-making?
   A. Enterprise Risk Management and Risk Management Framework
   B. Risk Profile
   C. Policies and Standards
   D. Organizational Assets

3. Senior leadership wants a consolidated view of the organization's key risks to support prioritization and oversight. Which concept best fits this request?
   A. Business Processes
   B. Risk Profile
   C. Three Lines of Defense
   D. Organizational Structure, Roles and Responsibilities

4. In a risk governance discussion, management is unsure which group should own day-to-day controls versus which group should provide oversight and challenge. Which concept most directly clarifies these responsibilities?
   A. Three Lines of Defense
   B. Risk Profile
   C. Enterprise Risk Management and Risk Management Framework
   D. Policies and Standards

5. A new risk program is being launched, and the first priority is to define common terminology, assessment steps, and how risk information will be documented and escalated. Which concept best describes what is being established?
   A. Risk Profile
   B. Organizational Strategy, Goals, and Objectives
   C. Enterprise Risk Management and Risk Management Framework
   D. Organizational Assets

6. A risk manager is asked to brief executives on “the big picture” of risk exposure and how it is evolving, without diving into individual control details. Which concept best supports that type of briefing?
   A. Risk Profile
   B. Three Lines of Defense
   C. Business Impact Analysis
   D. Control Objective

7. During an internal review, the team notices that oversight activities are being performed by the same group responsible for operating the controls, reducing independence. Which governance concept is most relevant to this issue?
   A. Enterprise Risk Management and Risk Management Framework
   B. Three Lines of Defense
   C. Risk Profile
   D. Policies and Standards

8. Two departments argue about whether a risk should be treated as a top organizational concern, but they lack an agreed summary of priority risks and their characteristics. Which concept is most directly missing?
   A. Risk Profile
   B. Enterprise Risk Management and Risk Management Framework
   C. Organizational Assets
   D. Business Processes

9. A risk manager is designing reporting so risk information can roll up from teams to leadership in a consistent, comparable way. Which concept most directly guides how that reporting should be structured?
   A. Risk Profile
   B. Organizational Culture
   C. Enterprise Risk Management and Risk Management Framework
   D. Business Processes

10. Management asks for clarity on how risk responsibilities should be separated so that execution, oversight, and independent challenge are not blended together. Which concept best answers this need?
    A. Risk Profile
    B. Enterprise Risk Management and Risk Management Framework
    C. Three Lines of Defense
    D. Policies and Standards

1. Correct Answer: B. Enterprise Risk Management and Risk Management Framework
   Explanation: This concept provides a consistent organization-wide approach for how risk is identified, assessed, documented, and managed. It is the best fit when different teams need a shared structure to produce comparable outcomes.

2. Correct Answer: A. Enterprise Risk Management and Risk Management Framework
   Explanation: A risk management framework establishes common methods and structure so risk decisions can be made consistently across units. It directly supports comparability by standardizing how risk information is evaluated and communicated.

3. Correct Answer: B. Risk Profile
   Explanation: A risk profile is used to present a consolidated view of key risks for oversight and prioritization. It aligns with leadership's need to understand major exposures without focusing on individual operational details.

4. Correct Answer: A. Three Lines of Defense
   Explanation: The Three Lines of Defense model clarifies responsibilities between those who manage and execute controls and those who provide oversight and challenge. It is designed to prevent confusion about who does day-to-day work versus who provides governance.

5. Correct Answer: C. Enterprise Risk Management and Risk Management Framework
   Explanation: Establishing common terminology, assessment steps, and escalation paths is the core purpose of a risk management framework. It sets the structure for how risk work is performed consistently across the organization.

6. Correct Answer: A. Risk Profile
   Explanation: A risk profile supports executive-level understanding of overall risk exposure and trends. It is suited for communicating the big-picture risk landscape without requiring deep control-level detail.

7. Correct Answer: B. Three Lines of Defense
   Explanation: This model relies on separation between those operating controls and those overseeing or challenging them to maintain independence. When the same group performs both, the issue is directly tied to Three Lines of Defense responsibilities.

8. Correct Answer: A. Risk Profile
   Explanation: The scenario describes the absence of an agreed summary of priority

risks and their characteristics at the organizational level. A risk profile fills that gap by consolidating and describing key risks for decision-making.

9. Correct Answer: C. Enterprise Risk Management and Risk Management Framework
   Explanation: A risk management framework guides how risk information should be documented, escalated, and reported so it can roll up consistently. It is the best match for designing reporting that is comparable across groups.

10. Correct Answer: C. Three Lines of Defense
    Explanation: The concept is specifically used to separate execution, oversight, and independent challenge to avoid blurred responsibilities. It directly addresses management's concern about mixing roles across lines of defense.

Bank 3

1. Leadership wants a clear statement that guides how much risk the organization is willing to take on to pursue its objectives, before teams propose specific controls or treatment plans. Which risk governance element best fits this need?
   A. Risk Profile
   B. Enterprise Risk Management and Risk Management Framework
   C. Risk Appetite and Risk Tolerance
   D. Policies and Standards

2. A risk response option looks cost-effective, but it would put the organization out of alignment with a mandatory obligation tied to how services are delivered. Which governance element is the primary constraint that must be addressed first?
   A. Professional Ethics of Risk Management
   B. Legal, Regulatory and Contractual Requirements
   C. Risk Appetite and Risk Tolerance
   D. Three Lines of Defense

3. A team proposes accepting a risk because "the odds feel low," but leadership has already set clear boundaries for what is acceptable. Which governance element should be used to evaluate whether acceptance is permitted?
   A. Risk Appetite and Risk Tolerance
   B. Risk Profile
   C. Organizational Culture
   D. Risk Management Framework

4. A risk manager is pressured to downplay a material risk in an executive summary to avoid delaying a high-visibility initiative. Which governance element is most directly tested by this pressure?
   A. Risk Appetite and Risk Tolerance
   B. Legal, Regulatory and Contractual Requirements
   C. Risk Profile
   D. Professional Ethics of Risk Management

5. Two business units disagree about whether the same risk is "acceptable," and the disagreement is driven by inconsistent thresholds and unclear boundaries for escalation. Which governance element most directly resolves this inconsistency?
   A. Three Lines of Defense
   B. Risk Profile

C. Risk Appetite and Risk Tolerance
D. Organizational Structure, Roles and Responsibilities

6. A vendor contract requires specific handling expectations, and the risk team must ensure risk decisions and responses do not conflict with those commitments. Which governance element is most relevant?
   A. Policies and Standards
   B. Legal, Regulatory and Contractual Requirements
   C. Risk Appetite and Risk Tolerance
   D. Organizational Culture

7. A risk manager discovers that an analysis was selectively summarized to favor a preferred outcome, even though the underlying risk scenario is unchanged. Which governance element is most directly implicated?
   A. Risk Profile
   B. Enterprise Risk Management and Risk Management Framework
   C. Legal, Regulatory and Contractual Requirements
   D. Professional Ethics of Risk Management

8. A risk assessment proposes treating a risk, but leadership asks for a clear statement of the boundary between “acceptable variation” and “unacceptable exposure” so approvals can be consistent. Which governance element best answers that request?
   A. Risk Appetite and Risk Tolerance
   B. Business Processes
   C. Risk Profile
   D. Three Lines of Defense

9. A risk treatment plan is ready for approval, but the organization must confirm that the plan aligns with externally imposed obligations before proceeding. Which governance element drives that confirmation?
   A. Professional Ethics of Risk Management
   B. Legal, Regulatory and Contractual Requirements
   C. Risk Appetite and Risk Tolerance
   D. Risk Profile

10. A risk manager is preparing a briefing and must ensure the communication reflects truthful, unbiased risk information rather than personal preference or organizational pressure. Which governance element most directly guides this expectation?
    A. Risk Profile

B. Policies and Standards
C. Professional Ethics of Risk Management
D. Three Lines of Defense

---

1. Correct Answer: C. Risk Appetite and Risk Tolerance
   Explanation: This element defines the organization’s boundaries for how much risk it is willing to accept in pursuit of objectives. It is used before selecting responses so decisions are anchored to agreed limits rather than individual opinions.

2. Correct Answer: B. Legal, Regulatory and Contractual Requirements
   Explanation: Mandatory obligations act as constraints that can limit or prohibit certain risk responses even if they appear efficient. The decision must address these requirements first because nonalignment is not treated as an optional tradeoff.

3. Correct Answer: A. Risk Appetite and Risk Tolerance
   Explanation: This element provides the criteria for deciding whether a risk can be accepted within defined boundaries. It prevents acceptance decisions from being based on informal judgments or inconsistent thresholds.

