CRISC IT Risk Exam Prep

Free Practice Test — 30 Real Exam-Style Questions

with full answer key & explanations

Practice Questions

Try all 30 first, then check the answer key at the back.

1. What type of audit ensures that a company's financial statements are prepared in accordance with established standards or regulations?

A. Internal
B. Operational
C. Forensic
D. Compliance

2. Which assessment method uses a quantitative approach to evaluate the impact of various financial scenarios on a company's risk profile?

A. Risk probability analysis
B. Scenario planning
C. Stress testing
D. SWOT analysis

3. Which of the following is NOT a risk factor when implementing an agile project management approach?

A. Issues with team collaboration
B. Difficulty in maintaining project scope
C. Project finishes ahead of schedule
D. Frequent changes in requirements

4. Which of the following is NOT a key factor in assessing risk mitigation strategies?

A. Cost-effectiveness
B. Implementation feasibility
C. Asset depreciation
D. Impact on business operations

5. Within the context of the NIST Risk Management Framework (RMF), what phase involves implementing and validating the security controls to ensure they achieve the desired security outcomes consistently?

A. Monitoring
B. Implementation
C. Assessment
D. Authorization

6. Which method ensures that confidential financial data remains protected when conducting risk assessments?

A. Data Mining
B. Data Dumping
C. Data Masking
D. Data Sharding

7. When analyzing risk for an information system, which type of metric provides insights only after security breaches have occurred?

A. Predictive
B. Preventive
C. Lagging
D. Leading

8. Which type of review ensures that a project's progress aligns with the planned objectives and milestones?

A. Code review
B. Peer review
C. Post-implementation review
D. Project evaluation review

9. In the context of risk response planning, which committee is generally responsible for coordinating and overseeing disaster recovery efforts?

A. SLA
B. CAB
C. DRC
D. QAR

10. What is the first step a risk practitioner should take when developing a risk response strategy?

A. Assess the current state of the risk environment
B. Estimate the financial cost of implementing new controls
C. Ignore existing risks and create new strategies from scratch
D. Rely solely on historical data without current analysis

11. When implementing a new data encryption system, which of the following vulnerabilities could potentially be introduced?

A. Improvement in data access time
B. No possible new vulnerabilities can be introduced.
C. Loss of existing encrypted data
D. Increase in data processing speed

12. Which tool or technique is commonly utilized by organizations to systematically identify and assess risks in their information systems?

A. Marketing strategies
B. Risk assessment framework
C. Employee training sessions
D. Customer feedback surveys

13. What is the primary risk associated with a new software deployment that relies heavily on untested technologies?

A. Technology failure
B. Excessive user training
C. Extended testing periods
D. Redundant system redundancies

14. What is the maximum fine for violating the Health Insurance Portability and Accountability Act (HIPAA) regulations?

A. $\$1.5$ million annually per violation category
B. No limit
C. 25% of the organization's yearly revenue
D. $\$5$ million per incident

15. Which of the following is NOT a criteria for selecting an information security framework for an organization?

A. Geographical location
B. Risk tolerance
C. Regulatory requirements
D. Business objectives

16. In the context of security operations, what risk factor makes it challenging to appropriately respond to an incident due to lack of awareness of involved assets?

A. Lack of network bandwidth
B. Lack of event logging
C. Lack of compliance
D. Lack of asset inventory

17. When dealing with unexpected IT system downtimes, what is the most effective risk management response to ensure system resilience?

A. Increasing staff training
B. Implementing redundancy
C. Reducing software licensing fees
D. Extending maintenance windows

18. In the context of an organization's cybersecurity strategy, what role should the risk practitioner assume when dealing with new and evolving cyber threats?

A. Reactive response
B. Policy enforcer
C. Threat mitigator only after an attack
D. Proactive monitoring

19. Which of the following principles is included in the ISACA Code of Professional Ethics?

A. Maintain confidentiality and privacy of information
B. Share all corporate information with external auditors without restriction
C. Allow only CRISC-certified individuals to access secure information
D. Renew ISACA certification bi-annually

20. Which role identifies the individual responsible for approving a risk management strategy and ensuring its alignment with organizational goals?

