Number: CRISC
Passing Score: 800
Time Limit: 120
File Version: 14.0

Exam Code: CRISC

Exam Name: Certified in Risk and Information Systems Control

Exam A

QUESTION 1
Mapping open risk issues to an enterprise risk heat map BEST facilitates:

A. risk response.
B. control monitoring.
C. risk identification.
D. risk ownership.

Correct Answer: A
Section:

QUESTION 2
Which of the following BEST enables the risk profile to serve as an effective resource to support business objectives?

A. Engaging external risk professionals to periodically review the risk
B. Prioritizing global standards over local requirements in the risk profile
C. Updating the risk profile with risk assessment results
D. Assigning quantitative values to qualitative metrics in the risk register

Correct Answer: C
Section:

QUESTION 3
Which of the following will BEST ensure that information security risk factors are mitigated when developing in-house applications?

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

Correct Answer: D
Section:

QUESTION 4
An organization has identified that terminated employee accounts are not disabled or deleted within the time required by corporate policy. Unsure of the reason, the organization has decided to monitor the situation for three months to obtain more information. As a result of this decision, the risk has been:

A. avoided.
B. accepted.
C. mitigated.
D. transferred.

Correct Answer: B
Section:

QUESTION 5
Which of the following is MOST effective in continuous risk management process improvement?

A. Periodic assessments
B. Change management
C. Awareness training
D. Policy updates

Correct Answer: A
Section:

QUESTION 6
Which of the following would provide executive management with the BEST information to make risk decisions as a result of a risk assessment?

A. A companion of risk assessment results to the desired state
B. A quantitative presentation of risk assessment results
C. An assessment of organizational maturity levels and readiness
D. A qualitative presentation of risk assessment results

Correct Answer: A
Section:

QUESTION 7
Implementing which of the following controls would BEST reduce the impact of a vulnerability that has been exploited?

A. Detective control
B. Deterrent control
C. Preventive control
D. Corrective control

Correct Answer: D
Section:

QUESTION 8
What should be the PRIMARY objective for a risk practitioner performing a post-implementation review of an IT risk mitigation project?

A. Documenting project lessons learned
B. Validating the risk mitigation project has been completed
C. Confirming that the project budget was not exceeded
D. Verifying that the risk level has been lowered

Correct Answer: D
Section:

QUESTION 9
Which of the following is MOST important when discussing risk within an organization?

A. Adopting a common risk taxonomy
B. Using key performance indicators (KPIs)
C. Creating a risk communication policy
D. Using key risk indicators (KRIs)

Correct Answer: A
Section:

QUESTION 10
Which of the following should an organization perform to forecast the effects of a disaster?

A. Develop a business impact analysis (BIA).
B. Define recovery time objectives (RTO).
C. Analyze capability maturity model gaps.
D. Simulate a disaster recovery.

Correct Answer: A
Section:

QUESTION 11
Which of the following can be used to assign a monetary value to risk?

A. Annual loss expectancy (ALE)
B. Business impact analysis
C. Cost-benefit analysis
D. Inherent vulnerabilities

Correct Answer: A
Section:

QUESTION 12
A recent internal risk review reveals the majority of core IT application recovery time objectives (RTOs) have exceeded the maximum time defined by the business application owners. Which of the following is MOST likely to change as a result?

A. Risk forecasting
B. Risk tolerance
C. Risk likelihood
D. Risk appetite

Correct Answer: B
Section:

QUESTION 13
A business manager wants to leverage an existing approved vendor solution from another area within the organization. Which of the following is the risk practitioner's BEST course of action?

A. Recommend allowing the new usage based on prior approval.
B. Request a new third-party review.
C. Request revalidation of the original use case.
D. Assess the risk associated with the new use case.

Correct Answer: D
Section:

QUESTION 14
It is MOST important to the effectiveness of an IT risk management function that the associated processes are:

A. aligned to an industry-accepted framework.
B. reviewed and approved by senior management.
C. periodically assessed against regulatory requirements.
D. updated and monitored on a continuous basis.

Correct Answer: C
Section:

QUESTION 15
A department has been granted an exception to bypass the existing approval process for purchase orders. The risk practitioner should verify the exception has been approved by which of the following?

A. Internal audit
B. Control owner
C. Senior management
D. Risk manager

Correct Answer: B
Section:

QUESTION 16
Which of the following would be MOST beneficial as a key risk indicator (KRI)?

A. Current capital allocation reserves
B. Negative security return on investment (ROI)
C. Project cost variances
D. Annualized loss projections

Correct Answer: D
Section:

QUESTION 17
Of the following, who should be responsible for determining the inherent risk rating of an application?

A. Application owner
B. Senior management

C. Risk practitioner
D. Business process owner

Correct Answer: C
Section:

QUESTION 18
Which of the following would provide the MOST comprehensive information for updating an organization's risk register?

A. Results of the latest risk assessment
B. Results of a risk forecasting analysis
C. A review of compliance regulations
D. Findings of the most recent audit

Correct Answer: A
Section:

QUESTION 19
Which of the following statements in an organization's current risk profile report is cause for further action by senior management?

A. Key performance indicator (KPI) trend data is incomplete.
B. New key risk indicators (KRIs) have been established.
C. Key performance indicators (KPIs) are outside of targets.
D. Key risk indicators (KRIs) are lagging.

Correct Answer: B
Section:

QUESTION 20
Which of the following provides the BEST evidence that risk responses have been executed according to their risk action plans?

A. Risk policy review
B. Business impact analysis (B1A)
C. Control catalog
D. Risk register

Correct Answer: D
Section:

QUESTION 21
Which of the following methods is the BEST way to measure the effectiveness of automated information security controls prior to going live?

A. Testing in a non-production environment
B. Performing a security control review
C. Reviewing the security audit report
D. Conducting a risk assessment

Correct Answer: A
Section:

QUESTION 22
A bank wants to send a critical payment order via email to one of its offshore branches. Which of the following is the BEST way to ensure the message reaches the intended recipient without alteration?

A. Add a digital certificate
B. Apply multi-factor authentication
C. Add a hash to the message
D. Add a secret key

Correct Answer: C
Section:

QUESTION 23
Which of the following will be MOST effective to mitigate the risk associated with the loss of company data stored on personal devices?

A. An acceptable use policy for personal devices
B. Required user log-on before synchronizing data
C. Enforced authentication and data encryption
D. Security awareness training and testing

Correct Answer: C
Section:

QUESTION 24
Who should be responsible for strategic decisions on risk management?

A. Chief information officer (CIO)
B. Executive management team
C. Audit committee
D. Business process owner

Correct Answer: B
Section:

QUESTION 25
Which of the following would MOST likely drive the need to review and update key performance indicators (KPIs) for critical IT assets?

A. The outsourcing of related IT processes
B. Outcomes of periodic risk assessments
C. Changes in service level objectives
D. Findings from continuous monitoring

Correct Answer: B
Section:

QUESTION 26
Which of the following will BEST help ensure that risk factors identified during an information systems review are addressed?

A. Informing business process owners of the risk
B. Reviewing and updating the risk register
C. Assigning action items and deadlines to specific individuals
D. Implementing new control technologies

Correct Answer: C
Section:

QUESTION 27
An internally developed payroll application leverages Platform as a Service (PaaS) infrastructure from the cloud. Who owns the related data confidentiality risk?

A. IT infrastructure head
B. Human resources head
C. Supplier management head
D. Application development head

Correct Answer: B
Section:

QUESTION 28
Following a review of a third-party vendor, it is MOST important for an organization to ensure:

A. results of the review are accurately reported to management.
B. identified findings are reviewed by the organization.
C. results of the review are validated by internal audit.
D. identified findings are approved by the vendor.

Correct Answer: A
Section:

QUESTION 29
A risk practitioner has observed that risk owners have approved a high number of exceptions to the information security policy. Which of the following should be the risk practitioner's GREATEST concern?

A. Security policies are being reviewed infrequently.
B. Controls are not operating efficiently.
C. Vulnerabilities are not being mitigated
D. Aggregate risk is approaching the tolerance threshold

Correct Answer: D
Section:

QUESTION 30
Which of the following BEST promotes commitment to controls?

A. Assigning control ownership
B. Assigning appropriate resources
C. Assigning a quality control review
D. Performing regular independent control reviews

Correct Answer: A
Section:

QUESTION 31
Which of the following is MOST important for developing effective key risk indicators (KRIs)?

A. Engaging sponsorship by senior management
B. Utilizing data and resources internal to the organization
C. Including input from risk and business unit management
D. Developing in collaboration with internal audit

Correct Answer: C
Section:

QUESTION 32
The MOST important reason to monitor key risk indicators (KRIs) is to help management:

A. identity early risk transfer strategies.
B. lessen the impact of realized risk.
C. analyze the chain of risk events.
D. identify the root cause of risk events.

