Q.No.1 Which of the following is MOST important for an organization that wants to reduce IT operational risk?

A. Increasing senior management's understanding of IT operations
B. Increasing the frequency of data backups
C. Minimizing complexity of IT infrastructure
D. Decentralizing IT infrastructure

Answer: C

Q.No.2 Deviation from a mitigation action plan's completion date should be determined by which of the following?

A. Benchmarking analysis with similar completed projects
B. Change management as determined by a change control board
C. The risk owner as determined by risk management processes
D. Project governance criteria as determined by the project office

Answer: C

Q.No.3 A business unit has decided to accept the risk of implementing an off-the-shelf, commercial software package that uses weak password controls. What is the BEST course of action?

A. Continue the implementation with no changes.
B. Obtain management approval for policy exception.
C. Select another application with strong password controls.
D. Develop an improved password software routine.

Answer: D

Q.No.4 Which of the following is the PRIMARY reason to have the risk management process reviewed by a third party?

A. Validate the threat management process.
B. Obtain objective assessment of the control environment
C. Ensure the risk profile is defined and communicated.
D. Obtain an objective view of process gaps and systemic errors.

Answer: B

Q.No.5 In an organization dependent on data analytics to drive decision-making, which of the following would BEST help to minimize the risk associated with inaccurate data?

A. Periodically reviewing big data strategies
B. Evaluating each of the data sources for vulnerabilities
C. Establishing an intellectual property agreement
D. Benchmarking to industry best practice

Answer: B

Q.No.6 Which of the following is MOST appropriate to prevent unauthorized retrieval of confidential information stored in a business application system?

A. Implement segregation of duties.
B. Enforce an internal data access policy.
C. Apply single sign-on for access control.
D. Enforce the use of digital signatures.

Answer: B

Q.No.7 The GREATEST concern when maintaining a risk register is that:

A. significant changes in risk factors are excluded.
B. impacts are recorded in qualitative terms.
C. executive management does not perform periodic reviews.
D. IT risk is not linked with IT assets,

Answer: A

Q.No.8 Which of the following will BEST help in communicating strategic risk priorities?

A. Heat map
B. Business impact analysis (BIA)
C. Balanced Scorecard
D. Risk register

Answer: C

Q.No.9 Which of the following is the BEST indicator of the effectiveness of a control action plan's implementation?

A. Stakeholder commitment
B. Increased risk appetite
C. Reduced risk level
D. Increased number of controls

Answer: C

Q.No.10 Which of the following is the BEST method for identifying vulnerabilities?

A. Batch job failure monitoring
B. Periodic network scanning
C. Risk assessments
D. Annual penetration testing

Answer: D

Q.No.11 Which of the following will BEST ensure that information security risk factors are mitigated when developing in-house applications?

A. Design key performance indicators (KPIs) for security in system specifications.
B. Include information security control specifications in business cases.
C. Identify key risk indicators (KRIs) as process output
D. Identify information security controls in the requirements analysis

Answer: D

Q.No.12 A management team is on an aggressive mission to launch a new product to penetrate new markets and overlooks IT risk factors, threats, and vulnerabilities. This scenario BEST demonstrates an organization's risk:

A. Tolerance.
B. culture.
C. Management.
D. analysis.

Answer: B

Q.No.13 During a control review, the control owner states that an existing control has deteriorated over time. What is the BEST recommendation to the control owner?

A. Discuss risk mitigation options with the risk owner.

B. Escalate the issue to senior management
C. Implement compensating controls to reduce residual risk.
D. Certify the control after documenting the concern.

Answer: C

Q.No.14 Which of the following is the BEST approach for determining whether a risk action plan is effective?

A. Assessing changes in residual risk
B. Comparing the remediation cost against budget
C. Assessing the inherent risk
D. Monitoring changes of key performance indicators (KPIs)

Answer: A

Q.No.15 Who is responsible for IT security controls that are outsourced to an external service provider?

A. Organization's information security manager
B. Organization's risk function
C. Service provider's IT management
D. Service provider's information security manager

Answer: B

Q.No.16 Which of the following approaches will BEST help to ensure the effectiveness of risk awareness training?

A. Piloting courses with focus groups
B. Using reputable third-party training programs
C. Reviewing content with senior management
D. Creating modules for targeted audiences

Answer: D

Q.No.17 A PRIMARY advantage of involving business management in evaluating and managing risk is that management:

A. is more objective than risk management
B. better understands the system architecture.

C. can balance technical and business risk.
D. can make better-informed business decisions.

Answer: D

Q.No.18 When reviewing a risk response strategy, senior management's PRIMARY focus should be placed on the:

A. cost-benefit analysis.
B. key performance indicators (KPIs).
C. investment portfolio
D. alignment with risk appetite.

Answer: D

Q.No.19 The effectiveness of a control has decreased. What is the MOST likely effect on the associated risk?

A. The risk impact changes.
B. The risk classification changes.
C. The inherent risk changes.
D. The residual risk changes.