4. Correct Answer: D. Professional Ethics of Risk Management
   Explanation: Ethical expectations apply when a risk professional is pressured to misrepresent, minimize, or distort risk information. The scenario tests whether the risk manager maintains integrity in reporting despite business pressure.

5. Correct Answer: C. Risk Appetite and Risk Tolerance
   Explanation: Appetite and tolerance establish consistent thresholds and escalation boundaries that different units can apply to similar risks. This reduces disputes caused by inconsistent interpretations of what “acceptable” means.

6. Correct Answer: B. Legal, Regulatory and Contractual Requirements
   Explanation: Contractual obligations are explicitly included in this governance element and must be considered in risk decisions and responses. The scenario centers on ensuring commitments in contracts are not violated by risk treatment choices.

7. Correct Answer: D. Professional Ethics of Risk Management
   Explanation: Selectively summarizing analysis to favor an outcome is an integrity issue in risk communication and decision support. Professional ethics addresses the expectation to present risk information accurately and fairly.

8. Correct Answer: A. Risk Appetite and Risk Tolerance
   Explanation: The request is for clear boundaries that define acceptable versus unacceptable exposure, which is exactly what appetite and tolerance provide. Using these boundaries supports consistent approvals and escalation decisions.

9. Correct Answer: B. Legal, Regulatory and Contractual Requirements
   Explanation: The question is about confirming alignment to externally imposed obligations before approving a treatment plan. This governance element directly covers legal, regulatory, and contractual constraints that must be satisfied.

10. Correct Answer: C. Professional Ethics of Risk Management
    Explanation: Ethical expectations require risk information to be communicated honestly and without bias or improper influence. The scenario tests maintaining professional integrity in reporting and briefing stakeholders.

Bank 4

1. A risk manager reviews an outage that occurred after a series of small configuration changes. To document the situation in a way that clearly links what led to the incident and what was lost, which IT risk identification concept should be used?
   A. Risk Events (e.g., contributing conditions, loss result)
   B. Threat Modelling and Threat Landscape
   C. Vulnerability and Control Deficiency Analysis (e.g., root cause analysis)
   D. Risk Scenario Development

2. A team is expanding a service and wants to anticipate how the external environment could affect exposure before selecting controls. Which IT risk identification concept best fits scanning likely threat paths and the broader context of threats?
   A. Risk Scenario Development
   B. Threat Modelling and Threat Landscape
   C. Risk Events (e.g., contributing conditions, loss result)
   D. Vulnerability and Control Deficiency Analysis (e.g., root cause analysis)

3. After repeated access issues, a risk manager is asked to determine whether the underlying problem is a weakness in existing controls and why it keeps recurring. Which IT risk identification concept is the best match?
   A. Threat Modelling and Threat Landscape
   B. Risk Scenario Development
   C. Vulnerability and Control Deficiency Analysis (e.g., root cause analysis)
   D. Risk Events (e.g., contributing conditions, loss result)

4. A risk manager has separate notes about a threat, a weakness, and a possible business impact, but leadership needs them combined into a clear, testable story that can be assessed. Which IT risk identification concept should be used to assemble this?
   A. Risk Events (e.g., contributing conditions, loss result)
   B. Threat Modelling and Threat Landscape
   C. Vulnerability and Control Deficiency Analysis (e.g., root cause analysis)
   D. Risk Scenario Development

5. A risk manager is asked to describe how likely threats could realistically interact with the organization’s environment, rather than listing generic threats. Which IT risk identification concept best supports this approach?
   A. Risk Events (e.g., contributing conditions, loss result)
   B. Threat Modelling and Threat Landscape

C. Risk Scenario Development
D. Vulnerability and Control Deficiency Analysis (e.g., root cause analysis)

6. During a lessons-learned review, stakeholders want a concise statement of what happened, what conditions contributed to it, and what the outcome was in terms of loss. Which IT risk identification concept best matches that request?
A. Risk Events (e.g., contributing conditions, loss result)
B. Risk Scenario Development
C. Vulnerability and Control Deficiency Analysis (e.g., root cause analysis)
D. Threat Modelling and Threat Landscape

7. An assessment shows a control exists, but it is not working as intended, and the organization needs to identify why the gap exists and what weakness it represents. Which IT risk identification concept is most appropriate?
A. Risk Events (e.g., contributing conditions, loss result)
B. Threat Modelling and Threat Landscape
C. Vulnerability and Control Deficiency Analysis (e.g., root cause analysis)
D. Risk Scenario Development

8. A risk manager needs to produce a set of consistent, comparable risk statements that can be evaluated and prioritized across multiple teams. Which IT risk identification concept best enables that outcome?
A. Threat Modelling and Threat Landscape
B. Vulnerability and Control Deficiency Analysis (e.g., root cause analysis)
C. Risk Events (e.g., contributing conditions, loss result)
D. Risk Scenario Development

9. A manager asks, “What exactly was the loss result, and what conditions made it possible?” before deciding whether the situation should be escalated. Which IT risk identification concept directly answers this question?
A. Risk Events (e.g., contributing conditions, loss result)
B. Vulnerability and Control Deficiency Analysis (e.g., root cause analysis)
C. Threat Modelling and Threat Landscape
D. Risk Scenario Development

10. A risk manager is preparing IT risk identification work and starts by examining how threats are changing and what forms of attack or pressure are most relevant to the environment. Which concept best fits this starting point?
A. Risk Scenario Development
B. Threat Modelling and Threat Landscape

C. Risk Events (e.g., contributing conditions, loss result)
D. Vulnerability and Control Deficiency Analysis (e.g., root cause analysis)

---

1. Correct Answer: A. Risk Events (e.g., contributing conditions, loss result)
   Explanation: This focuses on describing what happened by linking contributing conditions to the loss result. The other options focus on broader threat context, control weaknesses, or building a full scenario statement.
2. Correct Answer: B. Threat Modelling and Threat Landscape
   Explanation: This concept centers on understanding threats and how they could apply to the organization's environment. The other options emphasize documenting an event, analyzing control deficiencies, or packaging details into a scenario.
3. Correct Answer: C. Vulnerability and Control Deficiency Analysis (e.g., root cause analysis)
   Explanation: This concept targets identifying weaknesses and why controls fail or problems recur, including root cause analysis. The other options are oriented toward threat context, event description, or scenario narrative.
4. Correct Answer: D. Risk Scenario Development
   Explanation: This concept is used to combine threat, vulnerability or control gap, and potential impact into a clear risk scenario. The other options focus on event documentation, threat context, or analyzing control deficiencies rather than forming the scenario statement.
5. Correct Answer: B. Threat Modelling and Threat Landscape
   Explanation: This concept supports describing realistic threat interactions rather than generic lists. The other options concentrate on documenting an event, analyzing weaknesses, or assembling a scenario after inputs are identified.
6. Correct Answer: A. Risk Events (e.g., contributing conditions, loss result)
   Explanation: This concept directly captures what occurred, what contributed, and what loss resulted. The other options are about threat context, diagnosing weaknesses, or turning elements into a scenario for assessment.
7. Correct Answer: C. Vulnerability and Control Deficiency Analysis (e.g., root cause analysis)
   Explanation: This concept fits when a control exists but is deficient and the organization needs to understand the weakness and why it occurs. The other

options focus on event outcomes, threat context, or scenario packaging rather than deficiency analysis.

8. Correct Answer: D. Risk Scenario Development
   Explanation: This concept creates standardized risk statements that can be compared, assessed, and prioritized across teams. The other options describe events, analyze weaknesses, or examine threat context without producing the final scenario form.

9. Correct Answer: A. Risk Events (e.g., contributing conditions, loss result)
   Explanation: This concept is explicitly about identifying contributing conditions and the loss result tied to an event. The other options focus on threat context, diagnosing deficiencies, or developing a broader scenario statement.

10. Correct Answer: B. Threat Modelling and Threat Landscape
    Explanation: This concept begins with understanding the evolving threat environment and how threats apply. The other options focus on event documentation, deficiency analysis, or scenario development once threat and weakness inputs are available.