Correct Answer: C
Section:

QUESTION 33
The implementation of a risk treatment plan will exceed the resources originally allocated for the risk response. Which of the following should be the risk owner's NEXT action?

A. Perform a risk assessment.
B. Accept the risk of not implementing.
C. Escalate to senior management.
D. Update the implementation plan.

Correct Answer: C
Section:

QUESTION 34
Which of the following is MOST important to understand when developing key risk indicators (KRIs)?

A. KRI thresholds
B. Integrity of the source data
C. Control environment

D. Stakeholder requirements

Correct Answer: B
Section:

QUESTION 35
Which of the following is the PRIMARY benefit of identifying and communicating with stakeholders at the onset of an IT risk assessment?

A. Obtaining funding support
B. Defining the risk assessment scope
C. Selecting the risk assessment framework
D. Establishing inherent risk

Correct Answer: B
Section:

QUESTION 36
Which of the following is the BEST way to detect zero-day malware on an end user's workstation?

A. An antivirus program
B. Database activity monitoring
C. Firewall log monitoring
D. File integrity monitoring

Correct Answer: C
Section:

QUESTION 37
An organization has just implemented changes to close an identified vulnerability that impacted a critical business process. What should be the NEXT course of action?

A. Redesign the heat map.
B. Review the risk tolerance.
C. Perform a business impact analysis (BIA)
D. Update the risk register.

Correct Answer: C
Section:

QUESTION 38
Which of the following is MOST important for a risk practitioner to consider when evaluating plans for changes to IT services?

A. Change testing schedule
B. Impact assessment of the change
C. Change communication plan
D. User acceptance testing (UAT)

Correct Answer: B

Section:

QUESTION 39
Before implementing instant messaging within an organization using a public solution, which of the following should be in place to mitigate data leakage risk?

A. A data extraction tool
B. An access control list
C. An intrusion detection system (IDS)
D. An acceptable usage policy

Correct Answer: D
Section:

QUESTION 40
To mitigate the risk of using a spreadsheet to analyze financial data, IT has engaged a third-party vendor to deploy a standard application to automate the process. Which of the following parties should own the risk associated with calculation errors?

A. business owner
B. IT department
C. Risk manager
D. Third-party provider

Correct Answer: A
Section:

QUESTION 41
A risk practitioner shares the results of a vulnerability assessment for a critical business application with the business manager. Which of the following is the NEXT step?

A. Develop a risk action plan to address the findings.
B. Evaluate the impact of the vulnerabilities to the business application.
C. Escalate the findings to senior management and internal audit.
D. Conduct a penetration test to validate the vulnerabilities from the findings.

Correct Answer: B
Section:

QUESTION 42
Which of the following provides the MOST helpful reference point when communicating the results of a risk assessment to stakeholders?

A. Risk tolerance
B. Risk appetite
C. Risk awareness
D. Risk policy

Correct Answer: B
Section:

QUESTION 43
Which of the following is MOST influential when management makes risk response decisions?

A. Risk appetite
B. Audit risk
C. Residual risk
D. Detection risk

Correct Answer: A
Section:

QUESTION 44
The risk appetite for an organization could be derived from which of the following?

A. Cost of controls
B. Annual loss expectancy (ALE)
C. Inherent risk
D. Residual risk

Correct Answer: A
Section:

QUESTION 45
A third-party vendor has offered to perform user access provisioning and termination. Which of the following control accountabilities is BEST retained within the organization?

A. Reviewing access control lists
B. Authorizing user access requests
C. Performing user access recertification
D. Terminating inactive user access

Correct Answer: B
Section:

QUESTION 46
Which of the following BEST reduces the probability of laptop theft?

A. Cable lock
B. Acceptable use policy
C. Data encryption
D. Asset tag with GPS

Correct Answer: A
Section:

QUESTION 47
Which of the following resources is MOST helpful when creating a manageable set of IT risk scenarios?

A. Results of current and past risk assessments
B. Organizational strategy and objectives
C. Lessons learned from materialized risk scenarios
D. Internal and external audit findings

Correct Answer: B
Section:

QUESTION 48
The BEST key performance indicator (KPI) to measure the effectiveness of a vendor risk management program is the percentage of:

A. vendors providing risk assessments on time.
B. vendor contracts reviewed in the past year.
C. vendor risk mitigation action items completed on time.
D. vendors that have reported control-related incidents.

Correct Answer: A
Section:

QUESTION 49
What is the MOST important consideration when aligning IT risk management with the enterprise risk management (ERM) framework?

A. Risk and control ownership
B. Senior management participation
C. Business unit support
D. Risk nomenclature and taxonomy

Correct Answer: B
Section:

QUESTION 50
Which of the following is the MOST important enabler of effective risk management?

A. User awareness of policies and procedures
B. Implementation of proper controls
C. Senior management support
D. Continuous monitoring of threats and vulnerabilities

Correct Answer: C
Section:

QUESTION 51
Which of the following is MOST important when defining controls?

A. Identifying monitoring mechanisms
B. Including them in the risk register
C. Aligning them with business objectives

D. Prototyping compensating controls

Correct Answer: C
Section:

QUESTION 52
A risk practitioner is reviewing a vendor contract and finds there is no clause to control privileged access to the organization's systems by vendor employees. Which of the following is the risk practitioner's BEST course of action?

A. Contact the control owner to determine if a gap in controls exists.
B. Add this concern to the risk register and highlight it for management review.
C. Report this concern to the contracts department for further action.
D. Document this concern as a threat and conduct an impact analysis.

Correct Answer: D
Section:

QUESTION 53
Which of the following is the PRIMARY objective for automating controls?

A. Improving control process efficiency
B. Facilitating continuous control monitoring
C. Complying with functional requirements
D. Reducing the need for audit reviews

Correct Answer: A
Section:

QUESTION 54
Which of the following is the GREATEST risk associated with the use of data analytics?

A. Distributed data sources
B. Manual data extraction
C. Incorrect data selection
D. Excessive data volume

Correct Answer: C
Section:

QUESTION 55
An IT operations team implements disaster recovery controls based on decisions from application owners regarding the level of resiliency needed. Who is the risk owner in this scenario?

A. Business resilience manager
B. Disaster recovery team lead
C. Application owner
D. IT operations manager

Correct Answer: C
Section:

QUESTION 56
Which of the following is MOST important when developing risk scenarios?

A. The scenarios are based on industry best practice.
B. The scenarios focus on current vulnerabilities.
C. The scenarios are relevant to the organization.
D. The scenarios include technical consequences.

Correct Answer: C
Section:

QUESTION 57
An organization has initiated a project to implement an IT risk management program for the first time. The BEST time for the risk practitioner to start populating the risk register is when:

A. identifying risk scenarios.
B. determining the risk strategy.
C. calculating impact and likelihood.
D. completing the controls catalog.

Correct Answer: A
Section:

QUESTION 58
Which of the following is the PRIMARY reason for conducting peer reviews of risk analysis?

A. To enhance compliance with standards
B. To minimize subjectivity of assessments
C. To increase consensus among peers
D. To provide assessments for benchmarking

Correct Answer: B
Section:

QUESTION 59
Which of the following would be the GREATEST concern related to data privacy when implementing an Internet of Things (IoT) solution that collects personally identifiable information (PII)?

A. A privacy impact assessment has not been completed.
B. Data encryption methods apply to a subset of PII obtained.
C. The data privacy officer was not consulted.
D. Insufficient access controls are used on the IoT devices.

Correct Answer: A
Section:

QUESTION 60
Which of the following will MOST improve stakeholders' understanding of the effect of a potential threat?

A. Establishing a risk management committee
B. Updating the organization's risk register to reflect the new threat
C. Communicating the results of the threat impact analysis
D. Establishing metrics to assess the effectiveness of the responses

Correct Answer: C
Section:

QUESTION 61
A risk practitioner has just learned about new done FIRST?

A. Notify executive management.
B. Analyze the impact to the organization.
C. Update the IT risk register.
D. Design IT risk mitigation plans.

Correct Answer: B
Section:

QUESTION 62
When testing the security of an IT system, il is MOST important to ensure that;

A. tests are conducted after business hours.
B. operators are unaware of the test.
C. external experts execute the test.
D. agreement is obtained from stakeholders.

Correct Answer: D
Section:

QUESTION 63
Which of the following risk scenarios would be the GREATEST concern as a result of a single sign-on implementation?