Answer: D

Q.No.20 The BEST way to obtain senior management support for investment in a control implementation would be to articulate the reduction in:

A. Vulnerabilities
B. residual risk.
C. inherent risk.
D. detected incidents.

Answer: C

Q.No.21 During an IT department reorganization, the manager of a risk mitigation action plan was replaced. The new manager has begun implementing a new control after identifying a more effective option. Which of the following is the risk practitioner's BEST course of action?

A. Communicate the decision to the risk owner for approval.
B. Modify the action plan in the risk register.

C. Identify an owner for the new control.
D. Seek approval from the previous action plan manager.

Answer: A

Q.No.22 An organization is planning to acquire a new financial system. Which of the following stakeholders would provide the MOST relevant information for analyzing the risk associated with the new IT solution?

A. Internal auditor
B. Process owner
C. Project sponsor
D. Risk manager

Answer: B

Q.No.23 Which of the following is MOST important to sustainable development of secure IT services?

A. Security training for systems development staff
B. \Well-documented business cases
C. Security architecture principles
D. Secure coding practices

Answer: C

Q.No.24 An organization has outsourced a critical process involving highly regulated data to a third party with servers located in a foreign country. Who is accountable for the confidentiality of this data?

A. Third-party data custodian
B. Data custodian
C. Regional office executive
D. Data owner

Answer: D

Q.No.25 Which of the following would qualify as a key performance indicator (KPD)?

A. Aggregate risk of the organization
B. Number of attacks against the organization's website

C. Number of exception requests processed in the past 90 days
D. Number of identified system vulnerabilities

Answer: D

Q.No.26 When reviewing a report on the performance of control processes, it is MOST important to verify whether the:

A. control process is designed effectively,
B. residual risk objectives have been achieved.
C. business process objectives have been met
D. control adheres to regulatory standards.

Answer: D

Q.No.27 "Read" rights to application files in a controlled server environment should be approved by the:

A. systems administrator.
B. database administrator.
C. chief information officer.
D. business process owner.

Answer: D

Q.No.28 The MAIN purpose of a risk register is to:

A. enable well-informed risk management decisions.
B. promote an understanding of risk across the organization
C. document the risk universe of the organization.
D. identify stakeholders associated with risk scenarios.

Answer: A

Q.No.29 Which of the following is the BEST way to identify changes in the risk profile of an organization?

A. Conduct a gap analysis.
B. Monitor key performance indicators (KPIs).
C. Monitor key risk indicators (KRIs).
D. Interview the risk owner.

Answer: A

Q.No.30 An organization is making significant changes to an application. At what point should the application risk profile be updated?

A. After user acceptance testing (UAT)
B. Upon release to production
C. During backlog scheduling
D. When reviewing functional requirements

Answer: D

Q.No.31 Which of the following should be considered FIRST when assessing risk associated with the adoption of emerging technologies?

A. Organizational strategy
B. Cost-benefit analysis
C. Control self-assessment (CSA)
D. Business requirements

Answer: A

Q.No.32 The PRIMARY benefit of conducting continuous monitoring of access controls is the ability to identify:

A. possible noncompliant activities that lead to data disclosure.
B. unknown threats to undermine existing access controls.
C. leading or lagging key risk indicators (KRIS).
D. inconsistencies between security policies and procedures.

Answer: A

Q.No.33 Which of the following MOST effectively limits the impact of a ransomware attack?

A. Cyber insurance
B. Cryptocurrency reserve
C. Data backups
D. End user training

Answer: C

Q.No.34 To communicate the risk associated with IT in business terms, which of the following MUST be defined?

A. Compliance objectives
B. Organizational objectives
C. Risk appetite of the organization
D. Inherent and residual risk

Answer: B

Q.No.35 Which of the following is the MOST important objective of embedding risk management practices into the initiation phase of the project management life cycle?

A. To deliver projects on time and on budget
B. To assess inherent risk
C. To include project risk in the enterprise-wide IT risk profit.
D. To assess risk throughout the project

Answer: D

Q.No.36 To help identify high-risk situations, an organization should:

A. maintain a risk matrix.
B. develop key performance indicators (KPIs).
C. maintain a risk register.
D. continuously monitor the environment.

Answer: D

Q.No.37 An organization operates in a jurisdiction where heavy fines are imposed for leakage of customer data. Which of the following provides the BEST input to assess the inherent risk impact?

A. Number of customer records held
B. Number of databases that host customer data
C. Number of encrypted customer databases
D. Number of staff members having access to customer data

Answer: B

Q.No.38 An organization's risk practitioner learns a new third-party system on the corporate network has introduced vulnerabilities that could compromise corporate IT systems. What should the risk practitioner do FIRST?

A. Confirm the vulnerabilities with the third party
B. Identify procedures to mitigate the vulnerabilities.
C. Notify information security management.
D. Request IT to remove the system from the network.

Answer: B

Q.No.39 Which of the following is the MOST important component of effective security incident response?