Bank 5

1. A risk manager is asked to ensure that risk evaluations are performed consistently across departments and are comparable over time. Which IT risk analysis and evaluation element best supports this consistency?
   A. Risk Assessment Concepts, Standards and Frameworks
   B. Risk Register
   C. Business Impact Analysis
   D. Inherent and Residual Risk

2. A risk manager needs a centralized place to document identified risks, track their status, and maintain continuity as assessments are updated. Which element is the best fit?
   A. Risk Analysis Methodologies
   B. Risk Register
   C. Business Impact Analysis
   D. Risk Assessment Concepts, Standards and Frameworks

3. Two analysts review the same risk scenario and produce different likelihood and impact conclusions because they used different approaches. Which element most directly addresses choosing how analysis is performed?
   A. Risk Analysis Methodologies
   B. Risk Register
   C. Inherent and Residual Risk
   D. Business Impact Analysis

4. A risk manager is preparing an evaluation and needs to explain the potential business consequences if a process is disrupted, including what the disruption would mean to operations. Which element is most directly used?
   A. Risk Assessment Concepts, Standards and Frameworks
   B. Risk Register
   C. Business Impact Analysis
   D. Risk Analysis Methodologies

5. A leader asks, “What is the risk level before any controls are considered, and what remains after our current controls?” Which element best matches this question?
   A. Risk Register
   B. Business Impact Analysis
   C. Risk Analysis Methodologies
   D. Inherent and Residual Risk

6. A risk team wants to improve consistency by aligning their terminology, documentation expectations, and evaluation approach to recognized structures rather than informal local practices. Which element best supports that goal?
   A. Risk Assessment Concepts, Standards and Frameworks
   B. Risk Register
   C. Risk Analysis Methodologies
   D. Inherent and Residual Risk

7. A risk manager is asked to ensure that identified risks are not lost during staffing changes and that stakeholders can review decisions and updates over time. Which element best supports this continuity?
   A. Risk Register
   B. Risk Analysis Methodologies
   C. Inherent and Residual Risk
   D. Business Impact Analysis

8. A risk manager must select an approach for analyzing risk scenarios so results are repeatable and comparable across multiple assessments. Which element most directly covers that selection?
   A. Business Impact Analysis
   B. Risk Analysis Methodologies
   C. Risk Register
   D. Risk Assessment Concepts, Standards and Frameworks

9. A risk manager is evaluating a scenario and needs to separate the baseline exposure from the exposure that remains after existing controls and responses are applied. Which element is being applied?
   A. Risk Assessment Concepts, Standards and Frameworks
   B. Inherent and Residual Risk
   C. Business Impact Analysis
   D. Risk Register

10. During a review, leadership asks for a concise statement of the highest-impact consequences of a disruption to a critical business process to inform prioritization. Which element best provides that analysis?
    A. Risk Register
    B. Risk Analysis Methodologies
    C. Business Impact Analysis
    D. Inherent and Residual Risk

1. Correct Answer: A. Risk Assessment Concepts, Standards and Frameworks
   Explanation: Concepts, standards, and frameworks provide shared structure and terminology so assessments are consistent and comparable. They reduce variation across departments by defining how risk work should be performed and documented.

2. Correct Answer: B. Risk Register
   Explanation: A risk register is used to document risks and track their status over time in a centralized record. It supports continuity by preserving risk statements, decisions, and updates as assessments change.

3. Correct Answer: A. Risk Analysis Methodologies
   Explanation: Methodologies define the approach used to analyze risk scenarios, which directly affects how likelihood and impact are determined. Choosing and applying a methodology reduces inconsistent results caused by ad hoc approaches.

4. Correct Answer: C. Business Impact Analysis
   Explanation: Business impact analysis is specifically used to understand the consequences of disruption to business processes and operations. It supports impact estimation by focusing on what disruption would mean to the organization.

5. Correct Answer: D. Inherent and Residual Risk
   Explanation: Inherent risk is the level of risk before controls are applied, while residual risk is what remains after controls and responses. The question explicitly asks for both perspectives, making this the best fit.

6. Correct Answer: A. Risk Assessment Concepts, Standards and Frameworks
   Explanation: Standards and frameworks provide consistent definitions and expectations for how risk is assessed and reported. Using them reduces reliance on informal local practices and improves comparability.

7. Correct Answer: A. Risk Register
   Explanation: A risk register preserves identified risks and their status so they are not lost during staffing or organizational changes. It allows stakeholders to review past decisions and updates over time.

8. Correct Answer: B. Risk Analysis Methodologies
   Explanation: Methodologies determine how analysis is performed so results are repeatable across assessments. This directly supports comparability by using a consistent analytical approach.

9. Correct Answer: B. Inherent and Residual Risk
   Explanation: The task described is distinguishing baseline exposure from remaining exposure after controls are applied. That distinction is exactly what inherent and residual risk represent.

10. Correct Answer: C. Business Impact Analysis
    Explanation: Business impact analysis identifies and summarizes consequences of disruption to critical processes. It directly supports prioritization by clarifying the most significant operational impacts.

Bank 6

1. A risk manager presents several ways to address a documented risk scenario, and leadership must select the most appropriate path forward. Which element is most directly being applied?
   A. Risk Treatment / Risk Response Options
   B. Risk and Control Ownership
   C. Issue, Finding and Exception Management
   D. Third-Party Risk Management

2. A risk response is approved, but execution stalls because no one is clearly accountable for making sure the response is carried out. Which element is most directly missing?
   A. Management of Emerging Risk
   B. Risk and Control Ownership
   C. Risk Treatment / Risk Response Options
   D. Third-Party Risk Management

3. A critical service is provided by an external vendor, and risk decisions must include how that relationship affects exposure and controls. Which element best fits this situation?
   A. Risk Treatment / Risk Response Options
   B. Issue, Finding and Exception Management
   C. Third-Party Risk Management
   D. Risk and Control Ownership

4. An assessment identifies a control weakness, and the organization must track it, assign responsibility, and ensure it is resolved or formally handled. Which element best matches this need?
   A. Issue, Finding and Exception Management
   B. Risk and Control Ownership
   C. Management of Emerging Risk
   D. Risk Treatment / Risk Response Options

5. A previously stable environment changes quickly, creating new exposures that were not captured in earlier assessments. Which element most directly focuses on this problem?
   A. Risk and Control Ownership
   B. Third-Party Risk Management

C. Management of Emerging Risk
D. Issue, Finding and Exception Management

6. Leadership agrees that a risk must be addressed but asks, “Who owns the risk decision and who owns the controls that reduce it?” Which element best answers this question?
A. Risk Treatment / Risk Response Options
B. Risk and Control Ownership
C. Issue, Finding and Exception Management
D. Management of Emerging Risk

7. A vendor introduces changes that increase exposure, and the organization needs a structured approach to evaluate and respond to risk created outside its direct control. Which element best fits?
A. Management of Emerging Risk
B. Risk Treatment / Risk Response Options
C. Third-Party Risk Management
D. Issue, Finding and Exception Management

8. A risk manager must ensure that exceptions to established expectations are tracked, time-bounded, and not treated as invisible “one-off” decisions. Which element is most directly involved?
A. Risk and Control Ownership
B. Issue, Finding and Exception Management
C. Risk Treatment / Risk Response Options
D. Management of Emerging Risk

9. A team wants to ensure risk responses remain valid as new threats and technology shifts occur, rather than relying only on last year’s assumptions. Which element best supports this goal?
A. Management of Emerging Risk
B. Risk Treatment / Risk Response Options
C. Risk and Control Ownership
D. Third-Party Risk Management

10. A risk manager develops a plan to document the chosen response, confirm responsible parties, and ensure follow-through is visible to leadership. Which single element most directly describes the core focus on selecting and executing an appropriate response?
A. Third-Party Risk Management

B. Risk and Control Ownership
C. Issue, Finding and Exception Management
D. Risk Treatment / Risk Response Options

---

1. Correct Answer: A. Risk Treatment / Risk Response Options
   Explanation: This element focuses on identifying and selecting among available ways to address a risk scenario. The scenario is about presenting options and choosing the most appropriate response.
2. Correct Answer: B. Risk and Control Ownership
   Explanation: Risk and control ownership ensures accountability for risk decisions and for controls that mitigate risk. Without clear ownership, approved responses often fail to be executed.
3. Correct Answer: C. Third-Party Risk Management
   Explanation: This element addresses risks introduced or influenced by external parties such as vendors and service providers. The scenario centers on an external vendor relationship affecting exposure and controls.
4. Correct Answer: A. Issue, Finding and Exception Management
   Explanation: This element covers tracking, assigning, and resolving identified weaknesses or formally managing them as exceptions. The scenario describes a control weakness that must be managed through to closure or approved handling.
5. Correct Answer: C. Management of Emerging Risk
   Explanation: Emerging risk management focuses on new or rapidly changing exposures not captured in prior assessments. The scenario is about shifts that create new exposures beyond existing documentation.
6. Correct Answer: B. Risk and Control Ownership
   Explanation: The scenario asks who owns the risk decision and who owns the controls, which is the definition of ownership assignment. This element ensures responsibilities are clear for both risk and control outcomes.
7. Correct Answer: C. Third-Party Risk Management
   Explanation: Third-party risk management addresses risk introduced by vendor changes and external dependencies. The scenario involves increased exposure created outside the organization’s direct control.
8. Correct Answer: B. Issue, Finding and Exception Management
   Explanation: Managing exceptions requires tracking and controlling deviations so

they remain visible and governed. This element is the best fit because the scenario focuses on handling exceptions as formal, monitored items.