A. User access may be restricted by additional security.
B. Unauthorized access may be gained to multiple systems.
C. Security administration may become more complex.
D. User privilege changes may not be recorded.

Correct Answer: B
Section:

QUESTION 64
Which of the following would provide the MOST objective assessment of the effectiveness of an organization's security controls?

A. An internal audit
B. Security operations center review
C. Internal penetration testing
D. A third-party audit

Correct Answer: D
Section:

QUESTION 65
A risk owner has identified a risk with high impact and very low likelihood. The potential loss is covered by insurance. Which of the following should the risk practitioner do NEXT?

A. Recommend avoiding the risk.
B. Validate the risk response with internal audit.
C. Update the risk register.
D. Evaluate outsourcing the process.

Correct Answer: C
Section:

QUESTION 66
A maturity model will BEST indicate:

A. confidentiality and integrity.
B. effectiveness and efficiency.
C. availability and reliability.
D. certification and accreditation.

Correct Answer: B
Section:

QUESTION 67
An organization has recently updated its disaster recovery plan (DRP). Which of the following would be the GREATEST risk if the new plan is not tested?

A. External resources may need to be involved.
B. Data privacy regulations may be violated.
C. Recovery costs may increase significantly.
D. Service interruptions may be longer than anticipated.

Correct Answer: D
Section:

QUESTION 68
What are the MOST important criteria to consider when developing a data classification scheme to facilitate risk assessment and the prioritization of risk mitigation activities?

A. Mitigation and control value
B. Volume and scope of data generated daily
C. Business criticality and sensitivity

D. Recovery point objective (RPO) and recovery time objective (RTO)

Correct Answer: C
Section:

QUESTION 69
A control owner identifies that the organization's shared drive contains personally identifiable information (PII) that can be accessed by all personnel. Which of the following is the MOST effective risk response?

A. Protect sensitive information with access controls.
B. Implement a data loss prevention (DLP) solution.
C. Re-communicate the data protection policy.
D. Implement a data encryption solution.

Correct Answer: A
Section:

QUESTION 70
An organization has decided to outsource a web application, and customer data will be stored in the vendor's public cloud. To protect customer data, it is MOST important to ensure which of the following?

A. The organization's incident response procedures have been updated.
B. The vendor stores the data in the same jurisdiction.
C. Administrative access is only held by the vendor.
D. The vendor's responsibilities are defined in the contract.

Correct Answer: D
Section:

QUESTION 71
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

Correct Answer: A
Section:

QUESTION 72
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

Correct Answer: C

Section:

QUESTION 73
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

Correct Answer: B
Section:

QUESTION 74
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.

Correct Answer: B
Section:

QUESTION 75
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

Correct Answer: C
Section:

QUESTION 76
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.

Correct Answer: D
Section:

QUESTION 77
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.

Correct Answer: B
Section:

QUESTION 78
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

Correct Answer: D
Section:

QUESTION 79
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.

Correct Answer: B
Section:

QUESTION 80
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.

Correct Answer: A
Section:

QUESTION 81
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.

Correct Answer: B
Section:

QUESTION 82
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.

Correct Answer: C
Section:

QUESTION 83
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.

Correct Answer: C
Section:

QUESTION 84
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

Correct Answer: D
Section:

QUESTION 85
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.

Correct Answer: D
Section:

QUESTION 86
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)

Correct Answer: D
Section:

QUESTION 87
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).

Correct Answer: C
Section:

QUESTION 88
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

Correct Answer: A
Section:

QUESTION 89
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

Correct Answer: B

Section:

QUESTION 90
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

Correct Answer: A
Section:

QUESTION 91
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)

Correct Answer: B
Section:

QUESTION 92
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 cloud

Correct Answer: B
Section:

QUESTION 93
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.

Correct Answer: C
Section:

QUESTION 94

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

Correct Answer: C
Section:
Explanation:
Topic 3, Exam Pool C

QUESTION 95
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. Sales manager
C. Customer service manager
D. Access control manager

Correct Answer: D
Section:

QUESTION 96
A change management process has recently been updated with new testing procedures. What is the NEXT course of action?

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

Correct Answer: A
Section:

QUESTION 97
Which of the following should be done FIRST when information is no longer required to support business objectives?

A. Archive the information to a backup database.
B. Protect the information according to the classification policy.
C. Assess the information against the retention policy.
D. Securely and permanently erase the information

Correct Answer: C
Section:

QUESTION 98
When developing a new risk register, a risk practitioner should focus on which of the following risk management activities?

A. Risk management strategy planning
B. Risk monitoring and control
C. Risk identification
D. Risk response planning

Correct Answer: C
Section:

QUESTION 99
Which of the following BEST indicates whether security awareness training is effective?

A. User self-assessment
B. User behavior after training
C. Course evaluation
D. Quality of training materials

Correct Answer: B
Section:

QUESTION 100
An organizations 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, the risk practitioner's BEST course of action is to:

A. identify key risk indicators (KRIs) for ongoing monitoring
B. validate the CTO's decision with the business process owner
C. update the risk register with the selected risk response
D. recommend that the CTO revisit the risk acceptance decision.

Correct Answer: A
Section:

QUESTION 101
Several network user accounts were recently created without the required management approvals. Which of the following would be the risk practitioner's BEST recommendation to address this situation?

A. Conduct a comprehensive compliance review.
B. Develop incident response procedures for noncompliance.
C. Investigate the root cause of noncompliance.
D. Declare a security breach and Inform management.

Correct Answer: C
Section:

QUESTION 102
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. Enforce the use of digital signatures.
D. Apply single sign-on for access control.

Correct Answer: B
Section:

QUESTION 103
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. Readability of test data
C. Security of the test environment
D. Availability of data to authorized staff

Correct Answer: A
Section:

QUESTION 104
Which of the following is the GREATEST advantage of implementing a risk management program?

A. Enabling risk-aware decisions
B. Promoting a risk-aware culture
C. Improving security governance
D. Reducing residual risk

Correct Answer: A
Section:

QUESTION 105
When updating the risk register after a risk assessment, which of the following is MOST important to include?

A. Historical losses due to past risk events
B. Cost to reduce the impact and likelihood
C. Likelihood and impact of the risk scenario
D. Actor and threat type of the risk scenario

Correct Answer: C
Section:

QUESTION 106
The GREATEST benefit of including low-probability, high-impact events in a risk assessment is the ability to:

A. develop a comprehensive risk mitigation strategy
B. develop understandable and realistic risk scenarios
C. identify root causes for relevant events
D. perform an aggregated cost-benefit analysis

Correct Answer: D
Section:

QUESTION 107
Which of the following should be the FIRST consideration when a business unit wants to use personal information for a purpose other than for which it was originally collected?

A. Informed consent
B. Cross border controls
C. Business impact analysis (BIA)
D. Data breach protection

Correct Answer: A
Section:

QUESTION 108
The BEST metric to monitor the risk associated with changes deployed to production is the percentage of:

A. changes due to emergencies.
B. changes that cause incidents.
C. changes not requiring user acceptance testing.
D. personnel that have rights to make changes in production.

Correct Answer: B
Section:

QUESTION 109
Which of the following criteria associated with key risk indicators (KRIs) BEST enables effective risk monitoring?

A. Approval by senior management
B. Low cost of development and maintenance
C. Sensitivity to changes in risk levels
D. Use of industry risk data sources

Correct Answer: C
Section:

QUESTION 110
Which of the following BEST protects an organization against breaches when using a software as a service (SaaS) application?

A. Control self-assessment (CSA)
B. Security information and event management (SIEM) solutions
C. Data privacy impact assessment (DPIA)
D. Data loss prevention (DLP) tools

Correct Answer: B
Section:

QUESTION 111
When an organization's disaster recovery plan (DRP) has a reciprocal agreement, which of the following risk treatment options is being applied?

A. Acceptance
B. Mitigation
C. Transfer
D. Avoidance

Correct Answer: B
Section:

QUESTION 112
Which of the following is the MOST important reason to link an effective key control indicator (KCI) to relevant key risk indicators (KRIs)?

A. To monitor changes in the risk environment
B. To provide input to management for the adjustment of risk appetite
C. To monitor the accuracy of threshold levels in metrics
D. To obtain business buy-in for investment in risk mitigation measures

Correct Answer: A
Section:

QUESTION 113
Which of the following is MOST useful when communicating risk to management?

A. Risk policy
B. Audit report
C. Risk map
D. Maturity model

Correct Answer: C
Section:

QUESTION 114
Which of the following controls BEST enables an organization to ensure a complete and accurate IT asset inventory?