A. Network time protocol synchronization
B. Identification of attack sources
C. Early detection of breaches
D. A documented communications plan

Answer: C

Q.No.40 A control for mitigating risk in a key business area cannot be implemented immediately. Which of the following is the risk practitioner's BEST course of action when a compensating control needs to be applied?

A. Record the risk as accepted in the risk register.
B. Obtain the risk owner's approval.
C. Inform senior management.
D. Update the risk response plan.

Answer: B

Q.No.41 Which of the following provides the BEST measurement of an organization's risk management maturity level?

A. Level of residual risk
B. IT alignment to business objectives
C. The results of a gap analysis
D. Key risk indicators (KRIS)

Answer: B

Q.No.42 The BEST key performance indicator (KPI) for monitoring adherence to an organization's user accounts provisioning practices is the percentage of:

A. accounts without documented approval.
B. user accounts with default passwords.
C. active accounts belonging to former personnel.
D. accounts with dormant activity.

Answer: A

Q.No.43 A recent audit identified high-risk issues in a business unit though a previous control self-assessment (CSA) had good results. Which of the following is the MOST likely reason for the difference?

A. The audit had a broader scope than the CSA.
B. The CSA was not sample-based.
C. The CSA did not test control effectiveness.
D. The CSA was compliance-based, while the audit was risk-based.

Answer: D

Q.No.44 Which of the following is the MOST relevant information to include in a risk management strategy?

A. Cost of controls
B. Quantified risk triggers\
C. Regulatory requirements
D. Organizational goals

Answer: D

Q.No.45 A risk assessment indicates the residual risk associated with a new bring your own device (BYOD) program is within organizational risk tolerance. Which of the following should the risk practitioner recommend be done NEXT?

A. Implement targeted awareness training for new BYOD users.
B. Implement monitoring to detect control deterioration
C. Identify log sources to monitor BYOD usage and risk impact.
D. Reduce the risk tolerance level.

Answer: B

Q.No.46 The MOST significant benefit of using a consistent risk ranking methodology across an organization is that it enables:

A. allocation of available resources.
B. assignment of risk to the appropriate owners.
C. clear understanding of risk levels.
D. risk to be expressed in quantifiable terms.

Answer: C

Q.No.47 Which of the following is an IT business owner's BEST course of action following an unexpected increase in emergency changes?

A. Evaluating the impact to control objectives
B. Reconfiguring the IT infrastructure
C. Validating the adequacy of current processes
D. Conducting a root cause analysis

Answer: D

Q.No.48 Who is MOST likely to be responsible for the coordination between the IT risk strategy and the business risk strategy?

A. Internal audit director
B. Information security director
C. Chief financial officer (CFO)
D. Chief information officer (CIO)

Answer: B

Q.No.49 A risk practitioner has identified that the organization's secondary data center does not provide redundancy for a critical application Who should have the authority to accept the associated risk?

A. Business application owner
B. Data center manager
C. Disaster recovery manager
D. Business continuity director

Answer: A

Q.No.50 A risk practitioner discovers several key documents detailing the design of a product currently in development have been posted on the Internet. What should be the risk practitioner's FIRST course of action?

A. Inform internal audit.
B. Perform a root cause analysis.
C. Conduct an immediate risk assessment
D. Invoke the established incident response plan.

Answer: D

Q.No.51 A change management process has recently been updated with new testing procedures. What is the NEXT course of action?

A. Communicate to those who test and promote changes.
B. Monitor processes to ensure recent updates are being followed.
C. Conduct a cost-benefit analysis to justify the cost of the control.
D. Assess the maturity of the change management process.

Answer: B

Q.No.52 Which of the following is the BEST way to confirm whether appropriate automated controls are in place within a recently implemented system?

A. Conduct user acceptance testing (UAT).
B. Review the key performance indicators (KPIs).
C. Interview process owners.
D. Perform a post-implementation review.

Answer: B

Q.No.53 An IT control gap has been identified in a key process. Who would be the MOST appropriate owner of the risk associated with this gap?

A. Operational risk manager\
B. Chief information security officer (CISO)
C. Key control owner
D. Business process owner

Answer: D

Q.No.54 A risk practitioner is reviewing the status of an action plan to mitigate an emerging IT risk and finds the risk level has increased. What is the BEST course of action?

A. Evaluate whether selected controls are still appropriate.
B. Revise the action plan to include additional mitigating controls.
C. Implement the planned controls and accept the remaining risk.
D. Suspend the current action plan in order to reassess the risk.

Answer: A

Q.No.55 For no apparent reason, the time required to complete daily processing for a legacy application is approaching a risk threshold. Which of the following activities should be performed FIRST?

A. Conduct a root-cause analysis.
B. Temporarily increase the risk threshold.
C. Suspend processing to investigate the problem.
D. Initiate a feasibility study for a new application.

Answer: A

Q.No.56 Which of the following is the MOST effective key performance indicator (KPI) for change management?

A. Percentage of successful changes
B. Percentage of changes with a fallback plan
C. Average time required to implement a change
D. Number of changes implemented

Answer: A

Q.No.57 An organization's IT infrastructure is running end-of-life software that is not allowed without exception approval. Which of the following would provide the MOST helpful information to justify investing in updated software?

