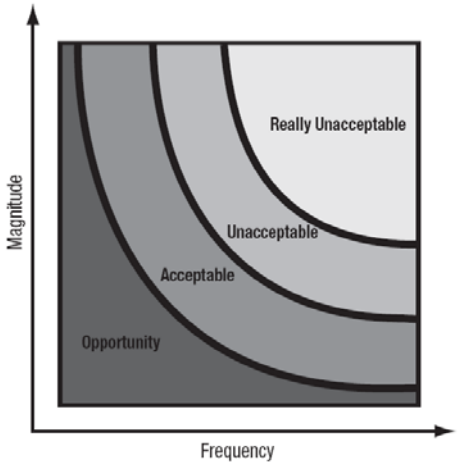
ISACA CRISC Practice Questions

1. What do different risk scenarios on the same bands/curve on a risk map indicate?



   A. All risk scenarios on the same curve of a risk map have the same level of risk.
   B. All risk scenarios on the same curve of a risk map have the same magnitude of impact.
   C. All risk scenarios on the same curve of a risk map require the same risk response.
   D. All risk scenarios on the same curve of a risk map are of the same type.

2. A business case developed to support risk mitigation efforts for a complex application development project should be retained until:
   A. the project is approved.
   B. user acceptance of the application.
   C. the application is deployed.
   D. the application's end of life.

3. Prior to releasing an operating system security patch into production, a leading practice is to have the patch:
   A. applied simultaneously to all systems.
   B. procured from an approved vendor.
   C. tested in a preproduction test environment.
   D. approved by business stakeholders.

4. Risk assessment techniques should be used by a risk practitioner to:
   A. maximize the return on investment (ROI).
   B. provide documentation for auditors and regulators.
   C. justify the selection of risk mitigation strategies.
   D. quantify the risk that would otherwise be subjective.

5. Which of the following information in the risk register **BEST** helps in developing proper risk scenarios? A list of:
   A. potential threats to assets.
   B. residual risk on individual assets.
   C. accepted risk.
   D. security incidents.

6. Despite a comprehensive security awareness program annually undertaken and assessed for all staff and contractors, an enterprise has experienced a breach through a spear phishing attack. What is the **MOST** effective way to improve security awareness?
   A. Review the security awareness program and improve coverage of social engineering threats.
   B. Launch a disciplinary process against the people who leaked the information.
   C. Perform a periodic social engineering test against all staff and communicate summary results to the staff.
   D. Implement a data loss prevention system that automatically points users to corporate policies.

7. A risk practitioner has collected several IT-related key risk indicators (KRIs) related for the core financial application. These would **MOST** likely be reported to:
   A. stakeholders.
   B. the IT administrator group.
   C. the finance department.
   D. senior management.

8. An enterprise is hiring a consultant to help determine the maturity level of the risk management program. The **MOST** important element of the request for proposal (RFP) is the:
   A. sample deliverable.
   B. past experience of the engagement team.
   C. methodology used in the assessment.
   D. references from other organizations.

9. Which of the following **BEST** addresses the risk of data leakage?
   A. Incident response procedures
   B. File backup procedures
   C. Acceptable use policies (AUPs)
   D. Database integrity checks

10. Which of the following is the **GREATEST** benefit of a risk-aware culture?
    A. Issues are escalated when suspicious activity is noticed.
    B. Controls are double-checked to anticipate any issues.
    C. Individuals communicate with peers for knowledge sharing.
    D. Employees are self-motivated to learn about costs and benefits.

11. The IT department wants to use a server for an enterprise database, but the server hardware is not certified by the operating system (OS) or the database vendor. A risk practitioner determines that the use of the database presents:
    A. a minimal level of risk.
    B. an unknown level of risk.
    C. a medium level of risk.
    D. a high level of risk.