9. Correct Answer: A. Management of Emerging Risk
   Explanation: This element focuses on keeping risk understanding current as threats and technology evolve. The scenario is explicitly about updating assumptions and responses as new conditions appear.

10. Correct Answer: D. Risk Treatment / Risk Response Options
    Explanation: This element is about choosing the appropriate risk response and documenting the chosen path. The scenario emphasizes selection and execution planning for the response itself.

Bank 7

1. A risk manager needs to classify a set of controls and describe them using a shared vocabulary that aligns to recognized structures rather than ad hoc local labels. Which element best supports this need?
   A. Control Types, Standards and Frameworks
   B. Control Design, Selection and Analysis
   C. Control Implementation
   D. Control Testing and Effectiveness Evaluation

2. A team has identified a risk scenario and must decide which controls best address it, including evaluating tradeoffs and fit to the situation. Which element is most directly being applied?
   A. Control Implementation
   B. Control Testing and Effectiveness Evaluation
   C. Control Design, Selection and Analysis
   D. Control Types, Standards and Frameworks

3. A control is approved on paper, but the organization must put it into operation so it actually exists in practice. Which element best matches this step?
   A. Control Types, Standards and Frameworks
   B. Control Implementation
   C. Control Testing and Effectiveness Evaluation
   D. Control Design, Selection and Analysis

4. After a control is implemented, management wants evidence that it works as intended and continues to operate effectively over time. Which element best fits this requirement?
   A. Control Testing and Effectiveness Evaluation
   B. Control Implementation
   C. Control Design, Selection and Analysis
   D. Control Types, Standards and Frameworks

5. A risk manager is reviewing a proposed safeguard and needs to confirm it is the right control for the specific risk scenario, not simply “more controls.” Which element most directly addresses this decision?
   A. Control Implementation
   B. Control Design, Selection and Analysis
   C. Control Types, Standards and Frameworks
   D. Control Testing and Effectiveness Evaluation

6. A team wants to align their control program to a recognized structure so controls are comparable across areas and easier to communicate to stakeholders. Which element best supports this alignment?
   A. Control Design, Selection and Analysis
   B. Control Implementation
   C. Control Types, Standards and Frameworks
   D. Control Testing and Effectiveness Evaluation

7. A control is deployed, but the organization needs to verify it actually reduces risk and is not merely present in name only. Which element is most directly involved?
   A. Control Types, Standards and Frameworks
   B. Control Testing and Effectiveness Evaluation
   C. Control Implementation
   D. Control Design, Selection and Analysis

8. A risk manager must analyze multiple control candidates and select the one that best addresses the risk scenario while fitting organizational constraints. Which element best matches this activity?
   A. Control Design, Selection and Analysis
   B. Control Types, Standards and Frameworks
   C. Control Implementation
   D. Control Testing and Effectiveness Evaluation

9. A control is selected and designed, and the next challenge is ensuring it is put in place and adopted so it functions in day-to-day operations. Which element best fits this focus?
   A. Control Testing and Effectiveness Evaluation
   B. Control Types, Standards and Frameworks
   C. Control Implementation
   D. Control Design, Selection and Analysis

10. Management requests assurance that controls are not only designed properly but are also operating effectively, and they want this demonstrated through evaluation rather than assumption. Which element most directly answers this request?
    A. Control Implementation
    B. Control Design, Selection and Analysis
    C. Control Testing and Effectiveness Evaluation
    D. Control Types, Standards and Frameworks

1. Correct Answer: A. Control Types, Standards and Frameworks
   Explanation: This element provides shared terminology and structure for describing and classifying controls. It supports consistent communication by aligning control descriptions to recognized standards and frameworks.
2. Correct Answer: C. Control Design, Selection and Analysis
   Explanation: This element focuses on choosing the right controls for a given risk scenario and analyzing how well they fit. The scenario is about evaluating options and selecting the best control approach.
3. Correct Answer: B. Control Implementation
   Explanation: Implementation is the step where an approved control is put into operation so it exists in practice. The scenario is specifically about moving from approval to actual deployment.
4. Correct Answer: A. Control Testing and Effectiveness Evaluation
   Explanation: This element addresses validating that controls work as intended and continue to operate effectively. It emphasizes evidence of performance rather than assuming that implementation automatically equals effectiveness.
5. Correct Answer: B. Control Design, Selection and Analysis
   Explanation: The scenario requires confirming the control is appropriate for the specific risk rather than adding controls indiscriminately. This decision sits in the design, selection, and analysis step.
6. Correct Answer: C. Control Types, Standards and Frameworks
   Explanation: Standards and frameworks help organize controls in a consistent way so they are comparable and easier to communicate. This aligns the control program to recognized structures rather than local one-off definitions.
7. Correct Answer: B. Control Testing and Effectiveness Evaluation
   Explanation: Testing and evaluation determine whether a control meaningfully reduces risk and operates as intended. The scenario calls for verification beyond simply confirming the control exists.
8. Correct Answer: A. Control Design, Selection and Analysis
   Explanation: Comparing control candidates and selecting the best fit for the risk scenario is the core of design, selection, and analysis. It focuses on suitability and tradeoffs before implementation.
9. Correct Answer: C. Control Implementation
   Explanation: Once a control is chosen, implementation ensures it is actually put in

place and functioning in daily operations. The scenario centers on deployment and adoption rather than selection or testing.

10. Correct Answer: C. Control Testing and Effectiveness Evaluation
    Explanation: The request is for demonstrated assurance that controls operate effectively, which is provided through testing and evaluation. This element focuses on evidence-based confirmation of control performance.

Bank 8

1. A risk response has been selected, but leadership asks for a documented plan that assigns actions, timing, and checkpoints to reduce risk to an acceptable level. Which monitoring and reporting element best fits this need?
   A. Risk Treatment Plans
   B. Key Risk Indicators (KRIs)
   C. Risk and Control Monitoring Techniques
   D. Risk and Control Reporting Techniques (heatmap, scorecards, dashboards)

2. A risk manager receives inputs from multiple teams but notices contradictions and missing context, and must ensure the final risk view is accurate before it is used for decisions. Which element is most directly being applied?
   A. Risk Treatment Plans
   B. Data Collection, Aggregation, Analysis and Validation
   C. Key Control Indicators (KCIs)
   D. Key Performance Indicators

3. A risk manager needs an approach to continually observe risk conditions and control operation over time, rather than relying on one-time assessments. Which element best matches this requirement?
   A. Key Risk Indicators (KRIs)
   B. Risk and Control Reporting Techniques (heatmap, scorecards, dashboards)
   C. Risk and Control Monitoring Techniques
   D. Data Collection, Aggregation, Analysis and Validation

4. Senior leadership requests a concise, visual summary of risk and control status that can be reviewed quickly during governance meetings. Which element best fits this request?
   A. Risk Treatment Plans
   B. Key Performance Indicators
   C. Key Risk Indicators (KRIs)
   D. Risk and Control Reporting Techniques (heatmap, scorecards, dashboards)

5. A risk manager needs to track whether a set of agreed risk responses is being executed and whether planned actions are progressing as intended. Which element best supports this tracking?
   A. Risk Treatment Plans
   B. Risk and Control Reporting Techniques (heatmap, scorecards, dashboards)

C. Key Control Indicators (KCIs)
D. Risk and Control Monitoring Techniques

6. Management wants a small set of measures that show whether a process is performing as intended after changes were made, without directly measuring risk exposure. Which element best matches this need?
A. Key Risk Indicators (KRIs)
B. Key Performance Indicators
C. Risk and Control Monitoring Techniques
D. Data Collection, Aggregation, Analysis and Validation

7. A risk manager needs measures that provide early warning that risk exposure is increasing, so action can be taken before losses occur. Which element best matches this requirement?
A. Key Performance Indicators
B. Key Control Indicators (KCIs)
C. Key Risk Indicators (KRIs)
D. Risk Treatment Plans