A. The balanced Scorecard
B. The risk management framework
C. A roadmap of IT strategic planning
D. A cost-benefit analysis

Answer: D

Q.No.58 Which of the following approaches BEST identifies information systems control deficiencies?

A. Gap analysis
B. Countermeasures analysis
C. Best practice assessment
D. Risk assessment

Answer: A

Q.No.59 A large organization needs to report risk at all levels for a new centralized virtualization project to reduce cost and improve performance. Which of the following would MOST effectively represent the overall risk of the project to senior management?

A. Centralized risk register
B. Key risk indicators (KRIS)
C. Aggregated key performance indicators (KPIs)
D. Risk heat map

Answer: D

Q.No.60 The annualized loss expectancy (ALE) method of risk analysis:

A. uses qualitative risk rankings such as low, medium, and high.
B. can be used in a cost-benefit analysis.
C. helps in calculating the expected cost of controls.
D. can be used to determine the indirect business impact.

Answer: B

Q.No.61 Which of the following is the PRIMARY objective of providing an aggregated view of IT risk to business management?

A. To enable consistent data on risk to be obtained
B. To provide consistent and dear terminology
C. To allow for proper review of risk tolerance
D. To identify dependencies for reporting risk

Answer: D

Q.No.62 Which of the following is the BEST way to determine whether new controls mitigate security gaps in a business system?

A. Perform a vulnerability assessment
B. Conduct a compliance check against standards.
C. Measure the change in inherent risk.
D. Complete an offsite business continuity exercise.

Answer: A

Q.No.63 Which of the following is the PRIMARY benefit of using an entry in the risk register to track the aggregate risk associated with server failure?

A. It provides historical information about the impact of individual servers malfunctioning,
B. It provides a cost-benefit analysis on control options available for implementation
C. It provides a comprehensive view of the impact should the servers simultaneously fail.
D. It provides a view on where controls should be applied to maximize the uptime of Servers.

Answer: C

Q.No.64 Which of the following should be a risk practitioner's MOST important consideration when developing IT risk scenarios?

A. Linkage of identified risk scenarios with enterprise risk management
B. The impact of controls on the efficiency of the business in delivering services
C. Potential threats and vulnerabilities that may have an impact on the business
D. Results of network vulnerability scanning and penetration testing hos

Answer: C

Q.No.65 Which of the following is the BEST way to promote adherence to the risk tolerance level set by management?

A. Increasing organizational resources to mitigate risks
B. Defining expectations in the enterprise risk policy
C. Communicating external audit results
D. Avoiding risks that could materialize into substantial losses

Answer: B

Q.No.66 An organization has opened a subsidiary in a foreign country. Which of the following would be the BEST way to measure the effectiveness of the subsidiary's IT systems controls?

A. Review design documentation of IT systems.
B. Implement IT systems in alignment with business objectives.
C. Review metrics and key performance indicators (KPIs).
D. Evaluate compliance with legal and regulatory requirements.

Answer: D

Q.No.67 Which of the following is MOST essential for an effective change control environment?

A. IT management review of implemented changes
B. Business management approval of change requests
C. Requirement of an implementation rollback plan
D. Separation of development and production environments

Answer: B

Q.No.68 Which of the following is MOST important to have in place to ensure the effectiveness of risk and security metrics reporting?

A. Organizational reporting process
B. Incident reporting procedures
C. Regularly scheduled audits
D. Incident management policy

Answer: A

Q.No.69 The PRIMARY benefit of classifying information assets is that it helps to:

A. communicate risk to senior management
B. assign risk ownership
C. facilitate internal audit
D. determine the appropriate level of control.

Answer: D

Q.No.70 A payroll manager discovers that fields in certain payroll reports have been modified without authorization. Which of the following control weaknesses could have contributed MOST to this problem?

A. The user requirements were not documented.
B. Payroll files were not under the control of a librarian.
C. The programmer had access to the production programs.
D. The programmer did not involve the user in testing.

Answer: B

Q.No.71 An organization's HR department has implemented a policy requiring staff members to take a minimum of five consecutive days leave per year to mitigate the risk of malicious insider activities. Which of the following is the BEST key performance indicator (KPI) of the effectiveness of this policy?

A. Financial loss incurred due to malicious activities during staff members' leave
B. Number of malicious activities occurring during staff members' leave
C. Percentage of staff members seeking exception to the policy
D. Percentage of staff members taking leave according to the policy

Answer: C

Q.No.72 Which of the following is the PRIMARY reason to establish the root cause of an IT security incident?

A. Update the risk register.
B. Assign responsibility and accountability for the incident.
C. Prepare a report for senior management
D. Avoid recurrence of the incident

Answer: D

Q.No.73 During the risk assessment of an organization that processes credit cards, a number of existing controls have been found to be ineffective and do not meet industry standards. The overall control environment may still be effective if:

A. compensating controls are in place.
B. a control mitigation plan is in place.
C. risk management is effective.
D. residual risk is accepted.