12. Which type of cost incurred is used when leveraging existing network cabling for an IT project?
    A. Indirect cost
    B. Infrastructure cost
    C. Project cost
    D. Maintenance cost

13. Which of the following is of **MOST** concern in a review of a virtual private network (VPN) implementation? Computers on the network are located:
    A. at the enterprise's remote offices.
    B. on the enterprise's internal network.
    C. at the backup site.
    D. in employees' homes

14. An enterprise is expanding into new nearby domestic locations (office park). Which of the following is **MOST** important for a risk practitioner to report on?
    A. Competitor analysis
    B. Legal and regulatory requirements
    C. Political issues
    D. The potential of natural disasters

15. The **MOST** effective method to conduct a risk assessment on an internal system in an organization is to start by understanding the:
    A. performance metrics and indicators.
    B. policies and standards.
    C. recent audit findings and recommendations.
    D. system and its subsystems.

16. Which of the following is the **BEST** indicator that incident response training is effective?
    A. Decreased reporting of security incidents to the incident response team
    B. Increased reporting of security incidents to the incident response team
    C. Decreased number of password resets
    D. Increased number of identified system vulnerabilities

17. Which of the following approaches is the **BEST** approach to exception management?
    A. Escalation processes are defined.
    B. Process deviations are not allowed.
    C. Decisions are based on business impact.
    D. Senior management judgment is required.

18. Which of the following is the **BEST** way to ensure that an accurate risk register is maintained over time?
    A. Monitor key risk indicators (KRIs), and record the findings in the risk register.
    B. Publish the risk register centrally with workflow features that periodically poll risk assessors.
    C. Distribute the risk register to business process owners for review and updating.
    D. Utilize audit personnel to perform regular audits and to maintain the risk register.

19. A substantive test to verify that tape library inventory records are accurate is:
    A. determining whether bar code readers are installed.
    B. conducting a physical count of the tape inventory.
    C. checking whether receipts and issues of tapes are accurately recorded.
    D. determining whether the movement of tapes is authorized.

20. Which of the following is **MOST** important for measuring the effectiveness of a security awareness program?
    A. Increased interest in focus groups on security issues
    B. A reduced number of security violation reports
    C. A quantitative evaluation to ensure user comprehension
    D. An increased number of security violation reports

21. Which of the following should management use to allocate resources for risk response?
    A. Audit report findings
    B. Penetration test results
    C. Risk analysis results
    D. Vulnerability test results

22. Which of the following is used to determine whether unauthorized modifications were made to production programs?
    A. An analytical review
    B. Compliance testing
    C. A system log analysis
    D. A forensic analysis

23. Which of the following **MOST** effectively ensures that service provider controls are within the guidelines set forth in the organization's information security policy?
    A. Service level monitoring
    B. Penetration testing
    C. Security awareness training
    D. Periodic auditing

24. Which of the following is **MOST** relevant to include in a cost-benefit analysis of a two-factor authentication system?
    A. The approved budget of the project
    B. The frequency of incidents
    C. The annual loss expectancy (ALE) of incidents
    D. The total cost of ownership (TCO)

25. The board of directors wants to know the financial impact of specific, individual risk scenarios. What type of approach is **BEST** suited to fulfill this requirement?
    A. Delphi method
    B. Quantitative analysis
    C. Qualitative analysis
    D. Financial risk modeling

26. Which of the following is **MOST** important for effective risk management?
    A. Assignment of risk owners to identified risk
    B. Ensuring compliance with regulatory requirements
    C. Integration of risk management into operational processes
    D. Implementation of a risk avoidance strategy

27. Previously accepted risk should be:
    A. reassessed periodically because the risk can be escalated to an unacceptable level due to revised conditions.
    B. removed from the risk log once it is accepted.
    C. accepted permanently because management has already spent resources (time and labor) to conclude that the risk level is acceptable.
    D. avoided next time because risk avoidance provides the best protection to the enterprise.

28. Which of the following **BEST** describes the risk-related roles and responsibilities of an organizational business unit (BU)? The BU management team:
    A. owns the mitigation plan for the risk belonging to their BU, while board members are responsible for identifying and assessing risk as well as reporting on that risk to the appropriate support functions.
    B. owns the risk and is responsible for identifying, assessing and mitigating risk as well as reporting on that risk to the appropriate support functions and the board of directors.
    C. carries out the respective risk-related responsibilities, but ultimate accountability for the day-to-day work of risk management and goal achievement belongs to the board members.
    D. is ultimately accountable for the day-to-day work of risk management and goal achievement, and board members own the risk.