8. A control is in place, but leadership wants a clear measure that indicates whether the control is operating as expected over time. Which element best fits this request?
A. Key Performance Indicators
B. Key Risk Indicators (KRIs)
C. Risk and Control Reporting Techniques (heatmap, scorecards, dashboards)
D. Key Control Indicators (KCIs)

9. A risk manager must combine inputs from different systems and teams into a single reliable view that supports monitoring and reporting decisions. Which element most directly describes this end-to-end activity?
A. Data Collection, Aggregation, Analysis and Validation
B. Risk and Control Reporting Techniques (heatmap, scorecards, dashboards)
C. Risk and Control Monitoring Techniques
D. Key Control Indicators (KCIs)

10. A risk manager is selecting methods to observe both risk conditions and control performance so that changes are identified and escalated appropriately. Which element best matches this selection activity?
A. Risk and Control Reporting Techniques (heatmap, scorecards, dashboards)
B. Key Performance Indicators

C. Risk and Control Monitoring Techniques
D. Risk Treatment Plans

---

1. Correct Answer: A. Risk Treatment Plans
   Explanation: Risk treatment plans document how approved responses will be executed, including actions and checkpoints. This is the best match when leadership wants a structured plan to drive risk reduction.
2. Correct Answer: B. Data Collection, Aggregation, Analysis and Validation
   Explanation: This element focuses on gathering inputs, combining them, analyzing them, and confirming they are accurate and usable. It directly applies when contradictions and missing information must be resolved before decisions are made.
3. Correct Answer: C. Risk and Control Monitoring Techniques
   Explanation: Monitoring techniques are used to continuously observe risk conditions and control operation over time. This fits the need for ongoing visibility rather than one-time assessment.
4. Correct Answer: D. Risk and Control Reporting Techniques (heatmap, scorecards, dashboards)
   Explanation: Reporting techniques provide summarized, often visual formats such as heatmaps, scorecards, and dashboards. They are designed for quick review by leadership in governance settings.
5. Correct Answer: A. Risk Treatment Plans
   Explanation: Treatment plans support tracking progress because they define the actions and milestones tied to the selected responses. This makes it possible to measure whether execution is occurring as intended.
6. Correct Answer: B. Key Performance Indicators
   Explanation: Key performance indicators measure how well a process or activity is performing without necessarily representing risk exposure. This matches the request for performance-oriented measures after changes.
7. Correct Answer: C. Key Risk Indicators (KRIs)
   Explanation: Key risk indicators are designed to signal changes in risk exposure early enough to prompt action. They best fit a requirement for early warning before losses occur.

8. Correct Answer: D. Key Control Indicators (KCIs)
   Explanation: Key control indicators measure whether a control is operating as expected and can reveal degradation over time. This is the best fit when leadership wants evidence of control operation, not just outcomes.

9. Correct Answer: A. Data Collection, Aggregation, Analysis and Validation
   Explanation: The scenario describes combining multiple inputs into a single reliable view and ensuring it is accurate. That end-to-end work is exactly what this element covers.

10. Correct Answer: C. Risk and Control Monitoring Techniques
    Explanation: Monitoring techniques define how risk and control conditions are observed and how changes are detected over time. Selecting these methods matches the scenario's focus on establishing ongoing observation and escalation.

Bank 9

1. A risk manager is evaluating whether technology changes align with how the organization structures and connects its systems and capabilities. Which Information Technology Principles topic best fits this evaluation?
   A. Enterprise Architecture
   B. Project Management
   C. Disaster Recovery Management (DRM)
   D. Data Lifecycle Management

2. A recurring pattern of issues appears after uncoordinated updates, and leadership wants more controlled handling of changes, incidents, and assets as part of day-to-day operations. Which topic is the best match?
   A. System Development Life Cycle (SDLC)
   B. IT Operations Management (e.g., change management, IT assets, problems, incidents)
   C. Emerging Technologies
   D. Enterprise Architecture

3. A risk manager must assess how work is planned, executed, tracked, and governed to ensure delivery aligns with expectations and constraints. Which topic best fits?
   A. Project Management
   B. Data Lifecycle Management
   C. Disaster Recovery Management (DRM)
   D. Enterprise Architecture

4. A risk scenario includes a major disruption, and leadership wants to ensure the organization can restore capability in a structured way. Which topic is most directly relevant?
   A. IT Operations Management (e.g., change management, IT assets, problems, incidents)
   B. Disaster Recovery Management (DRM)
   C. System Development Life Cycle (SDLC)
   D. Emerging Technologies

5. A risk manager is reviewing how data is handled from creation through use, storage, and eventual disposition, and wants to ensure risk decisions match those stages. Which topic best fits?
   A. Data Lifecycle Management
   B. Enterprise Architecture

C. Project Management
D. Emerging Technologies

6. A new application is being built, and the risk manager wants to ensure the development process follows defined stages from requirements through build, testing, and release. Which topic best matches this concern?
A. Project Management
B. System Development Life Cycle (SDLC)
C. Disaster Recovery Management (DRM)
D. IT Operations Management (e.g., change management, IT assets, problems, incidents)

7. A business unit proposes adopting a new, unfamiliar capability, and the risk manager must consider how rapidly changing technology could create new exposures not captured in current practices. Which topic best fits this situation?
A. Enterprise Architecture
B. Emerging Technologies
C. Data Lifecycle Management
D. Project Management

8. Leadership wants an organized view of how systems, processes, and technology components fit together so risk can be assessed in context rather than in isolated pieces. Which topic best supports this?
A. Enterprise Architecture
B. IT Operations Management (e.g., change management, IT assets, problems, incidents)
C. System Development Life Cycle (SDLC)
D. Disaster Recovery Management (DRM)

9. A risk manager is asked to confirm that ongoing operations handle problems and incidents in a repeatable way so disruptions are managed consistently. Which topic best applies?
A. Data Lifecycle Management
B. IT Operations Management (e.g., change management, IT assets, problems, incidents)
C. Project Management
D. Emerging Technologies

10. A risk manager is reviewing governance for technology work and needs to ensure the effort is planned and controlled as a defined initiative with responsibilities and

progress tracking. Which topic best matches this focus?
A. Project Management
B. Disaster Recovery Management (DRM)
C. Enterprise Architecture
D. System Development Life Cycle (SDLC)

---

1. Correct Answer: A. Enterprise Architecture
Explanation: Enterprise architecture provides an organized view of how systems and capabilities are structured and connected. It supports evaluating whether technology changes align with the organization's overall design and intended structure.

2. Correct Answer: B. IT Operations Management (e.g., change management, IT assets, problems, incidents)
Explanation: IT operations management covers day-to-day operational activities including change management, asset management, problem handling, and incident handling. The scenario centers on operational control and repeatability for changes and disruptions.

3. Correct Answer: A. Project Management
Explanation: Project management focuses on planning, executing, tracking, and governing work to meet objectives within constraints. The scenario is about ensuring delivery is controlled and aligned with expectations.

4. Correct Answer: B. Disaster Recovery Management (DRM)
Explanation: Disaster recovery management addresses structured restoration of capability after major disruption. The scenario explicitly involves restoring operations in a planned way.

5. Correct Answer: A. Data Lifecycle Management
Explanation: Data lifecycle management focuses on how data is handled across stages from creation through storage and disposition. The scenario is about aligning risk decisions to those lifecycle stages.

6. Correct Answer: B. System Development Life Cycle (SDLC)
Explanation: SDLC addresses defined stages for building and releasing systems, including requirements through testing and deployment. The scenario is focused on ensuring development follows a structured lifecycle.

7. Correct Answer: B. Emerging Technologies
   Explanation: Emerging technologies relate to new or rapidly changing capabilities that can introduce exposures not yet addressed by current practices. The scenario is about assessing new, unfamiliar technology risk.

8. Correct Answer: A. Enterprise Architecture
   Explanation: Enterprise architecture provides a holistic context for how systems and components fit together. This supports assessing risk with an understanding of dependencies rather than evaluating isolated elements.

9. Correct Answer: B. IT Operations Management (e.g., change management, IT assets, problems, incidents)
   Explanation: Operational management includes repeatable handling of incidents and problems to manage disruptions consistently. The scenario is specifically about consistent operational processes for issues and incidents.

10. Correct Answer: A. Project Management
    Explanation: Project management governs defined initiatives through responsibilities, planning, and progress tracking. The scenario centers on ensuring technology work is controlled as a formal project.