Answer: A

Q.No.74 Which of the following is the MOST important information to be communicated during security awareness training?

A. Recent security incidents
B. Management's expectations
C. Corporate risk profile
D. The current risk management capability

Answer: B

Q.No.75 Which of the following will BEST help to ensure that information system controls are effective?

A. Implementing compensating controls
B. Testing controls periodically
C. Automating manual controls
D. Responding promptly to control exceptions

Answer: B

Q.No.76 Once a risk owner has decided to implement a control to mitigate risk, it is MOST important to develop:

A. a process for measuring and reporting control performance.
B. an alternate control design in case of failure of the identified control.
C. a process for bypassing control procedures in case of exceptions.
D. procedures to ensure the effectiveness of the control.

Answer: A

Q.No.77 After migrating a key financial system to a new provider, it was discovered that a developer could gain access to the production environment. Which of the following is the BEST way to mitigate the risk in this situation?

A. Escalate the issue to the service provider.
B. Re-certify the application access controls.
C. Remove the developer's access.
D. Review the results of pre-migration testing.

Answer: B

Q.No.78 The MOST effective approach to prioritize risk scenarios is by:

A. assessing impact to the strategic plan.
B. evaluating the cost of risk response.
C. aligning with industry best practices.
D. soliciting input from risk management experts,

Answer: A

Q.No.79 The acceptance of control costs that exceed risk exposure MOST likely demonstrates:

A. low risk tolerance.
B. high risk tolerance
C. corporate culture misalignment
D. corporate culture alignment

Answer: A

Q.No.80 An organization's chief technology officer (CTO) has decided to accept the risk associated with the potential loss from a denial-of-service (DoS) attack. In this situation, what is the risk practitioner's BEST course of action?

A. Recommend that the CTO revisit the risk acceptance decision
B. Validate the CTO's decision with the business process owner.
C. Identify key risk indicators (KRIs) for ongoing monitoring.
D. Update the risk register with the selected risk response.

Answer: C

Q.No.81 After identifying new risk events during a project the project manager's NEXT step should be to:

A. continue with a quantitative risk analysis.
B. record the scenarios into the risk register.
C. determine if the scenarios need to be accepted or responded to.
D. continue with a qualitative risk analysis.

Answer: B

Q.No.82 Which of the following is the GREATEST benefit to an organization when updates to the risk register are made promptly after the completion of a risk assessment?

A. Improved collaboration among risk professionals
B. Improved senior management communication
C. Optimized risk treatment decisions
D. Enhanced awareness of risk management

Answer: C

Q.No.83 Which of the following controls would BEST reduce the likelihood of a successful network attack through social engineering?

A. Employee sanctions
B. Automated controls
C. Security awareness training
D. Multifactor authentication

Answer: C

Q.No.84 Who should be accountable for monitoring the control environment to ensure controls are effective?

A. Risk owner
B. Security monitoring operations
C. Impacted data owner
D. System owner

Answer: A

Q.No.85 Which of the following techniques would be used during a risk assessment to demonstrate to stakeholders that all known alternatives were evaluated?

A. Decision tree
B. Control chart
C. Sensitivity analysis
D. Trend analysis

Answer: A

Q.No.86 The PRIMARY purpose of IT control status reporting is to:

A. assist internal audit in evaluating and initiating remediation efforts.
B. facilitate the comparison of the current and desired states.
C. benchmark IT controls with industry standards.
D. ensure compliance with IT governance strategy.

Answer: B

Q.No.87 Which of the following data would be used when performing a business impact analysis (BIA)?

A. Projected impact of current business on future business
B. Expected costs for recovering the business
C. Cost-benefit analysis of running the current business
D. Cost of regulatory compliance

Answer: A

Q.No.88 An organization is considering allowing users to access company data from their personal devices. Which of the following is the MOST important factor when assessing the risk?

A. Remote management capabilities
B. Type of device
C. Volume of data
D. Classification of the data

Answer: D

Q.No.89 Which of the following provides the MOST helpful information in identifying risk in an organization?

A. Risk analysis
B. Risk responses
C. Risk registers
D. Risk scenarios

Answer: D

Q.No.90 Which of the following is the PRIMARY purpose of periodically reviewing an organization's risk profile?

A. Enable risk-based decision making.
B. Design and implement risk response action plans.
C. Update risk responses in the risk register.
D. Align business objectives with risk appetite.

Answer: A

Q.No.91 Which of the following would offer the MOST insight with regard to an organization's risk culture?

A. Risk management framework
B. Risk management procedures
C. Benchmark analyses
D. Senior management interviews

Answer: D

Q.No.92 Accountability for a particular risk is BEST represented in a

A. risk scenario.
B. RACI matrix.
C. risk catalog.
D. risk register.

Answer: D

Q.No.93 Which of the following is the MOST important data attribute of key risk indicators (KRIs)?

A. The data is measurable.
B. The data is calculated continuously.
C. The data is relevant.
D. The data is automatically produced.