29. Information that is no longer required to support the main purpose of the business from an information security perspective should be:
    A. analyzed under the retention policy.
    B. protected under the information classification policy.
    C. analyzed under the backup policy.
    D. protected under the business impact analysis (BIA).

30. If risk has been identified, but not yet mitigated, the enterprise would:
    A. record and mitigate serious risk and disregard low-level risk.
    B. obtain management commitment to mitigate all identified risk within a reasonable time frame.
    C. document all risk in the risk register and maintain the status of the remediation.
    D. conduct an annual risk assessment, but disregard previous assessments to prevent risk bias.

31. The **PRIMARY** benefit of using a maturity model to assess the enterprise's data management process is that it:
    A. can be used for benchmarking.
    B. helps identify gaps.
    C. provides goals and objectives.
    D. enforces continuous improvement.

32. Which of the following provides the **BEST** view of risk management?
    A. An interdisciplinary team
    B. A third-party risk assessment service provider
    C. The enterprise's IT department
    D. The enterprise's internal compliance department

33. Which of the following is minimized when acceptable risk is achieved?
    A. Transferred risk
    B. Control risk
    C. Residual risk
    D. Inherent risk

34. Risk assessments are **MOST** effective in a software development organization when they are performed:
    A. before system development begins.
    B. during system deployment.
    C. during each stage of the system development life cycle (SDLC).
    D. before developing a business case.

35. When requesting information for an e-discovery, an enterprise learned that their email cloud provider was never contracted to back up the messages even though the company's email retention policy explicitly states that all emails are to be saved for three years. Which of the following would have **BEST** safeguarded the company from this outcome?
    A. Providing the contractor with the record retention policy up front
    B. Validating the company policies to the provider's contract
    C. Providing the contractor with the email retention policy up front
    D. Backing up the data on the company's internal network nightly

36. Which of the following is the **BEST** approach when conducting an IT risk awareness campaign?
    A. Provide technical details on exploits.
    B. Provide common messages tailored for different groups.
    C. Target system administrators and help desk staff.
    D. Target senior managers and business process owners.

37. Who grants formal authorization for user access to a protected file?
    A. The process owner
    B. The system administrator
    C. The data owner
    D. The security manager

38. A risk response report includes recommendations for:
    A. acceptance.
    B. assessment.
    C. evaluation.
    D. quantification.

39. The likelihood of an attack being launched against an enterprise is **MOST** dependent on:
    A. the skill and motivation of the potential attacker.
    B. the frequency that monitoring systems are reviewed.
    C. the ability to respond quickly to any incident.
    D. the effectiveness of the controls.

40. Which of the following measures is **MOST** effective against insider threats to confidential information?
    A. Audit trail monitoring
    B. A privacy policy
    C. Role-based access control (RBAC)
    D. Defense in depth

41. Which of the following would **PRIMARILY** help an enterprise select and prioritize risk responses?
    A. A cost-benefit analysis of available risk mitigation options
    B. The level of acceptable risk per risk appetite
    C. The potential to transfer or eliminate the risk
    D. The number of controls necessary to reduce the risk

42. Risk assessments should be repeated at regular intervals because:
    A. omissions in earlier assessments can be addressed.
    B. periodic assessments allow various methodologies.
    C. business threats are constantly changing.
    D. they help raise risk awareness among staff.

43. Which type of risk assessment methods involves conducting interviews and using anonymous questionnaires by subject matter experts?
    A. Quantitative
    B. Probabilistic
    C. Monte Carlo
    D. Qualitative

44. Which of the following is the **MOST** important information to include in a risk management strategic plan?
    A. Risk management staffing requirements
    B. The risk management mission statement
    C. Risk mitigation investment plans
    D. The current state and desired future state

45. When a significant vulnerability is discovered in the security of a critical web server, immediate notification should be made to the:
    A. development team to remediate.
    B. data owners to mitigate damage.
    C. system owner to take corrective action.
    D. incident response team to investigate.