A. Prohibiting the use of personal devices for business
B. Performing network scanning for unknown devices
C. Requesting an asset list from business owners
D. Documenting asset configuration baselines

Correct Answer: B
Section:

QUESTION 115
Reviewing historical risk events is MOST useful for which of the following processes within the risk management life cycle?

A. Risk monitoring
B. Risk mitigation
C. Risk aggregation
D. Risk assessment

Correct Answer: D
Section:

QUESTION 116
Participants in a risk workshop have become focused on the financial cost to mitigate risk rather than choosing the most appropriate response. Which of the following is the BEST way to address this type of issue in the long term?

A. Perform a return on investment analysis.
B. Review the risk register and risk scenarios.
C. Calculate annualized loss expectancy of risk scenarios.
D. Raise the maturity of organizational risk management.

Correct Answer: D
Section:

QUESTION 117
Which of the following facilitates a completely independent review of test results for evaluating control effectiveness?

A. Segregation of duties
B. Three lines of defense
C. Compliance review
D. Quality assurance review

Correct Answer: B
Section:

QUESTION 118
Which of the following provides the MOST up-to-date information about the effectiveness of an organization's overall IT control environment?

A. Key performance indicators (KPIs)
B. Risk heat maps
C. Internal audit findings
D. Periodic penetration testing

Correct Answer: A
Section:

QUESTION 119
An organization recently received an independent security audit report of its cloud service provider that indicates significant control weaknesses. What should be done NEXT in response to this report?

A. Migrate all data to another compliant service provider.
B. Analyze the impact of the provider's control weaknesses to the business.

C. Conduct a follow-up audit to verify the provider's control weaknesses.
D. Review the contract to determine if penalties should be levied against the provider.

Correct Answer: B
Section:

QUESTION 120
A global organization is planning to collect customer behavior data through social media advertising. Which of the following is the MOST important business risk to be considered?

A. Regulatory requirements may differ in each country.
B. Data sampling may be impacted by various industry restrictions.
C. Business advertising will need to be tailored by country.
D. The data analysis may be ineffective in achieving objectives.

Correct Answer: A
Section:

QUESTION 121
Which of the following is the MOST important component in a risk treatment plan?

A. Technical details
B. Target completion date
C. Treatment plan ownership
D. Treatment plan justification

Correct Answer: D
Section:

QUESTION 122
When evaluating enterprise IT risk management it is MOST important to:

A. create new control processes to reduce identified IT risk scenarios
B. confirm the organization's risk appetite and tolerance
C. report identified IT risk scenarios to senior management
D. review alignment with the organization's investment plan

Correct Answer: B
Section:

QUESTION 123
The MAIN reason for creating and maintaining a risk register is to:

A. assess effectiveness of different projects.
B. define the risk assessment methodology.
C. ensure assets have low residual risk.
D. account for identified key risk factors.

Correct Answer: D
Section:

QUESTION 124
Which of the following is MOST important to the successful development of IT risk scenarios?

A. Cost-benefit analysis
B. Internal and external audit reports
C. Threat and vulnerability analysis
D. Control effectiveness assessment

Correct Answer: C
Section:

QUESTION 125
Which of The following should be the FIRST step when a company is made aware of new regulatory requirements impacting IT?

A. Perform a gap analysis.
B. Prioritize impact to the business units.
C. Perform a risk assessment.
D. Review the risk tolerance and appetite.

Correct Answer: C
Section:

QUESTION 126
Which of the following represents a vulnerability?

A. An identity thief seeking to acquire personal financial data from an organization
B. Media recognition of an organization's market leadership in its industry
C. A standard procedure for applying software patches two weeks after release
D. An employee recently fired for insubordination

Correct Answer: C
Section:

QUESTION 127
Which of the following is the PRIMARY reason to use key control indicators (KCIs) to evaluate control operating effectiveness?

A. To measure business exposure to risk
B. To identify control vulnerabilities
C. To monitor the achievement of set objectives
D. To raise awareness of operational issues

Correct Answer: C
Section:

QUESTION 128
The design of procedures to prevent fraudulent transactions within an enterprise resource planning (ERP) system should be based on:

A. stakeholder risk tolerance.
B. benchmarking criteria.
C. suppliers used by the organization.
D. the control environment.

Correct Answer: D
Section:

QUESTION 129
Which of the following is the BEST course of action to help reduce the probability of an incident recurring?

A. Perform a risk assessment.
B. Perform root cause analysis.
C. Initiate disciplinary action.
D. Update the incident response plan.

Correct Answer: B
Section:

QUESTION 130
Which of the following is MOST important to the integrity of a security log?

A. Least privilege access
B. Inability to edit
C. Ability to overwrite
D. Encryption

Correct Answer: B
Section:

QUESTION 131
Which of the following is the PRIMARY reason to have the risk management process reviewed by a third party?

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

Correct Answer: A
Section:

QUESTION 132
An organization has been notified that a disgruntled, terminated IT administrator has tried to break into the corporate network. Which of the following discoveries should be of GREATEST concern to the organization?

A. Authentication logs have been disabled.
B. An external vulnerability scan has been detected.
C. A brute force attack has been detected.
D. An increase in support requests has been observed.

Correct Answer: A
Section:

QUESTION 133
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. management.
B. tolerance.
C. culture.
D. analysis.

Correct Answer: C
Section:

QUESTION 134
Which of the following should be done FIRST when developing a data protection management plan?

A. Perform a cost-benefit analysis.
B. Identify critical data.
C. Establish a data inventory.
D. Conduct a risk analysis.

Correct Answer: B
Section:

QUESTION 135
Which of the following is the BEST way to determine whether new controls mitigate security gaps in a business system?

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

Correct Answer: C
Section:

QUESTION 136
A vulnerability assessment of a vendor-supplied solution has revealed that the software is susceptible to cross-site scripting and SQL injection attacks. Which of the following will BEST mitigate this issue?

A. Monitor the databases for abnormal activity
B. Approve exception to allow the software to continue operating
C. Require the software vendor to remediate the vulnerabilities

D. Accept the risk and let the vendor run the software as is

Correct Answer: C
Section:

QUESTION 137
Which of the following methods is an example of risk mitigation?

A. Not providing capability for employees to work remotely
B. Outsourcing the IT activities and infrastructure
C. Enforcing change and configuration management processes
D. Taking out insurance coverage for IT-related incidents

Correct Answer: C
Section:

QUESTION 138
A service provider is managing a client's servers. During an audit of the service, a noncompliant control is discovered that will not be resolved before the next audit because the client cannot afford the downtime required to correct the issue. The service provider's MOST appropriate action would be to:

A. develop a risk remediation plan overriding the client's decision
B. make a note for this item in the next audit explaining the situation
C. insist that the remediation occur for the benefit of other customers
D. ask the client to document the formal risk acceptance for the provider

Correct Answer: D
Section:

QUESTION 139
The PRIMARY purpose of IT control status reporting is to:

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

Correct Answer: A
Section:

QUESTION 140
An IT risk practitioner has been asked to regularly report on the overall status and effectiveness of the IT risk management program. Which of the following is MOST useful for this purpose?

A. Balanced scorecard
B. Capability maturity level
C. Internal audit plan
D. Control self-assessment (CSA)

Correct Answer: A
Section:

QUESTION 141
Which of the following risk management practices BEST facilitates the incorporation of IT risk scenarios into the enterprise-wide risk register?

A. Key risk indicators (KRIs) are developed for key IT risk scenarios
B. IT risk scenarios are assessed by the enterprise risk management team
C. Risk appetites for IT risk scenarios are approved by key business stakeholders.
D. IT risk scenarios are developed in the context of organizational objectives.

Correct Answer: D
Section:

QUESTION 142
Senior management has asked a risk practitioner to develop technical risk scenarios related to a recently developed enterprise resource planning (ERP) system. These scenarios will be owned by the system manager. Which of the following would be the BEST method to use when developing the scenarios?

A. Cause-and-effect diagram
B. Delphi technique
C. Bottom-up approach
D. Top-down approach

Correct Answer: A
Section:

QUESTION 143
An organization must make a choice among multiple options to respond to a risk. The stakeholders cannot agree and decide to postpone the decision. Which of the following risk responses has the organization adopted?

A. Transfer
B. Mitigation
C. Avoidance
D. Acceptance

Correct Answer: D
Section:

QUESTION 144
Which of the following is the MOST important technology control to reduce the likelihood of fraudulent payments committed internally?

A. Automated access revocation
B. Daily transaction reconciliation
C. Rule-based data analytics
D. Role-based user access model

Correct Answer: B
Section:

QUESTION 145
Which of the following should be included in a risk scenario to be used for risk analysis?