Bank 10

1. A risk manager wants to ensure security practices are defined and communicated using recognized structures rather than ad hoc local rules. Which Information Security Principles topic best supports this?
   A. Information Security Concepts, Frameworks and Standards
   B. Information Security Awareness Training
   C. Business Continuity Management
   D. Data Privacy and Data Protection Principles

2. An organization has recurring security issues tied to employee behavior, and leadership wants a structured approach to improving how people understand and follow expected security practices. Which topic best fits?
   A. Business Continuity Management
   B. Information Security Awareness Training
   C. Data Privacy and Data Protection Principles
   D. Information Security Concepts, Frameworks and Standards

3. A major disruption scenario is evaluated, and leadership needs a plan to sustain critical operations and continue essential services during the disruption. Which topic is most directly relevant?
   A. Business Continuity Management
   B. Data Privacy and Data Protection Principles
   C. Information Security Awareness Training
   D. Information Security Concepts, Frameworks and Standards

4. A risk manager is reviewing how sensitive information is handled and needs to ensure appropriate protection and privacy considerations are addressed throughout its use. Which topic best matches this focus?
   A. Information Security Awareness Training
   B. Business Continuity Management
   C. Data Privacy and Data Protection Principles
   D. Information Security Concepts, Frameworks and Standards

5. A team wants to describe security expectations in a consistent way so stakeholders can compare requirements across different areas of the organization. Which topic best supports that consistency?
   A. Information Security Awareness Training
   B. Information Security Concepts, Frameworks and Standards

C. Business Continuity Management
D. Data Privacy and Data Protection Principles

6. After several near-miss incidents, a risk manager is asked to strengthen how staff recognize security responsibilities and reduce errors that lead to exposure. Which topic best fits?
   A. Data Privacy and Data Protection Principles
   B. Business Continuity Management
   C. Information Security Awareness Training
   D. Information Security Concepts, Frameworks and Standards

7. Leadership requests assurance that the organization can continue operating through disruption, rather than only focusing on restoring systems after the fact. Which topic best matches this emphasis?
   A. Business Continuity Management
   B. Information Security Concepts, Frameworks and Standards
   C. Data Privacy and Data Protection Principles
   D. Information Security Awareness Training

8. A risk manager is defining security expectations and wants to anchor them to established concepts and recognized structures for how security should be organized. Which topic best applies?
   A. Information Security Awareness Training
   B. Data Privacy and Data Protection Principles
   C. Information Security Concepts, Frameworks and Standards
   D. Business Continuity Management

9. A risk manager is asked to ensure that protection of information includes both privacy considerations and safeguards for handling and exposure reduction. Which topic best fits?
   A. Business Continuity Management
   B. Data Privacy and Data Protection Principles
   C. Information Security Awareness Training
   D. Information Security Concepts, Frameworks and Standards

10. A risk manager is preparing security guidance and needs to select the topic area that covers structured security concepts and how they are organized through frameworks and standards. Which is the best match?
    A. Business Continuity Management
    B. Data Privacy and Data Protection Principles

C. Information Security Concepts, Frameworks and Standards
D. Information Security Awareness Training

---

1. Correct Answer: A. Information Security Concepts, Frameworks and Standards
Explanation: This topic covers security concepts organized through recognized frameworks and standards, which supports consistency across the organization. It fits when the goal is structured, common security expectations rather than local one-off rules.

2. Correct Answer: B. Information Security Awareness Training
Explanation: Awareness training focuses on improving employee understanding and behavior related to security expectations. The scenario centers on recurring issues tied to people and the need to strengthen knowledge and adherence.

3. Correct Answer: A. Business Continuity Management
Explanation: Business continuity management focuses on sustaining critical operations during disruption. The scenario is about continuing essential services rather than only restoring systems afterward.

4. Correct Answer: C. Data Privacy and Data Protection Principles
Explanation: This topic addresses protecting sensitive information and incorporating privacy considerations into how information is handled. It matches a review focused on safeguarding information and privacy throughout its use.

5. Correct Answer: B. Information Security Concepts, Frameworks and Standards
Explanation: Frameworks and standards provide consistent security structure and terminology across different areas. This supports comparability of requirements and expectations across the organization.

6. Correct Answer: C. Information Security Awareness Training
Explanation: The scenario is about reducing exposure caused by staff errors by strengthening how people recognize security responsibilities. Awareness training directly targets this need by improving understanding and behavior.

7. Correct Answer: A. Business Continuity Management
Explanation: The scenario emphasizes continuing operations through disruption, which is the core purpose of business continuity management. It differs from restoration-focused efforts by prioritizing sustained critical services.

8. Correct Answer: C. Information Security Concepts, Frameworks and Standards
Explanation: This topic is the best fit when anchoring security expectations to

established concepts and organized structures. It provides a foundation for consistent security organization and communication.

9. Correct Answer: B. Data Privacy and Data Protection Principles
Explanation: This topic explicitly covers both privacy considerations and protective handling of information. It fits when the requirement is to address privacy and protection together as part of safeguarding information.

10. Correct Answer: C. Information Security Concepts, Frameworks and Standards
Explanation: This topic is specifically about structured security concepts and how they are organized through frameworks and standards. It best matches the request for guidance grounded in recognized security structures.

Bank 11

1. A risk manager is assigned to begin an IT risk assessment but discovers there is no consolidated understanding of the organization's current business and IT environments. What is the most appropriate first action based on the provided task statements?
   A. Collect and review existing information regarding the organization's business and IT environments
   B. Establish accountability by assigning and validating appropriate levels of risk and control ownership
   C. Evaluate threats, vulnerabilities and risk to identify IT risk scenarios
   D. Identify potential or realized impacts of IT risk to the organization's business objectives and operations

2. A risk scenario is being discussed, but leadership keeps asking, "So what does this mean for our business objectives and day-to-day operations?" Which task best matches what the risk manager should do next?
   A. Identify threats and vulnerabilities to the organization's people, processes and technology
   B. Identify potential or realized impacts of IT risk to the organization's business objectives and operations
   C. Collect and review existing information regarding the organization's business and IT environments
   D. Establish accountability by assigning and validating appropriate levels of risk and control ownership

3. During an assessment, the team has documented the environment and business context, but they have not yet identified what could exploit weaknesses across people, processes, or technology. Which task best fits the missing step?
   A. Evaluate threats, vulnerabilities and risk to identify IT risk scenarios
   B. Identify potential or realized impacts of IT risk to the organization's business objectives and operations
   C. Identify threats and vulnerabilities to the organization's people, processes and technology
   D. Collect and review existing information regarding the organization's business and IT environments

4. A risk manager has identified several threats and vulnerabilities, but stakeholders want these translated into clear IT risk scenarios that can be assessed and prioritized. Which task best matches this request?

A. Identify potential or realized impacts of IT risk to the organization’s business objectives and operations
B. Establish accountability by assigning and validating appropriate levels of risk and control ownership
C. Collect and review existing information regarding the organization’s business and IT environments
D. Evaluate threats, vulnerabilities and risk to identify IT risk scenarios

5. A risk response is proposed, but no one can confirm who owns the risk decision and who owns the controls involved. Which task most directly addresses this gap?
A. Establish accountability by assigning and validating appropriate levels of risk and control ownership
B. Identify threats and vulnerabilities to the organization’s people, processes and technology
C. Evaluate threats, vulnerabilities and risk to identify IT risk scenarios
D. Identify potential or realized impacts of IT risk to the organization’s business objectives and operations

6. A risk manager is asked to begin work on IT risk but chooses to first gather information about both business operations and IT components so later analysis is grounded in the real environment. Which task is being performed?
A. Identify potential or realized impacts of IT risk to the organization’s business objectives and operations
B. Collect and review existing information regarding the organization’s business and IT environments
C. Identify threats and vulnerabilities to the organization’s people, processes and technology
D. Establish accountability by assigning and validating appropriate levels of risk and control ownership

7. Stakeholders have provided a list of threats and weaknesses, but the risk manager must determine how those combine into a risk scenario rather than leaving them as separate observations. Which task best fits that need?
A. Collect and review existing information regarding the organization’s business and IT environments
B. Identify potential or realized impacts of IT risk to the organization’s business objectives and operations
C. Evaluate threats, vulnerabilities and risk to identify IT risk scenarios

D. Establish accountability by assigning and validating appropriate levels of risk and control ownership

8. A team wants to move from “we have some threats and vulnerabilities” to “we have a defined IT risk scenario,” and they want the risk manager to do the analysis that connects those pieces. Which task most directly supports that transition?
   A. Identify threats and vulnerabilities to the organization’s people, processes and technology
   B. Identify potential or realized impacts of IT risk to the organization’s business objectives and operations
   C. Collect and review existing information regarding the organization’s business and IT environments
   D. Evaluate threats, vulnerabilities and risk to identify IT risk scenarios

9. A risk manager is preparing to identify threats and vulnerabilities but realizes they do not yet understand the organization’s current business objectives, operational processes, and IT environment well enough to proceed. What should they do first?
   A. Collect and review existing information regarding the organization’s business and IT environments
   B. Establish accountability by assigning and validating appropriate levels of risk and control ownership
   C. Evaluate threats, vulnerabilities and risk to identify IT risk scenarios
   D. Identify potential or realized impacts of IT risk to the organization’s business objectives and operations

10. A risk scenario has been documented, but decision-making is stalled because it is unclear who should be accountable for the risk and who should be accountable for the controls associated with it. Which task best resolves this?
    A. Identify threats and vulnerabilities to the organization’s people, processes and technology
    B. Establish accountability by assigning and validating appropriate levels of risk and control ownership
    C. Collect and review existing information regarding the organization’s business and IT environments
    D. Identify potential or realized impacts of IT risk to the organization’s business objectives and operations

1. Correct Answer: A. Collect and review existing information regarding the organization’s business and IT environments
   Explanation: The first task explicitly states to collect and review existing information about the business and IT environments. This establishes the baseline context needed before impacts, threats, or scenarios can be evaluated.