46. Who is accountable for business risk related to IT?
    A. The chief information officer (CIO)
    B. The chief financial officer (CFO)
    C. Users of IT services—the business
    D. The chief architect

47. The **PRIMARY** reason for developing an enterprise security architecture is to:
    A. align security strategies between the functional areas of an enterprise and external entities.
    B. build a barrier between the IT systems of an enterprise and the outside world.
    C. help with understanding of the enterprise's technologies and the interactions between them.
    D. protect the enterprise from external threats and proactively monitor the corporate network.

48. Which of the following **MOST** enables risk-aware business decisions?
    A. Robust information security policies
    B. An exchange of accurate and timely information
    C. Skilled risk management personnel
    D. Effective process controls

49. Which of the following is **MOST** critical when system configuration files for a critical enterprise application system are being reviewed?
    A. Configuration files are frequently changed.
    B. Changes to configuration files are recorded.
    C. Access to configuration files is not restricted.
    D. Configuration values do not impact system efficiency.

50. The **BEST** method for detecting and monitoring a hacker's activities without exposing information assets to unnecessary risk is to utilize:
    A. firewalls.
    B. bastion hosts.
    C. honeypots.
    D. screened subnets.

51. Which of the following devices should be placed within a demilitarized zone (DMZ)?
    A. An authentication server
    B. A mail relay
    C. A firewall
    D. A router

52. Which of the following statements **BEST** describes the value of a risk register?
    A. It captures the risk inventory.
    B. It drives the risk response plan.
    C. It is a risk reporting tool.
    D. It lists internal risk and external risk.

53. Which of the following activities provides the **BEST** basis for establishing risk ownership?
    A. Documenting interdependencies between departments
    B. Mapping identified risk to a specific business process
    C. Referring to available RACI charts
    D. Distributing risk equally among all asset owners

54. What is the **FIRST** step for a risk practitioner when an enterprise has decided to outsource all IT services and support to a third party?
    A. Validate that the internal systems of the service provider are secure.
    B. Enforce the regulations and standards associated with outsourcing data management for restrictions on transborder data flow.
    C. Ensure that security requirements are addressed in all contracts and agreements.
    D. Build a business case to perform an onsite audit of the third-party vendor.

55. Which of the following should be of **MOST** concern to a risk practitioner?
    A. Failure to notify the public of an intrusion
    B. Failure to notify the police of an attempted intrusion
    C. Failure to internally report a successful attack
    D. Failure to examine access rights periodically

56. A company is confident about the state of its organizational security and compliance program. Many improvements have been made since the last security review was conducted one year ago. What should the company do to evaluate its current risk profile?
    A. Review previous findings and ensure that all issues have been resolved.
    B. Conduct follow-up audits in areas that were found deficient in the previous review.
    C. Monitor the results of the key risk indicators (KRIs) and use those to develop targeted assessments.
    D. Perform a new enterprise risk assessment using an independent expert.

57. The cost of mitigating a risk should not exceed the:
    A. expected benefit to be derived.
    B. annual loss expectancy (ALE).
    C. value of the physical asset.
    D. cost to exploit the weakness.

58. Which of the following approaches to corporate policy **BEST** supports an enterprise's expansion to other regions, where different local laws apply?
    A. A global policy that does not contain content that might be disputed at a local level
    B. A global policy that is locally amended to comply with local laws
    C. A global policy that complies with law at corporate headquarters and that all employees must follow
    D. Local policies to accommodate laws within each region

59. Which of the following **BEST** ensures that identified risk is kept at an acceptable level?
    A. Reviewing of the controls periodically, according to the risk action plan
    B. Listing each risk as a separate entry in the risk register
    C. Creating a separate risk register for every department
    D. Maintaining a key risk indicator (KRI) for assets in the risk register

60. What is the **MOST** important reason for periodically testing controls?
    A. To meet regulatory requirements
    B. To meet due care requirements
    C. To ensure that control objectives are met
    D. To achieve compliance with standard policy

61. The **MOST** important objective of regularly testing information system controls is to:
    A. identify design flaws, failures and redundancies.
    B. provide the necessary evidence to support management assertions.
    C. assess the control risk and formulate an opinion on the level of reliability.
    D. evaluate the need for a risk assessment and indicate the corrective action(s) to be taken, where applicable.