Answer: A

Q.No.94 Prior to selecting key performance indicators (KPIs), itis MOST important to ensure:

A. trending data is available.
B. process flowcharts are current
C. measurement objectives are defined.

D. data collection technology is available.

Answer: C

Q.No.95 Which of the following should be the PRIMARY recipient of reports showing the progress of a current IT risk mitigation project?

A. Senior management
B. Project manager
C. Project sponsor
D. IT risk manager

Answer: A

Q.No.96 Controls should be defined during the design phase of system development because:

A. it is more cost-effective to determine controls in the early design phase.
B. technical specifications are defined during this phase.
C. structured analysis techniques exclude identification of controls.
D. structured programming techniques require that controls be designed before coding begins.

Answer: A

Q.No.97 When reviewing a business continuity plan (BCP), which of the following would be the MOST significant deficiency?

A. BCP is often tested using the walk-through method.
B. BCP testing is not in conjunction with the disaster recovery plan (DRP)
C. Each business location has separate, inconsistent BCPS.
D. Recovery time objectives (RTOS) do not meet business requirements. A

Answer: D

Q.No.98 Which of the following is a risk practitioner's BEST course of action upon learning that a control under internal review may no longer be necessary?

A. Obtain approval to retire the control.
B. Consult the internal auditor for a second opinion.
C. Update the status of the control as obsolete.

D. Verify the effectiveness of the original mitigation plan.

Answer: C

Q.No.99 Which of these documents is MOST important to request from a cloud service provider during a vendor risk assessment?

A. Nondisclosure agreement (NDA)
B. Independent audit report
C. Business impact analysis (BIA)
D. Service level agreement (SLA)

Answer: B

Q.No.100 Periodically reviewing and updating a risk register with details on identified risk factors PRIMARILY helps to:

A. minimize the number of risk scenarios for risk assessment
B. aggregate risk scenarios identified across different business units.
C. provide a current reference to stakeholders for risk-based decisions.
D. build a threat profile of the organization for management review. W

Answer: D

Q.No.101 The BEST way to test the operational effectiveness of a data backup procedure is to:

A. conduct an audit of files stored offsite.
B. demonstrate a successful recovery from backup files.
C. interview employees to compare actual with expected procedures.
D. inspect a selection of audit trails and backup logs,

Answer: B

Q.No.102 Which of the following is MOST important to the effective monitoring of key risk indicators (KRIS)?

A. Updating the threat inventory with new threats
B. Automating log data analysis
C. Preventing the generation of false alerts
D. Determining threshold levels

Answer: D

Q.No.103 Which of the following statements BEST describes risk appetite?\

A. The amount of risk an organization is willing to accept
B. Acceptable variation between risk thresholds and business objectives
C. The effective management of risk and internal control environments
D. The acceptable variation relative to the achievement of objectives a

Answer: A

Q.No.104 Which of the following is the GREATEST concern when using a generic set of IT risk scenarios for risk analysis?

A. Quantitative analysis might not be possible.
B. Inherent risk might not be considered.
C. Implementation costs might increase.
D. Risk factors might not be relevant to the organization

Answer: D

Q.No.105 A newly hired risk practitioner finds that the risk register has not been updated in the past year. What is the risk practitioner's BEST course of action?

A. Outsource the process for updating the risk register.
B. Implement a process improvement and replace the old risk register.
C. Identify changes in risk factors and initiate risk reviews.
D. Engage an external consultant to redesign the risk management process.

Answer: C

Q.No.106 Business areas within an organization have engaged various cloud service providers directly without assistance from the IT department. What should the risk practitioner do?

A. Engage with the business area managers to review controls applied.
B. Recommend a risk assessment be conducted.
C. Recommend the IT department remove access to the cloud services.
D. Escalate to the risk committee.

Answer: A

Q.No.107 Which of the following would present the GREATEST challenge when assigning accountability for control ownership?

A. Weak governance structures
B. Complex regulatory environment
C. Unclear reporting relationships
D. Senior management scrutiny

Answer: C

Q.No.108 The PRIMARY purpose of vulnerability assessments is to:

A. test intrusion detection systems (IDS) and response procedures.
B. provide clear evidence that the system is sufficiently secure.
C. determine the impact of potential threats.
D. detect weaknesses that could lead to a system compromise.

Answer: D

Q.No.109 When developing IT risk scenarios, it is MOST important to consider:

A. the organization's threat profile.
B. executive management directives.
C. organizational objectives.
D. external audit findings.

Answer: C

Q.No.110 Which of the following BEST indicates effective information security incident management?

A. Percentage of high risk security incidents
B. Frequency of information security incident response plan testing
C. Monthly trend of information security-related incidents
D. Average time to identify critical information security incidents

Answer: B

Q.No.111 The PRIMARY reason for periodically monitoring key risk indicators (KRIs) is to:

A. detect changes in the risk profile.
B. rectify errors in results of KRI s.
C. reduce costs of risk mitigation controls.
D. continually improve risk assessments.