2. Correct Answer: B. Identify potential or realized impacts of IT risk to the organization’s business objectives and operations
   Explanation: The task statement directly focuses on identifying impacts to business objectives and operations. It matches leadership’s request to translate risk into business and operational consequences.

3. Correct Answer: C. Identify threats and vulnerabilities to the organization’s people, processes and technology
   Explanation: The task statement explicitly calls for identifying threats and vulnerabilities across people, processes, and technology. This is the missing step after environment context is established but before scenario evaluation.

4. Correct Answer: D. Evaluate threats, vulnerabilities and risk to identify IT risk scenarios
   Explanation: The task statement directly describes evaluating threats and vulnerabilities in order to identify IT risk scenarios. It is the step that turns inputs into assessable scenarios.

5. Correct Answer: A. Establish accountability by assigning and validating appropriate levels of risk and control ownership
   Explanation: The task statement explicitly requires assigning and validating risk and control ownership. This addresses the exact gap where no one can confirm accountability for the risk decision and related controls.

6. Correct Answer: B. Collect and review existing information regarding the organization’s business and IT environments
   Explanation: The task statement describes gathering and reviewing information about both business and IT environments. That is the described activity before deeper risk analysis steps occur.

7. Correct Answer: C. Evaluate threats, vulnerabilities and risk to identify IT risk scenarios
   Explanation: The task statement ties evaluation of threats and vulnerabilities to the identification of IT risk scenarios. This matches the need to connect observations into a defined scenario.

8. Correct Answer: D. Evaluate threats, vulnerabilities and risk to identify IT risk scenarios
   Explanation: The task statement is the one that explicitly moves from threats and vulnerabilities to risk scenarios through evaluation. It best supports the transition the team is asking for.

9. Correct Answer: A. Collect and review existing information regarding the organization's business and IT environments
   Explanation: The task statement makes collecting and reviewing environment information the foundational step. Without that context, threat and vulnerability identification is likely to be incomplete or misaligned.

10. Correct Answer: B. Establish accountability by assigning and validating appropriate levels of risk and control ownership
    Explanation: The task statement directly addresses accountability by assigning and validating ownership for risk and controls. This resolves the stalled decision-making caused by unclear ownership.

Bank 12

1. A risk manager discovers that risk information is scattered across emails and team documents, and leadership cannot see how IT risks roll up into a consolidated view of top organizational risks. Which task best addresses this need?
   A. Establish and maintain the IT risk register and incorporate it into the enterprise-wide risk profile
   B. Conduct a risk assessment by analyzing IT risk scenarios and determining their likelihood and impact
   C. Identify the current state of existing controls and evaluate their effectiveness for IT risk mitigation
   D. Review risk and control analysis results to assess gaps between current and desired states of the IT risk environment

2. During planning, senior stakeholders disagree on what level of IT risk is acceptable and when escalation is required. Which task best fits what the risk manager should facilitate?
   A. Promote a risk-aware culture by contributing to the development and implementation of security awareness training
   B. Facilitate the identification of risk appetite and risk tolerance by key stakeholders
   C. Establish and maintain the IT risk register and incorporate it into the enterprise-wide risk profile
   D. Review risk and control analysis results to assess gaps between current and desired states of the IT risk environment

3. An organization has repeated risk-related errors tied to employee behavior, and management wants the risk function to help strengthen how people recognize and respond to security expectations. Which task best matches this objective?
   A. Promote a risk-aware culture by contributing to the development and implementation of security awareness training
   B. Identify the current state of existing controls and evaluate their effectiveness for IT risk mitigation
   C. Conduct a risk assessment by analyzing IT risk scenarios and determining their likelihood and impact
   D. Establish and maintain the IT risk register and incorporate it into the enterprise-wide risk profile

4. A risk manager has documented several IT risk scenarios and must now determine how likely they are and how severe their consequences could be. Which task best matches this step?

A. Review risk and control analysis results to assess gaps between current and desired states of the IT risk environment
B. Conduct a risk assessment by analyzing IT risk scenarios and determining their likelihood and impact
C. Facilitate the identification of risk appetite and risk tolerance by key stakeholders
D. Identify the current state of existing controls and evaluate their effectiveness for IT risk mitigation

5. A risk manager is asked to evaluate whether the organization’s existing controls are currently operating effectively to reduce IT risk, rather than relying on assumptions about what controls should do. Which task best fits?
   A. Conduct a risk assessment by analyzing IT risk scenarios and determining their likelihood and impact
   B. Promote a risk-aware culture by contributing to the development and implementation of security awareness training
   C. Identify the current state of existing controls and evaluate their effectiveness for IT risk mitigation
   D. Establish and maintain the IT risk register and incorporate it into the enterprise-wide risk profile

6. After completing risk and control analysis, leadership asks, “Where are we today compared to where we need to be?” Which task best addresses this request?
   A. Review risk and control analysis results to assess gaps between current and desired states of the IT risk environment
   B. Conduct a risk assessment by analyzing IT risk scenarios and determining their likelihood and impact
   C. Identify the current state of existing controls and evaluate their effectiveness for IT risk mitigation
   D. Promote a risk-aware culture by contributing to the development and implementation of security awareness training

7. A risk manager is updating documentation and must ensure the IT risk register stays current and that its contents are represented in enterprise-level summaries used for governance. Which task best fits?
   A. Facilitate the identification of risk appetite and risk tolerance by key stakeholders
   B. Establish and maintain the IT risk register and incorporate it into the enterprise-wide risk profile
   C. Conduct a risk assessment by analyzing IT risk scenarios and determining their likelihood and impact

D. Review risk and control analysis results to assess gaps between current and desired states of the IT risk environment

8. An organization wants to strengthen consistency in decision-making by clarifying boundaries for acceptable risk and escalation thresholds, and the risk manager is asked to drive that conversation with leaders. Which task best matches?
A. Facilitate the identification of risk appetite and risk tolerance by key stakeholders
B. Promote a risk-aware culture by contributing to the development and implementation of security awareness training
C. Identify the current state of existing controls and evaluate their effectiveness for IT risk mitigation
D. Establish and maintain the IT risk register and incorporate it into the enterprise-wide risk profile

9. A risk manager is reviewing the environment and needs to understand whether current controls reduce risk enough, or whether control performance leaves the organization exposed. Which task best applies?
A. Review risk and control analysis results to assess gaps between current and desired states of the IT risk environment
B. Identify the current state of existing controls and evaluate their effectiveness for IT risk mitigation
C. Promote a risk-aware culture by contributing to the development and implementation of security awareness training
D. Conduct a risk assessment by analyzing IT risk scenarios and determining their likelihood and impact

10. A risk manager completes likelihood and impact determinations and then compares those results, along with control effectiveness observations, against a desired target state to identify what must change. Which task best fits this comparison step?
A. Establish and maintain the IT risk register and incorporate it into the enterprise-wide risk profile
B. Facilitate the identification of risk appetite and risk tolerance by key stakeholders
C. Review risk and control analysis results to assess gaps between current and desired states of the IT risk environment
D. Promote a risk-aware culture by contributing to the development and implementation of security awareness training