62. It is **MOST** important that risk appetite be aligned with business objectives to ensure that:
    A. resources are directed toward areas of low risk tolerance.
    B. major risk is identified and eliminated.
    C. IT and business goals are aligned.
    D. the risk strategy is adequately communicated.

63. Who is **MOST** likely responsible for data classification?
    A. The data user
    B. The data owner
    C. The data custodian
    D. The system administrator

64. A global financial institution has decided not to take any further action on a denial-of-service (DoS) vulnerability found by the risk assessment team. The **MOST** likely reason for making this decision is that:
    A. the needed countermeasure is too complicated to deploy.
    B. there are sufficient safeguards in place to prevent this risk from happening.
    C. the likelihood of the risk occurring is unknown.
    D. the cost of countermeasure outweighs the value of the asset and potential loss.

65. What role does the risk professional have in regard to the IS control monitoring process? The risk professional:
    A. maintains and operates IS controls.
    B. approves the policies for IS control monitoring.
    C. determines the frequency of control testing by internal audit.
    D. assists in planning, reporting and scheduling tests of IS controls.

66. It is **MOST** important for risk mitigation to:
    A. eliminate threats and vulnerabilities.
    B. reduce the likelihood of risk occurrence.
    C. reduce risk within acceptable cost.
    D. reduce inherent risk to zero.

67. The goal of IT risk analysis is to:
    A. enable the alignment of IT risk management with enterprise risk management (ERM).
    B. enable the prioritization of risk responses.
    C. satisfy legal and regulatory compliance requirements.
    D. identify known threats and vulnerabilities to information assets.

68. A risk assessment indicates a risk to the enterprise that exceeds the risk acceptance level set by senior management. What is the **BEST** way to address this risk?
    A. Ensure that the risk is quickly brought within acceptable limits, regardless of cost.
    B. Recommend mitigating controls if the cost and/or benefit would justify the controls.
    C. Recommend that senior management revise the risk acceptance level.
    D. Ensure that risk calculations are performed to revalidate the controls.

69. Once a risk assessment has been completed, the documented test results should be:
    A. destroyed.
    B. retained.
    C. summarized.
    D. published.

70. What is the **MOST** effective method to evaluate the potential impact of legal, regulatory and contractual requirements on business objectives?
    A. A compliance-oriented gap analysis
    B. Interviews with business process stakeholders
    C. A mapping of compliance requirements to policies and procedures
    D. A compliance-oriented business impact analysis (BIA)

71. Which of the following metrics is the **MOST** useful in measuring the monitoring of violation logs?
    A. Penetration attempts investigated
    B. Violation log reports produced
    C. Violation log entries
    D. Frequency of corrective actions taken

72. After a risk assessment study, a bank with global operations decided to continue doing business in certain regions of the world where identity theft is widespread. To **MOST** effectively deal with the risk, the business should:
    A. implement monitoring techniques to detect and react to potential fraud.
    B. make the customer liable for losses if the customer fails to follow the bank's advice.
    C. increase its customer awareness efforts in those regions.
    D. outsource credit card processing to a third party.

73. Which of the following provides the formal authorization on user access?
    A. Database administrator
    B. Data owner
    C. Process owner
    D. Data custodian

74. An enterprise expanded operations into Europe, Asia and Latin America. The enterprise has a single-version, multiple-language employee handbook last updated three years ago. Which of the following is of **MOST** concern?
    A. The handbook may not have been correctly translated into all languages.
    B. Newer policies may not be included in the handbook.
    C. Expired policies may be included in the handbook.
    D. The handbook may violate local laws and regulations.

75. Which of the following is **MOST** important to determine when defining risk management strategies?
    A. Risk assessment criteria
    B. IT architecture complexity
    C. An enterprise disaster recovery plan (DRP)
    D. Organizational objectives