A. Risk appetite
B. Threat type
C. Risk tolerance
D. Residual risk

Correct Answer: B
Section:

QUESTION 146
While reviewing a contract of a cloud services vendor, it was discovered that the vendor refuses to accept liability for a sensitive data breach. Which of the following controls will BES reduce the risk associated with such a data breach?

A. Ensuring the vendor does not know the encryption key
B. Engaging a third party to validate operational controls
C. Using the same cloud vendor as a competitor
D. Using field-level encryption with a vendor supplied key

Correct Answer: B
Section:

QUESTION 147
Which of the following data would be used when performing a business impact analysis (BIA)?

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

Correct Answer: D
Section:

QUESTION 148
Prudent business practice requires that risk appetite not exceed:

A. inherent risk.
B. risk tolerance.
C. risk capacity.
D. residual risk.

Correct Answer: C
Section:

QUESTION 149
Which of the following MUST be updated to maintain an IT risk register?

A. Expected frequency and potential impact
B. Risk tolerance
C. Enterprise-wide IT risk assessment
D. Risk appetite

Correct Answer: C
Section:

QUESTION 150
Which of the following is the GREATEST benefit when enterprise risk management (ERM) provides oversight of IT risk management?

A. Aligning IT with short-term and long-term goals of the organization
B. Ensuring the IT budget and resources focus on risk management
C. Ensuring senior management's primary focus is on the impact of identified risk
D. Prioritizing internal departments that provide service to customers

Correct Answer: A
Section:

QUESTION 151
An organization automatically approves exceptions to security policies on a recurring basis. This practice is MOST likely the result of:

A. a lack of mitigating actions for identified risk
B. decreased threat levels
C. ineffective service delivery
D. ineffective IT governance

Correct Answer: D
Section:

QUESTION 152
Which of the following is the BEST reason to use qualitative measures to express residual risk levels related to emerging threats?

A. Qualitative measures require less ongoing monitoring.
B. Qualitative measures are better aligned to regulatory requirements.
C. Qualitative measures are better able to incorporate expert judgment.
D. Qualitative measures are easier to update.

Correct Answer: C
Section:

QUESTION 153
Which of the following is the BEST indicator of the effectiveness of IT risk management processes?

A. Percentage of business users completing risk training
B. Percentage of high-risk scenarios for which risk action plans have been developed

C. Number of key risk indicators (KRIs) defined
D. Time between when IT risk scenarios are identified and the enterprise's response

Correct Answer: B
Section:

QUESTION 154
A highly regulated organization acquired a medical technology startup company that processes sensitive personal information with weak data protection controls. Which of the following is the BEST way for the acquiring company to reduce its risk while still enabling the flexibility needed by the startup company?

A. Identify previous data breaches using the startup company's audit reports.
B. Have the data privacy officer review the startup company's data protection policies.
C. Classify and protect the data according to the parent company's internal standards.
D. Implement a firewall and isolate the environment from the parent company's network.

Correct Answer: A
Section:

QUESTION 155
Which of the following is the BEST indication of a mature organizational risk culture?

A. Corporate risk appetite is communicated to staff members.
B. Risk owners understand and accept accountability for risk.
C. Risk policy has been published and acknowledged by employees.
D. Management encourages the reporting of policy breaches.

Correct Answer: B
Section:

QUESTION 156
Which of the following should be the MOST important consideration for senior management when developing a risk response strategy?

A. Cost of controls
B. Risk tolerance
C. Risk appetite
D. Probability definition

Correct Answer: A
Section:

QUESTION 157
Which of the following provides the BEST measurement of an organization's risk management maturity level?

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

Correct Answer: C
Section:

QUESTION 158
Which of the following statements BEST illustrates the relationship between key performance indicators (KPIs) and key control indicators (KCIs)?

A. KPIs measure manual controls, while KCIs measure automated controls.
B. KPIs and KCIs both contribute to understanding of control effectiveness.
C. A robust KCI program will replace the need to measure KPIs.
D. KCIs are applied at the operational level while KPIs are at the strategic level.

Correct Answer: B
Section:

QUESTION 159
Which of the following is the GREATEST risk associated with an environment that lacks documentation of the architecture?

A. Unknown vulnerabilities
B. Legacy technology systems
C. Network isolation
D. Overlapping threats

Correct Answer: D
Section:

QUESTION 160
The BEST way to determine the likelihood of a system availability risk scenario is by assessing the:

A. availability of fault tolerant software.
B. strategic plan for business growth.
C. vulnerability scan results of critical systems.
D. redundancy of technical infrastructure.

Correct Answer: D
Section:

QUESTION 161
An organization uses a vendor to destroy hard drives. Which of the following would BEST reduce the risk of data leakage?

A. Require the vendor to degauss the hard drives
B. Implement an encryption policy for the hard drives.
C. Require confirmation of destruction from the IT manager.
D. Use an accredited vendor to dispose of the hard drives.

Correct Answer: B
Section:

QUESTION 162
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.

Correct Answer: A
Section:

QUESTION 163
Which of the following BEST enables the identification of trends in risk levels?

A. Correlation between risk levels and key risk indicators (KRIs) is positive.
B. Measurements for key risk indicators (KRIs) are repeatable
C. Quantitative measurements are used for key risk indicators (KRIs).
D. Qualitative definitions for key risk indicators (KRIs) are used.

Correct Answer: B
Section:

QUESTION 164
While reviewing an organization's monthly change management metrics, a risk practitioner notes that the number of emergency changes has increased substantially Which of the following would be the BEST approach for the risk practitioner to take?

A. Temporarily suspend emergency changes.
B. Document the control deficiency in the risk register.
C. Conduct a root cause analysis.
D. Continue monitoring change management metrics.

Correct Answer: C
Section:

QUESTION 165
An organization has implemented a preventive control to lock user accounts after three unsuccessful login attempts. This practice has been proven to be unproductive, and a change in the control threshold value has been recommended. Who should authorize changing this threshold?

A. Risk owner
B. IT security manager
C. IT system owner
D. Control owner

Correct Answer: D
Section:

QUESTION 166

Which of the following is the MOST effective control to maintain the integrity of system configuration files?

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

Correct Answer: D
Section:

QUESTION 167
When reviewing a business continuity plan (BCP). which of the following would be the MOST significant deficiency?

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

Correct Answer: B
Section:

QUESTION 168
Which of the following is the STRONGEST indication an organization has ethics management issues?

A. Employees do not report IT risk issues for fear of consequences.
B. Internal IT auditors report to the chief information security officer (CISO).
C. Employees face sanctions for not signing the organization's acceptable use policy.
D. The organization has only two lines of defense.

Correct Answer: A
Section:

QUESTION 169
Which of the following is the BEST evidence that a user account has been properly authorized?

A. An email from the user accepting the account
B. Notification from human resources that the account is active
C. User privileges matching the request form
D. Formal approval of the account by the user's manager

Correct Answer: C
Section:

QUESTION 170
Which of the following is the BEST way to manage the risk associated with malicious activities performed by database administrators (DBAs)?

A. Activity logging and monitoring

B. Periodic access review
C. Two-factor authentication
D. Awareness training and background checks

Correct Answer: A
Section:

QUESTION 171
Which of the following would BEST assist in reconstructing the sequence of events following a security incident across multiple IT systems in the organization's network?

A. Network monitoring infrastructure
B. Centralized vulnerability management
C. Incident management process
D. Centralized log management

Correct Answer: D
Section:

QUESTION 172
To communicate the risk associated with IT in business terms, which of the following MUST be defined?

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

Correct Answer: C
Section:

QUESTION 173
Which of the following is the GREATEST risk associated with the misclassification of data?

A. inadequate resource allocation
B. Data disruption
C. Unauthorized access
D. Inadequate retention schedules

Correct Answer: A
Section:

QUESTION 174
Which of the following is the MOST critical element to maximize the potential for a successful security implementation?

A. The organization's knowledge
B. Ease of implementation
C. The organization's culture
D. industry-leading security tools

Correct Answer: C
Section:

QUESTION 175
Which of the following is the PRIMARY purpose of periodically reviewing an organization's risk profile?

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

Correct Answer: B
Section:

QUESTION 176
Which of the following is necessary to enable an IT risk register to be consolidated with the rest of the organization's risk register?

A. Risk taxonomy
B. Risk response
C. Risk appetite
D. Risk ranking

Correct Answer: A
Section:

QUESTION 177
To reduce the risk introduced when conducting penetration tests, the BEST mitigating control would be to:

A. require the vendor to sign a nondisclosure agreement
B. clearly define the project scope.
C. perform background checks on the vendor.
D. notify network administrators before testing

Correct Answer: A
Section:

QUESTION 178
Which of the following tasks should be completed prior to creating a disaster recovery plan (DRP)?