A. Consulted
B. Informed
C. Realized
D. Accountable

21. Which elements form the foundation of a solid information security management framework?

A. Policies, procedures, guidelines
B. Technology, systems, protocols
C. Services, applications, policies
D. Hardware, software, techniques

22. In what scenario might an organization decide to accept the risk of not complying with industry standards?

A. If the organization is only partially involved in the industry
B. If the organization has not faced regulatory action in the past year
C. If they plan to merge with a compliant company
D. If the cost of compliance is greater than the risk of non-compliance

23. What is the primary goal of an enterprise risk management framework versus a departmental risk management framework?

A. To select appropriate risk assessment tools
B. To establish a comprehensive strategy for managing all types of risks across the entire organization
C. To categorize risks based on financial impact
D. To outline individual employee responsibilities in risk management

24. Which personnel role is primarily responsible for the continuous assessment and mitigation of cybersecurity risks within an organization?

A. Cybersecurity officer
B. Compliance manager
C. IT support specialist
D. Risk analyst

25. Which risk governance principle helps an organization consistently establish levels of risk appetite?

A. Risk oversight framework
B. Common risk perspective
C. Risk response alignment
D. Risk metrics standardization

26. In the context of IT governance, which role is primarily informed about the progress of IT compliance activities?

A. Informed
B. Responsible
C. Accountable
D. Consulted

27. Which risk assessment method involves identifying potential threats based on the specific functions and operations of individual business units?

A. Enterprise risk assessment
B. Systematic risk assessment
C. Operational risk assessment
D. Strategic risk assessment

28. What is the primary function of an asset register in an IT risk management framework?

A. Eliminate IT assets
B. Catalog IT assets
C. Decentralize IT assets
D. Filter IT assets

29. Which network architecture model allows an organization to manage its own networking hardware and software?

A. Cloud-based
B. Hybrid
C. Virtualized
D. On-premises

30. Which method of risk identification relies on evaluating past project outcomes, stakeholder feedback, and historical performance data?

A. Statistical
B. Historical
C. Predictive
D. Qualitative

Answer Key & Explanations

1. D — Compliance
Compliance audits are performed to ensure that financial statements and other reports adhere to industry standards and governmental regulations. This is crucial for legal and ethical business operations.

2. C — Stress testing
Answer: Stress testing Stress testing uses numerical methods to evaluate how different financial scenarios impact a company's risk profile. It examines the extent to which unexpected events or market changes can affect the company's financial stability.

3. C — Project finishes ahead of schedule
Answer: Project finishes ahead of schedule An agile project management approach often involves iterative cycles, frequent testing, and constant feedback. These characteristics can lead to challenges such as managing frequent changes, ensuring proper collaboration among team members, and maintaining the project scope. Finishing ahead of schedule is not typically considered a risk factor.

4. C — Asset depreciation
Answer: Asset depreciation While asset depreciation can affect an organization's overall financial health, it is not a primary factor in assessing the effectiveness of risk mitigation strategies. Key factors include the impact on business operations, cost-effectiveness, and implementation feasibility.

5. B — Implementation
Answer: Implementation According to the NIST RMF, the Implementation phase involves putting security controls into place and ensuring they function effectively, thus achieving the desired security outcomes consistently across the organization.

6. C — Data Masking
Answer: Data Masking Data masking involves altering the original data to hide sensitive information while maintaining its usability for testing purposes. This ensures that confidential financial data remains protected during risk assessments or other analytical activities.

7. C — Lagging
Lagging metrics report on the impact of a security breach after it has occurred, demonstrating the consequences of such events.

8. D — Project evaluation review
Project evaluation review is conducted to ensure that a project's progress aligns with the planned objectives and milestones. This review is crucial for making adjustments to keep the project on track.

9. C — DRC
Answer: DRC A Disaster Recovery Committee (DRC) is a group of stakeholders responsible for coordinating and overseeing disaster recovery efforts. Their collective oversight helps to ensure a comprehensive and effective response to minimize business disruption.

10. A — Assess the current state of the risk environment
Answer: Assess the current state of the risk environment Understanding the current risk environment helps ensure that the risk practitioner can identify which risks are already accounted for and which require new strategies. This initial assessment is crucial for effective risk management.

11. C — Loss of existing encrypted data
Answer: Loss of existing encrypted data When implementing a new data encryption system, if the migration process is not handled properly, existing encrypted data could become inaccessible, resulting in data loss.

12. B — Risk assessment framework
Answer: Risk assessment framework A risk assessment framework is a structured tool used by organizations to identify, evaluate, and prioritize risks in their information systems. These frameworks provide a systematic approach, including methodologies, processes, and best practices, to help organizations manage and mitigate risks effectively.