Answer: A

Q.No.112 The PRIMARY objective for requiring an independent review of an organization's IT risk management process should be to:

A. ensure IT risk management is focused on mitigating potential risk.
B. confirm that IT risk assessment results are expressed as business impact
C. assess gaps in IT risk management operations and strategic focus.
D. verify implemented controls to reduce the likelihood of threat materişlization.

Answer: A

Q.No.113 IT stakeholders have asked a risk practitioner for IT risk profile reports associated with specific departments to allocate resources for risk mitigation. The BEST way to address this request would be to use:

A. the cost associated with each control.
B. key risk indicators (KRIs),
C. information from the risk register.
D. historical risk assessments.

Answer: C

Q.no.114 Which type of cloud computing deployment provides the consumer the GREATEST degree of control over the environment?

A. Community cloud
B. Private cloud
C. Hybrid cloud
D. Public doud

Answer: B

Q.No.115 The PRIMARY goal of a risk management program is to:

A. help ensure objectives are met

B. safeguard corporate assets.
C. facilitate resource availability.
D. help prevent operational losses.

Answer: A

Q.No.116 Which of the following BEST indicates that an organization has implemented IT performance requirements?

A. Accountability matrix
B. Benchmarking data
C. Service level agreements (SLA)
D. Vendor references

Answer: C

Q.No.117 Which of the following would be MOST useful to senior management when determining an appropriate risk response?

A. A comparison of current risk levels with established tolerance
B. A comparison of cost variance with defined response strategies
C. A comparison of current risk levels with estimated inherent risk levels
D. A comparison of accepted risk scenarios associated with regulatory compliance

Answer: A

Q.No.118 The PRIMARY reason for periodic penetration testing of Internet-facing applications is to:

A. ensure policy and regulatory compliance.
B. verify Internet firewall control settings.
C. assess the proliferation of new threats.
D. identify vulnerabilities in the system.

Answer: D

Q.No.119 Which of the following would BEST enable a risk practitioner to embed risk management within the organization?

A. Provide risk management feedback to key stakeholders.
B. Collect and analyze risk data for report generation.

C. Monitor and prioritize risk data according to the heat map.
D. Engage key stakeholders in risk management practices.

Answer: D

Q.No.120 Which of the following is a PRIMARY benefit of engaging the risk owner during the risk assessment process?

A. Identification of controls gaps that may lead to noncompliance
B. Early detection of emerging threats
C. Accurate measurement of loss impact
D. Prioritization of risk action plans across departments

Answer: C

Q.No.121 A risk assessment has identified increased losses associated with an IT risk scenario. It is MOST important for the risk practitioner to:

A. update the risk rating
B. implement additional controls.
C. reevaluate inherent risk.
D. develop new risk scenarios.

Answer: A

Q.No.122 Which of the following BEST facilitates the development of effective IT risk scenarios?

A. Validation by senior management
B. Participation by IT subject matter experts
C. Integration of contingency planning
D. Utilization of a cross-functional team

Answer: D

Q.No.123 An organization is preparing to transfer a large number of customer service representatives to the sales department of the following, who is responsible for mitigating the risk associated with residual system access?

A. IT service desk manager
B. Access control manager

C. Customer service manager
D. Sales manager

Answer: B

Q.No.124 Which stakeholders are PRIMARILY responsible for determining enterprise IT risk appetite?

A. Enterprise risk management and business process owners
B. Executive management and the board of directors
C. The chief information officer (CIO) and the chief financial officer (CFO)
D. Audit and compliance management

Answer: B

Q.No.125 The PRIMARY benefit associated with key risk indicators (KRIS) is that they:

A. help an organization identify emerging threats.
B. benchmark the organization's risk profile.
C. identify trends in the organization's vulnerabilities.
D. enable ongoing monitoring of emerging risk.

Answer: D

Q.No.126 Which of the following is the MOST effective control to maintain the integrity of system configuration files?

A. Monitoring against the configuration standard
B. Implementing automated vulnerability scanning
C. Recording changes to configuration files
D. Restricting access to configuration documentation

Answer: A

Q.No.127 Who should be responsible for implementing and maintaining security controls?

A. Internal auditor
B. Data custodian
C. End user
D. Data owner

Answer: D

Q.No.128 Which of the following would be a weakness in procedures for controlling the migration of changes to production libraries?

A. Only operations personnel are authorized to access production libraries.
B. Test and production programs are in distinct libraries.
C. The programming project leader solely reviews test results before approving the transfer to production
D. A synchronized migration of executable and source code from the test environment to the production environment is allowed.

Answer: C

Q.No.129 Which of the following is the PRIMARY consideration when establishing an organization's risk management methodology?

A. Resource requirements
B. Risk tolerance level
C. Business context
D. Benchmarking information

Answer: C

Q.No.130 Which of the following BEST ensures that identified risk scenarios are addressed?

A. Creating a separate risk register for key business units
B. Performing real-time monitoring of threats
C. Reviewing the implementation of the risk response
D. Performing regular risk control self-assessments (CSA)

Answer: B

Q.No.131 An organization is considering adopting artificial intelligence (AI). Which of the following is the risk practitioner's MOST important course of action?