A. Conducting a business impact analysis (BIA)
B. Identifying the recovery response team
C. Procuring a recovery site
D. Assigning sensitivity levels to data

Correct Answer: A
Section:

QUESTION 179
Which of the following BEST indicates the efficiency of a process for granting access privileges?

A. Average time to grant access privileges
B. Number of changes in access granted to users
C. Average number of access privilege exceptions
D. Number and type of locked obsolete accounts

Correct Answer: C
Section:

QUESTION 180
Several newly identified risk scenarios are being integrated into an organization's risk register. The MOST appropriate risk owner would be the individual who:

A. is in charge of information security.
B. is responsible for enterprise risk management (ERM)
C. can implement remediation action plans.
D. is accountable for loss if the risk materializes.

Correct Answer: D
Section:

QUESTION 181
An internal audit report reveals that not all IT application databases have encryption in place. Which of the following information would be MOST important for assessing the risk impact?

A. The number of users who can access sensitive data
B. A list of unencrypted databases which contain sensitive data
C. The reason some databases have not been encrypted
D. The cost required to enforce encryption

Correct Answer: B
Section:

QUESTION 182
Which of the following is the GREATEST benefit of analyzing logs collected from different systems?

A. A record of incidents is maintained.
B. Forensic investigations are facilitated.
C. Security violations can be identified.
D. Developing threats are detected earlier.

Correct Answer: C
Section:

QUESTION 183
Which of the following is the BEST approach when a risk practitioner has been asked by a business unit manager for special consideration during a risk assessment of a system?

A. Conduct an abbreviated version of the assessment.
B. Report the business unit manager for a possible ethics violation.
C. Perform the assessment as it would normally be done.
D. Recommend an internal auditor perform the review.

Correct Answer: B
Section:

QUESTION 184
What is the PRIMARY reason to periodically review key performance indicators (KPIs)?

A. Ensure compliance.
B. Identify trends.
C. Promote a risk-aware culture.
D. Optimize resources needed for controls

Correct Answer: A
Section:

QUESTION 185
The MOST important reason for implementing change control procedures is to ensure:

A. only approved changes are implemented
B. timely evaluation of change events
C. an audit trail exists.
D. that emergency changes are logged.

Correct Answer: A
Section:

QUESTION 186
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 allow for proper review of risk tolerance
C. To identify dependencies for reporting risk
D. To provide consistent and clear terminology

Correct Answer: B
Section:

QUESTION 187
Which of the following is MOST important when considering risk in an enterprise risk management (ERM) process?

A. Financial risk is given a higher priority.
B. Risk with strategic impact is included.
C. Security strategy is given a higher priority.

D. Risk identified by industry benchmarking is included.

Correct Answer: B
Section:

QUESTION 188
Which of the following is a KEY consideration for a risk practitioner to communicate to senior management evaluating the introduction of artificial intelligence (AI) solutions into the organization?

A. AI requires entirely new risk management processes.
B. AI potentially introduces new types of risk.
C. AI will result in changes to business processes.
D. Third-party AI solutions increase regulatory obligations.

Correct Answer: B
Section:

QUESTION 189
The BEST way to obtain senior management support for investment in a control implementation would be to articulate the reduction in:

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

Correct Answer: D
Section:

QUESTION 190
All business units within an organization have the same risk response plan for creating local disaster recovery plans. In an effort to achieve cost effectiveness, the BEST course of action would be to:

A. select a provider to standardize the disaster recovery plans.
B. outsource disaster recovery to an external provider.
C. centralize the risk response function at the enterprise level.
D. evaluate opportunities to combine disaster recovery plans.

Correct Answer: D
Section:

QUESTION 191
Which of the following would BEST mitigate the risk associated with reputational damage from inappropriate use of social media sites by employees?

A. Validating employee social media accounts and passwords
B. Monitoring Internet usage on employee workstations
C. Disabling social media access from the organization's technology
D. Implementing training and awareness programs

Correct Answer: D

Section:

QUESTION 192
After the review of a risk record, internal audit questioned why the risk was lowered from medium to low. Which of the following is the BEST course of action in responding to this inquiry?

A. Obtain industry benchmarks related to the specific risk.
B. Provide justification for the lower risk rating.
C. Notify the business at the next risk briefing.
D. Reopen the risk issue and complete a full assessment.

Correct Answer: B
Section:

QUESTION 193
Which of the following issues should be of GREATEST concern when evaluating existing controls during a risk assessment?

A. A high number of approved exceptions exist with compensating controls.
B. Successive assessments have the same recurring vulnerabilities.
C. Redundant compensating controls are in place.
D. Asset custodians are responsible for defining controls instead of asset owners.

Correct Answer: B
Section:

QUESTION 194
Which of the following would be MOST helpful to a risk practitioner when ensuring that mitigated risk remains within acceptable limits?

A. Building an organizational risk profile after updating the risk register
B. Ensuring risk owners participate in a periodic control testing process
C. Designing a process for risk owners to periodically review identified risk
D. Implementing a process for ongoing monitoring of control effectiveness

Correct Answer: D
Section:

QUESTION 195
Which of the following should be the PRIMARY focus of a risk owner once a decision is made to mitigate a risk?

A. Updating the risk register to include the risk mitigation plan
B. Determining processes for monitoring the effectiveness of the controls
C. Ensuring that control design reduces risk to an acceptable level
D. Confirming to management the controls reduce the likelihood of the risk

Correct Answer: C
Section:

QUESTION 196

Which of the following is the MOST appropriate key risk indicator (KRI) for backup media that is recycled monthly?

A. Time required for backup restoration testing
B. Change in size of data backed up
C. Successful completion of backup operations
D. Percentage of failed restore tests

Correct Answer: D
Section:

QUESTION 197
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

Correct Answer: A
Section:

QUESTION 198
The BEST indication that risk management is effective is when risk has been reduced to meet:

A. risk levels.
B. risk budgets.
C. risk appetite.
D. risk capacity.

Correct Answer: C
Section:

QUESTION 199
What is the PRIMARY purpose of a business impact analysis (BIA)?

A. To determine the likelihood and impact of threats to business operations
B. To identify important business processes in the organization
C. To estimate resource requirements for related business processes
D. To evaluate the priority of business operations in case of disruption

Correct Answer: D
Section:

QUESTION 200
Which of the following is the MOST important factor when deciding on a control to mitigate risk exposure?

A. Relevance to the business process

B. Regulatory compliance requirements
C. Cost-benefit analysis
D. Comparison against best practice

Correct Answer: B
Section:

QUESTION 201
Which of the following would be MOST helpful to an information security management team when allocating resources to mitigate exposures?

A. Relevant risk case studies
B. Internal audit findings
C. Risk assessment results
D. Penetration testing results

Correct Answer: C
Section:

QUESTION 202
Which of the following is the MOST important topic to cover in a risk awareness training program for all staff?

A. Internal and external information security incidents
B. The risk department's roles and responsibilities
C. Policy compliance requirements and exceptions process
D. The organization's information security risk profile

Correct Answer: C
Section:

QUESTION 203
Upon learning that the number of failed back-up attempts continually exceeds the current risk threshold, the risk practitioner should:

A. inquire about the status of any planned corrective actions
B. keep monitoring the situation as there is evidence that this is normal
C. adjust the risk threshold to better reflect actual performance
D. initiate corrective action to address the known deficiency

Correct Answer: D
Section:

QUESTION 204
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. Identify changes in risk factors and initiate risk reviews.
B. Engage an external consultant to redesign the risk management process.
C. Outsource the process for updating the risk register.
D. Implement a process improvement and replace the old risk register.

Correct Answer: A
Section:

QUESTION 205
Which of the following should be implemented to BEST mitigate the risk associated with infrastructure updates?

A. Role-specific technical training
B. Change management audit
C. Change control process
D. Risk assessment

Correct Answer: C
Section:

QUESTION 206
An organization practices the principle of least privilege. To ensure access remains appropriate, application owners should be required to review user access rights on a regular basis by obtaining:

A. business purpose documentation and software license counts
B. an access control matrix and approval from the user's manager
C. documentation indicating the intended users of the application
D. security logs to determine the cause of invalid login attempts

Correct Answer: B
Section:

QUESTION 207
Which of the following BEST indicates the condition of a risk management program?

A. Number of risk register entries
B. Number of controls
C. Level of financial support
D. Amount of residual risk

Correct Answer: D
Section:

QUESTION 208
Vulnerabilities have been detected on an organization's systems. Applications installed on these systems will not operate if the underlying servers are updated. Which of the following is the risk practitioner's BEST course of action?