1. Correct Answer: A. Establish and maintain the IT risk register and incorporate it into the enterprise-wide risk profile
   Explanation: This task explicitly requires maintaining the IT risk register and incorporating it into the enterprise-wide risk profile. It directly addresses scattered risk information and the need to roll IT risk into a consolidated organizational view.
2. Correct Answer: B. Facilitate the identification of risk appetite and risk tolerance by key stakeholders
   Explanation: The task statement explicitly focuses on facilitating identification of risk appetite and risk tolerance by key stakeholders. It fits when leaders disagree about acceptable risk levels and escalation thresholds.
3. Correct Answer: A. Promote a risk-aware culture by contributing to the development and implementation of security awareness training
   Explanation: This task is specifically about promoting a risk-aware culture through security awareness training development and implementation. It aligns with behavior-driven risk issues and management's desire to improve awareness and response.
4. Correct Answer: B. Conduct a risk assessment by analyzing IT risk scenarios and determining their likelihood and impact
   Explanation: The task statement directly describes analyzing risk scenarios and determining likelihood and impact. This is the core step when moving from scenario descriptions to assessed risk levels.
5. Correct Answer: C. Identify the current state of existing controls and evaluate their effectiveness for IT risk mitigation
   Explanation: This task explicitly requires identifying the current state of controls and evaluating their effectiveness. It matches the need to assess actual control performance rather than relying on assumptions.
6. Correct Answer: A. Review risk and control analysis results to assess gaps between current and desired states of the IT risk environment
   Explanation: The task statement focuses on assessing gaps between current and desired states based on risk and control analysis results. It directly answers the question of where the organization is today versus where it needs to be.
7. Correct Answer: B. Establish and maintain the IT risk register and incorporate it into the enterprise-wide risk profile
   Explanation: The task statement includes both maintaining the risk register and

ensuring it is reflected in the enterprise-wide risk profile. It fits when the focus is keeping the register current and visible in governance reporting.

8. Correct Answer: A. Facilitate the identification of risk appetite and risk tolerance by key stakeholders
   Explanation: The task statement is about facilitating leadership agreement on appetite and tolerance boundaries. It matches the goal of strengthening decision consistency through clear thresholds and escalation triggers.

9. Correct Answer: B. Identify the current state of existing controls and evaluate their effectiveness for IT risk mitigation
   Explanation: This task focuses on evaluating existing controls and their effectiveness in mitigating IT risk. It aligns with determining whether current controls reduce exposure sufficiently.

10. Correct Answer: C. Review risk and control analysis results to assess gaps between current and desired states of the IT risk environment
    Explanation: The task statement describes reviewing analysis results to find gaps between current and desired states. The scenario is exactly that comparison step after likelihood, impact, and control effectiveness are known.

Bank 13

1. A risk manager has completed analysis and must help leaders choose the best path to address the risk, ensuring the decision is made by the appropriate stakeholders. Which task best applies?
   A. Collaborate with risk owners on development of risk treatment plans
   B. Facilitate selection of recommended risk responses by key stakeholders
   C. Validate that risk responses have been executed according to risk treatment plans
   D. Monitor and analyze KRIs

2. After a risk response is selected, the risk manager needs to work with the people accountable for the risk to document the planned actions and how the response will be carried out. Which task best fits this work?
   A. Collaborate with risk owners on development of risk treatment plans
   B. Define and establish key risk indicators (KRIs)
   C. Facilitate selection of recommended risk responses by key stakeholders
   D. Validate that risk responses have been executed according to risk treatment plans

3. A new mitigation approach is proposed, but the risk manager must coordinate with those responsible for controls to ensure the correct controls are selected, designed appropriately, implemented, and kept effective over time. Which task best matches?
   A. Validate that risk responses have been executed according to risk treatment plans
   B. Collaborate with control owners on selection, design, implementation and maintenance of controls
   C. Monitor and analyze KRIs
   D. Collaborate with risk owners on development of risk treatment plans

4. Leadership approved a risk treatment plan last quarter, and the risk manager is now asked to confirm that the agreed actions were actually completed as planned. Which task best applies?
   A. Validate that risk responses have been executed according to risk treatment plans
   B. Facilitate selection of recommended risk responses by key stakeholders
   C. Monitor and analyze KRIs
   D. Define and establish key risk indicators (KRIs)

5. A risk manager wants to create a small set of measures that will signal changes in risk exposure so stakeholders can act early. Which task best matches this objective?
   A. Collaborate with control owners on selection, design, implementation and maintenance of controls
   B. Define and establish key risk indicators (KRIs)
   C. Monitor and analyze KRIs
   D. Collaborate with risk owners on development of risk treatment plans

6. A set of KRIs has been defined, and the risk manager is asked to review trends and results regularly to detect changes in risk levels. Which task best fits?
   A. Monitor and analyze KRIs
   B. Validate that risk responses have been executed according to risk treatment plans
   C. Define and establish key risk indicators (KRIs)
   D. Facilitate selection of recommended risk responses by key stakeholders

7. Stakeholders are presented with several recommended responses, and the risk manager's role is to ensure a decision is reached and documented by the appropriate decision-makers. Which task best applies?
   A. Collaborate with risk owners on development of risk treatment plans
   B. Facilitate selection of recommended risk responses by key stakeholders
   C. Collaborate with control owners on selection, design, implementation and maintenance of controls
   D. Monitor and analyze KRIs

8. A risk manager is asked to work with risk owners to convert a selected response into a practical plan that defines what will be done and how it will be tracked. Which task best matches this responsibility?
   A. Validate that risk responses have been executed according to risk treatment plans
   B. Define and establish key risk indicators (KRIs)
   C. Collaborate with risk owners on development of risk treatment plans
   D. Monitor and analyze KRIs

9. A control owner reports that certain controls are being changed, and the risk manager must ensure these controls remain properly selected, designed, implemented, and maintained as part of the risk response. Which task best applies?
   A. Collaborate with control owners on selection, design, implementation and maintenance of controls

B. Facilitate selection of recommended risk responses by key stakeholders
C. Validate that risk responses have been executed according to risk treatment plans
D. Define and establish key risk indicators (KRIs)

10. A risk manager needs to confirm that the organization is not only tracking risk through indicators but also taking the agreed response actions according to the plan. Which task best fits this confirmation activity?
    A. Monitor and analyze KRIs
    B. Collaborate with risk owners on development of risk treatment plans
    C. Validate that risk responses have been executed according to risk treatment plans
    D. Define and establish key risk indicators (KRIs)

---

1. Correct Answer: B. Facilitate selection of recommended risk responses by key stakeholders
   Explanation: This task explicitly focuses on facilitating stakeholder selection of recommended risk responses. It matches the scenario where leaders must choose the response and the risk manager supports that decision process.

2. Correct Answer: A. Collaborate with risk owners on development of risk treatment plans
   Explanation: This task is specifically about collaborating with risk owners to develop risk treatment plans after a response is selected. It fits when the goal is documenting planned actions and execution details with the accountable risk owners.

3. Correct Answer: B. Collaborate with control owners on selection, design, implementation and maintenance of controls
   Explanation: This task directly describes working with control owners across the full control lifecycle, from selection and design through implementation and maintenance. The scenario focuses on ensuring controls supporting the response are properly built and sustained.

4. Correct Answer: A. Validate that risk responses have been executed according to risk treatment plans
   Explanation: This task explicitly requires validating execution of risk responses against the treatment plan. It fits when leadership asks for confirmation that approved actions were actually completed.

5. Correct Answer: B. Define and establish key risk indicators (KRIs)
   Explanation: This task is about defining and establishing KRIs, which are measures that signal changes in risk exposure. The scenario describes creating indicators so stakeholders can detect rising risk early.

6. Correct Answer: A. Monitor and analyze KRIs
   Explanation: This task focuses on ongoing monitoring and analysis of KRIs after they are established. It matches the scenario of reviewing trends and results regularly to detect changes in risk levels.

7. Correct Answer: B. Facilitate selection of recommended risk responses by key stakeholders
   Explanation: The scenario describes enabling decision-making by key stakeholders among recommended responses. This aligns directly with facilitating selection of risk responses.

8. Correct Answer: C. Collaborate with risk owners on development of risk treatment plans
   Explanation: The scenario is about turning the selected response into a practical, trackable plan with risk owners. That is the purpose of collaborating on development of risk treatment plans.

9. Correct Answer: A. Collaborate with control owners on selection, design, implementation and maintenance of controls
   Explanation: This task covers ensuring controls remain properly selected, designed, implemented, and maintained. The scenario is specifically about controls changing and the need to ensure they continue to support the response.

10. Correct Answer: C. Validate that risk responses have been executed according to risk treatment plans
    Explanation: The scenario emphasizes confirming that agreed response actions were executed according to the plan. That confirmation is exactly what this validation task requires.