13. A — Technology failure
Answer: Technology failure Deploying new software that relies on untested technologies can lead to technology failures, which can compromise the system's functioning and result in significant project delays.

14. A — $\$1.5$ million annually per violation category
Answer: $\$1.5$ million annually per violation category. HIPAA sets stringent penalties for non-compliance to ensure the protection of sensitive patient health information.

15. A — Geographical location
Answer: Geographical location Selecting an information security framework involves considering the organization's risk tolerance, regulatory requirements, and business objectives to ensure comprehensive security measures.

16. D — Lack of asset inventory
Answer: Lack of asset inventory Without a comprehensive asset inventory, it becomes very difficult to identify and respond to incidents effectively. Asset inventory ensures that all assets are accounted for, thus facilitating better incident management.

17. B — Implementing redundancy
Answer: Implementing redundancy Unexpected IT system downtimes often occur due to hardware or software failures. Implementing redundancy—having backup systems in place—ensures that the system can continue to operate even if primary components fail, thereby enhancing resilience.

18. D — Proactive monitoring
Risk practitioners should engage in proactive monitoring to identify and address cyber threats before they materialize. This approach ensures that the organization stays ahead of potential risks, thereby aligning with its cybersecurity strategy and goals.

19. A — Maintain confidentiality and privacy of information
Answer: Maintain confidentiality and privacy of information. The ISACA Code of Professional Ethics requires risk practitioners to uphold the confidentiality and privacy of information obtained during work engagements.

20. D — Accountable
Answer: Accountable Individuals who are accountable are responsible for approving the risk management

strategy. They ensure it aligns with organizational goals and oversee its implementation. Their accountability is crucial for the success of the strategy.

21. A — Policies, procedures, guidelines
Policies, procedures, and guidelines form the backbone of a robust information security management framework. These elements provide structured and comprehensive approaches to identify, manage, and mitigate security risks across an organization. Unlike technical controls or specific software applications, these practices focus on consistency, clarity, and compliance to ensure all business functions adhere to security best practices and regulatory requirements.

22. D — If the cost of compliance is greater than the risk of non-compliance
Answer: If the cost of compliance is greater than the risk of non-compliance. Risk decisions are made based on an organization's risk appetite, which is set by senior management. If the cost of meeting industry standards outweighs the potential impacts of not complying, an organization might choose to accept the risk.

23. B — To establish a comprehensive strategy for managing all types of risks across the entire organization
Answer: To establish a comprehensive strategy for managing all types of risks across the entire organization An enterprise risk management (ERM) framework is designed to address the organization’s overarching approach to risk and to define the overall risk tolerance. The target audience is senior management and the board of directors. It does not provide detailed instructions or processes. A departmental risk management framework, on the other hand, focuses on specific procedures and strategies at the departmental level.

24. D — Risk analyst
A risk analyst is responsible for the continuous assessment and mitigation of cybersecurity risks. This role involves identifying vulnerabilities and potential threats, and implementing appropriate measures to safeguard organizational information systems.

25. B — Common risk perspective
Answer: Common risk perspective A common risk perspective allows an organization to uniformly establish risk appetite levels throughout the enterprise, ensuring a balanced risk portfolio and posture.

26. A — Informed
Answer: Informed Individuals whose role is to be informed are generally senior management or the Board of Directors. While they do not have direct input or involvement in the delivery of IT compliance activities, it is very important that they are informed of the actions taken and the end result.

27. C — Operational risk assessment
Answer: Operational risk assessment The operational risk assessment method focuses on specific functions and operations within individual business units. It aims to identify risks that could impact particular areas of the organization.

28. B — Catalog IT assets
Answer: Catalog IT assets The primary function of an asset register in an IT risk management framework is to catalog IT assets. This includes details like the owner, value, location, and significance of each asset to manage and mitigate risks effectively.

29. D — On-premises
Answer: On-premises On-premises network architecture allows organizations to manage and maintain their

own networking hardware and software. Organizations have complete control over their network infrastructure.

30. B — Historical
Risk practitioners can use historical methods, which are also known as evidence-based methods. Historical information such as past project outcomes, feedback from stakeholders, and performance data provides empirical evidence that can be used to forecast potential risks going forward.

Ready to pass?

Unlock the full CRISC IT Risk Exam Prep bank, every explanation, and unlimited timed mock exams.

Scan to start practising
https://certs.theorypractice.app/crisc

Also on iOS & Android — search your exam name on the App Store or Google Play