A. Develop key risk indicators (KRIs).
B. Ensure sufficient pre-implementation testing.
C. Identify applicable risk scenarios.
D. Identify the organization's critical data.

Answer: C

Q.No.132 Which of the following is MOST helpful in determining the effectiveness of an organization's IT risk mitigation efforts?

A. Assigning identification dates for risk scenarios in the risk register
B. Updating impact assessments for risk scenario
C. Verifying whether risk action plans have been completed
D. Reviewing key risk indicators (KRIS)

Answer: D

Q.No.133 Which of the following BEST measures the impact of business interruptions caused by an IT service outage?

A. Duration of service outage
B. Sustained financial loss
C. Cost of remediation efforts
D. Average time to recovery

Answer: B

Q.No.134 Who is accountable for risk treatment?

A. Business process owner
B. Enterprise risk management team
C. Risk mitigation manager
D. Risk owner

Answer: D

Q.No.135 Which of the following should be of GREATEST concern for an organization considering the adoption of a bring your own device (BYOD) initiative?

A. Device corruption
B. User support
C. Data loss
D. Malicious users

Answer: D

Q.No.136 Mitigating technology risk to acceptable levels should be based PRIMARILY upon:

A. organizational risk appetite.
B. business sector best practices.
C. business process requirements.
D. availability of automated solutions.

Answer: C

Q.No.137 Which of the following is the BEST way to ensure ongoing control effectiveness?

A. Measuring trends in control performance
B. Establishing policies and procedures
C. Periodically reviewing control design
D. Obtaining management control attestations

Answer: A

Q.No.138 What should a risk practitioner do FIRST when vulnerability assessment results identify a weakness in an application?

A. Review regular control testing results.
B. Recommend a penetration test.
C. Assess the risk to determine mitigation needed.
D. Analyze key performance indicators (KPIs).

Answer: C

Q.No.139 IT disaster recovery point objectives (RPOs) should be based on the

A. need of each business unit.
B. maximum tolerable loss of data.
C. type of business.
D. maximum tolerable downtime.

Answer: A

Q.No.140 Which of the following is the MOST effective way to integrate business risk management with IT operations?

A. Require a risk assessment with change requests.
B. Provide security awareness training.
C. Perform periodic IT control self-assessments (CSAS).
D. Perform periodic risk assessments.

Answer: D

Q.No.141 Which of the following is MOST helpful to management when determining the resources needed to mitigate a risk?

A. A vulnerability report
B. An internal audit
C. A business impact analysis (BIA)
D. A heat map

Answer: C

Q.No.142 From a risk management perspective, which of the following is the PRIMARY benefit of using automated system configuration validation tools?

A. Inherent risk is reduced
B. Operational costs are reduced.
C. Staff costs are reduced.
D. Residual risk is reduced

Answer: B

Q.No.143 Which of the following is MOST important for a risk practitioner to verify when evaluating the effectiveness of an organization's existing controls?

A. Residual risk remains within acceptable levels.
B. Inherent risk has been reduced from original levels.
C. Costs for control maintenance are reasonable.
D. Senior management has approved the control design.

Answer: A

Q.No.144 Which of the following is the MOST important responsibility of a risk owner?

A. Establishing business information criteria
B. Establishing the risk register

C. Accepting residual risk
D. Testing control design

Answer: C

Q.No.145 A risk practitioner notices a trend of noncompliance with an IT-related control. Which of the following would BEST assist in making a recommendation to management?

A. Assessing the degree to which the control hinders business objectives
B. Reviewing the IT policy with the risk owner
C. Reviewing the roles and responsibilities of control process owners
D. Assessing noncompliance with control best practices

Answer: A

Q.No.146 A risk practitioner has become aware of production data being used in a test environment. Which of the following should be the practitioner's PRIMARY concern?

A. Sensitivity of the data
B. Availability of data to authorized staff
C. Security of the test environment
D. Readability of test data

Answer: A

Q.No.147 An organization striving to be on the leading edge in regard to risk monitoring would MOST likely implement:

A. a tool for monitoring critical activities and controls.
B. real-time monitoring of risk events and control exceptions.
C. procedures to monitor the operation of controls.
D. monitoring activities for all critical assets.

Answer: B

Q.No.148 The MOST essential content to include in an IT risk awareness program is how to:

A. comply with the organization's IT risk and information security policies
B. define the IT risk framework for the organization
C. prioritize IT-related actions by considering risk appetite and risk tolerance.
D. populate risk register entries and build a risk profile for management reporting,

Answer: A

Q.No.149 Within the three lines of defense model, the accountability for the system of internal control resides with:

A. the chief information officer (CIO).
B. the board of directors
C. enterprise risk management
D. the risk practitioner

Answer: B

Q.No.150 Which of the following is performed after a risk assessment is completed?

A. Defining risk taxonomy
B. Conducting an impact analysis
C. Identifying vulnerabilities
D. Defining risk response options

Answer: B