A. Recommend the business change the application.
B. Recommend a risk treatment plan.
C. Include the risk in the next quarterly update to management.
D. Implement compensating controls.

Correct Answer: D
Section:

QUESTION 209
Which of the following should be management's PRIMARY consideration when approving risk response action plans?

A. Ability of the action plans to address multiple risk scenarios
B. Ease of implementing the risk treatment solution
C. Changes in residual risk after implementing the plans
D. Prioritization for implementing the action plans

Correct Answer: C
Section:

QUESTION 210
Which of the following is the MOST common concern associated with outsourcing to a service provider?

A. Lack of technical expertise
B. Combining incompatible duties
C. Unauthorized data usage
D. Denial of service attacks

Correct Answer: C
Section:

QUESTION 211
Which of the following roles would be MOST helpful in providing a high-level view of risk related to customer data loss?

A. Customer database manager
B. Customer data custodian
C. Data privacy officer
D. Audit committee

Correct Answer: B
Section:

QUESTION 212
When an organization is having new software implemented under contract, which of the following is key to controlling escalating costs?

A. Risk management
B. Change management
C. Problem management
D. Quality management

Correct Answer: B
Section:

QUESTION 213
Which of the following is the FIRST step in risk assessment?

A. Review risk governance
B. Asset identification
C. Identify risk factors
D. Inherent risk identification

Correct Answer: B
Section:

QUESTION 214
The PRIMARY objective of a risk identification process is to:

A. evaluate how risk conditions are managed.
B. determine threats and vulnerabilities.
C. estimate anticipated financial impact of risk conditions.
D. establish risk response options.

Correct Answer: B
Section:

QUESTION 215
A risk practitioner has received an updated enterprise risk management (ERM) report showing that residual risk is now within the organization's defined appetite and tolerance levels. Which of the following is the risk practitioner's BEST course of action?

A. Identify new risk entries to include in ERM.
B. Remove the risk entries from the ERM register.
C. Re-perform the risk assessment to confirm results.
D. Verify the adequacy of risk monitoring plans.

Correct Answer: D
Section:

QUESTION 216
An organization's risk register contains a large volume of risk scenarios that senior management considers overwhelming. Which of the following would BEST help to improve the risk register?

A. Analyzing the residual risk components
B. Performing risk prioritization
C. Validating the risk appetite level
D. Conducting a risk assessment

Correct Answer: D
Section:

QUESTION 217
Which of the following is MOST important when developing key risk indicators (KRIs)?

A. Alignment with regulatory requirements
B. Availability of qualitative data

C. Properly set thresholds
D. Alignment with industry benchmarks

Correct Answer: C
Section:

QUESTION 218
A risk practitioner has been asked by executives to explain how existing risk treatment plans would affect risk posture at the end of the year. Which of the following is MOST helpful in responding to this request?

A. Assessing risk with no controls in place
B. Showing projected residual risk
C. Providing peer benchmarking results
D. Assessing risk with current controls in place

Correct Answer: D
Section:

QUESTION 219
Which of the following presents the GREATEST risk to change control in business application development over the complete life cycle?

A. Emphasis on multiple application testing cycles
B. Lack of an integrated development environment (IDE) tool
C. Introduction of requirements that have not been approved
D. Bypassing quality requirements before go-live

Correct Answer: C
Section:

QUESTION 220
An IT risk practitioner has determined that mitigation activities differ from an approved risk action plan. Which of the following is the risk practitioner's BEST course of action?

A. Report the observation to the chief risk officer (CRO).
B. Validate the adequacy of the implemented risk mitigation measures.
C. Update the risk register with the implemented risk mitigation actions.
D. Revert the implemented mitigation measures until approval is obtained

Correct Answer: B
Section:

QUESTION 221
Which of the following is MOST important to communicate to senior management during the initial implementation of a risk management program?

A. Regulatory compliance
B. Risk ownership
C. Best practices
D. Desired risk level

Correct Answer: D
Section:

QUESTION 222
Determining if organizational risk is tolerable requires:

A. mapping residual risk with cost of controls
B. comparing against regulatory requirements
C. comparing industry risk appetite with the organization's.
D. understanding the organization's risk appetite.

Correct Answer: D
Section:

QUESTION 223
Which of the following would BEST help an enterprise define and communicate its risk appetite?

A. Gap analysis
B. Risk assessment
C. Heat map
D. Risk register

Correct Answer: C
Section:

QUESTION 224
An IT department has provided a shared drive for personnel to store information to which all employees have access. Which of the following parties is accountable for the risk of potential loss of confidential information?

A. Risk manager
B. Data owner
C. End user
D. IT department

Correct Answer: D
Section:

QUESTION 225
From a risk management perspective, the PRIMARY objective of using maturity models is to enable:

A. solution delivery.
B. resource utilization.
C. strategic alignment.
D. performance evaluation.

Correct Answer: C
Section:

QUESTION 226
During an internal IT audit, an active network account belonging to a former employee was identified. Which of the following is the BEST way to prevent future occurrences?

A. Conduct a comprehensive review of access management processes.
B. Declare a security incident and engage the incident response team.
C. Conduct a comprehensive awareness session for system administrators.
D. Evaluate system administrators' technical skills to identify if training is required.

Correct Answer: A
Section:

QUESTION 227
An organization has initiated a project to launch an IT-based service to customers and take advantage of being the first to market. Which of the following should be of GREATEST concern to senior management?

A. More time has been allotted for testing.
B. The project is likely to deliver the product late.
C. A new project manager is handling the project.
D. The cost of the project will exceed the allotted budget.

Correct Answer: B
Section:

QUESTION 228
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. Data loss
C. Malicious users
D. User support

Correct Answer: B
Section:

QUESTION 229
While conducting an organization-wide risk assessment, it is noted that many of the information security policies have not changed in the past three years. The BEST course of action is to:

A. review and update the policies to align with industry standards.
B. determine that the policies should be updated annually.
C. report that the policies are adequate and do not need to be updated frequently.
D. review the policies against current needs to determine adequacy.

Correct Answer: D
Section:

QUESTION 230
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. Obtain the risk owner's approval.
B. Record the risk as accepted in the risk register.
C. Inform senior management.
D. update the risk response plan.

Correct Answer: A
Section:

QUESTION 231
Which of the following would MOST likely cause a risk practitioner to change the likelihood rating in the risk register?

A. Risk appetite
B. Control cost
C. Control effectiveness
D. Risk tolerance

Correct Answer: C
Section:

QUESTION 232
An organization operates in an environment where reduced time-to-market for new software products is a top business priority. Which of the following should be the risk practitioner's GREATEST concern?

A. Sufficient resources are not assigned to IT development projects.
B. Customer support help desk staff does not have adequate training.
C. Email infrastructure does not have proper rollback plans.
D. The corporate email system does not identify and store phishing emails.

Correct Answer: A
Section:

QUESTION 233
Which of the following BEST mitigates the risk of sensitive personal data leakage from a software development environment?

A. Tokenized personal data only in test environments
B. Data loss prevention tools (DLP) installed in passive mode
C. Anonymized personal data in non-production environments
D. Multi-factor authentication for access to non-production environments

Correct Answer: C
Section:

QUESTION 234
Which of the following should be an element of the risk appetite of an organization?

A. The effectiveness of compensating controls
B. The enterprise's capacity to absorb loss
C. The residual risk affected by preventive controls

D. The amount of inherent risk considered appropriate

Correct Answer: B
Section:

QUESTION 235
In an organization where each division manages risk independently, which of the following would BEST enable management of risk at the enterprise level?

A. A standardized risk taxonomy
B. A list of control deficiencies
C. An enterprise risk ownership policy
D. An updated risk tolerance metric

Correct Answer: A
Section:

QUESTION 236
Which of the following would require updates to an organization's IT risk register?

A. Discovery of an ineffectively designed key IT control
B. Management review of key risk indicators (KRIs)
C. Changes to the team responsible for maintaining the register
D. Completion of the latest internal audit

Correct Answer: A
Section:

QUESTION 237
Which of the following controls BEST helps to ensure that transaction data reaches its destination?

A. Securing the network from attacks
B. Providing acknowledgments from receiver to sender
C. Digitally signing individual messages
D. Encrypting data-in-transit

Correct Answer: B
Section:

QUESTION 238
Which of the following is the BEST control to detect an advanced persistent threat (APT)?

A. Utilizing antivirus systems and firewalls
B. Conducting regular penetration tests
C. Monitoring social media activities
D. Implementing automated log monitoring

Correct Answer: D

Section:

QUESTION 239
Which of the following BEST supports ethical IT risk management practices?

A. Robust organizational communication channels
B. Mapping of key risk indicators (KRIs) to corporate strategy
C. Capability maturity models integrated with risk management frameworks
D. Rigorously enforced operational service level agreements (SLAs)

Correct Answer: A
Section:

QUESTION 240
Which of the following is the MOST effective way to integrate risk and compliance management?

A. Embedding risk management into compliance decision-making
B. Designing corrective actions to improve risk response capabilities
C. Embedding risk management into processes that are aligned with business drivers
D. Conducting regular self-assessments to verify compliance

Correct Answer: A
Section:

QUESTION 241
A business unit is implementing a data analytics platform to enhance its customer relationship management (CRM) system primarily to process data that has been provided by its customers. Which of the following presents the GREATEST risk to the organization's reputation?

A. Third-party software is used for data analytics.
B. Data usage exceeds individual consent.
C. Revenue generated is not disclosed to customers.
D. Use of a data analytics system is not disclosed to customers.

Correct Answer: B
Section:

QUESTION 242
Which of the following should be the MOST important consideration when performing a vendor risk assessment?

A. Results of the last risk assessment of the vendor
B. Inherent risk of the business process supported by the vendor
C. Risk tolerance of the vendor
D. Length of time since the last risk assessment of the vendor

Correct Answer: B
Section:

QUESTION 243
While evaluating control costs, management discovers that the annual cost exceeds the annual loss expectancy (ALE) of the risk. This indicates the:

A. control is ineffective and should be strengthened
B. risk is inefficiently controlled.
C. risk is efficiently controlled.
D. control is weak and should be removed.

Correct Answer: B
Section:

QUESTION 244
The PRIMARY reason to have risk owners assigned to entries in the risk register is to ensure:

A. risk is treated appropriately
B. mitigating actions are prioritized
C. risk entries are regularly updated
D. risk exposure is minimized.

Correct Answer: A
Section:

QUESTION 245
In response to the threat of ransomware, an organization has implemented cybersecurity awareness activities. The risk practitioner's BEST recommendation to further reduce the impact of ransomware attacks would be to implement:

A. two-factor authentication.
B. continuous data backup controls.
C. encryption for data at rest.
D. encryption for data in motion.

Correct Answer: B
Section:

QUESTION 246
Which of the following should a risk practitioner recommend FIRST when an increasing trend of risk events and subsequent losses has been identified?

A. Conduct root cause analyses for risk events.
B. Educate personnel on risk mitigation strategies.
C. Integrate the risk event and incident management processes.
D. Implement controls to prevent future risk events.

Correct Answer: C
Section:

QUESTION 247
When reviewing a report on the performance of control processes, it is MOST important to verify whether the:

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

Correct Answer: D
Section:

QUESTION 248
Which of the following BEST enforces access control for an organization that uses multiple cloud technologies?

A. Senior management support of cloud adoption strategies
B. Creation of a cloud access risk management policy
C. Adoption of a cloud access security broker (CASB) solution
D. Expansion of security information and event management (SIEM) to cloud services

Correct Answer: C
Section:

QUESTION 249
Which of the following scenarios presents the GREATEST risk for a global organization when implementing a data classification policy?

A. Data encryption has not been applied to all sensitive data across the organization.
B. There are many data assets across the organization that need to be classified.
C. Changes to information handling procedures are not documented.
D. Changes to data sensitivity during the data life cycle have not been considered.

Correct Answer: D
Section:

QUESTION 250
Which of the following should be considered when selecting a risk response?

A. Risk scenarios analysis
B. Risk response costs
C. Risk factor awareness
D. Risk factor identification

Correct Answer: B
Section:

QUESTION 251
Which of the following is the MOST important consideration when selecting key risk indicators (KRIs) to monitor risk trends over time?

A. Ongoing availability of data
B. Ability to aggregate data

C. Ability to predict trends
D. Availability of automated reporting systems

Correct Answer: D
Section:

QUESTION 252
Which of the following should be the GREATEST concern for an organization that uses open source software applications?

A. Lack of organizational policy regarding open source software
B. Lack of reliability associated with the use of open source software
C. Lack of monitoring over installation of open source software in the organization
D. Lack of professional support for open source software

Correct Answer: A
Section:

QUESTION 253
An organization has recently been experiencing frequent data corruption incidents. Implementing a file corruption detection tool as a risk response strategy will help to:

A. reduce the likelihood of future events
B. restore availability
C. reduce the impact of future events
D. address the root cause

Correct Answer: D
Section:

QUESTION 254
Accountability for a particular risk is BEST represented in a:

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

Correct Answer: D
Section:

QUESTION 255
Which of the following is MOST likely to cause a key risk indicator (KRI) to exceed thresholds?

A. Occurrences of specific events
B. A performance measurement
C. The risk tolerance level
D. Risk scenarios

Correct Answer: C
Section:

QUESTION 256
Which of the following is the MOST important responsibility of a risk owner?

A. Testing control design
B. Accepting residual risk
C. Establishing business information criteria
D. Establishing the risk register

Correct Answer: C
Section:

QUESTION 257
The PRIMARY objective for requiring an independent review of an organization's IT risk management process should be to:

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

Correct Answer: D
Section:

QUESTION 258
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 a cost-benefit analysis on control options available for implementation.
B. It provides a view on where controls should be applied to maximize the uptime of servers.
C. It provides historical information about the impact of individual servers malfunctioning.
D. It provides a comprehensive view of the impact should the servers simultaneously fail.

Correct Answer: D
Section:

QUESTION 259
An information system for a key business operation is being moved from an in-house application to a Software as a Service (SaaS) vendor. Which of the following will have the GREATEST impact on the ability to monitor risk?

A. Reduced ability to evaluate key risk indicators (KRIs)
B. Reduced access to internal audit reports
C. Dependency on the vendor's key performance indicators (KPIs)
D. Dependency on service level agreements (SLAs)

Correct Answer: A
Section:

QUESTION 260
Key risk indicators (KRIs) are MOST useful during which of the following risk management phases?

A. Monitoring
B. Analysis
C. Identification
D. Response selection

Correct Answer: A
Section:

QUESTION 261
Which of the following BEST enables an organization to determine whether external emerging risk factors will impact the organization's risk profile?

A. Control identification and mitigation
B. Adoption of a compliance-based approach
C. Prevention and detection techniques
D. Scenario analysis and stress testing

Correct Answer: D
Section:

QUESTION 262
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. Establishing an intellectual property agreement
B. Evaluating each of the data sources for vulnerabilities
C. Periodically reviewing big data strategies
D. Benchmarking to industry best practice

Correct Answer: B
Section:

QUESTION 263
A risk practitioner is developing a set of bottom-up IT risk scenarios. The MOST important time to involve business stakeholders is when:

A. updating the risk register
B. documenting the risk scenarios.
C. validating the risk scenarios
D. identifying risk mitigation controls.

Correct Answer: C
Section:

QUESTION 264
A department allows multiple users to perform maintenance on a system using a single set of credentials. A risk practitioner determined this practice to be high-risk. Which of the following is the MOST effective way to mitigate this risk?

A. Single sign-on
B. Audit trail review
C. Multi-factor authentication
D. Data encryption at rest

Correct Answer: B
Section:

QUESTION 265
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.

Correct Answer: D
Section:

QUESTION 266
Which of the following BEST informs decision-makers about the value of a notice and consent control for the collection of personal information?

A. A comparison of the costs of notice and consent control options
B. Examples of regulatory fines incurred by industry peers for noncompliance
C. A report of critical controls showing the importance of notice and consent
D. A cost-benefit analysis of the control versus probable legal action

Correct Answer: D
Section:

QUESTION 267
Which of the following is MOST important for a risk practitioner to verify when evaluating the effectiveness of an organization's existing controls?

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

Correct Answer: C
Section:

QUESTION 268
Which of the following would be the BEST key performance indicator (KPI) for monitoring the effectiveness of the IT asset management process?

A. Percentage of unpatched IT assets
B. Percentage of IT assets without ownership

C. The number of IT assets securely disposed during the past year
D. The number of IT assets procured during the previous month

Correct Answer: B
Section:

QUESTION 269
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. A cost-benefit analysis
C. The risk management framework D, A roadmap of IT strategic planning

Correct Answer: B
Section:

QUESTION 270
Which of the following BEST indicates that an organization has implemented IT performance requirements?

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

Correct Answer: A
Section:

QUESTION 271
The BEST reason to classify IT assets during a risk assessment is to determine the:

A. priority in the risk register.
B. business process owner.
C. enterprise risk profile.
D. appropriate level of protection.

Correct Answer: D
Section:

QUESTION 272
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

Correct Answer: A

Section:

QUESTION 273
When a high-risk security breach occurs, which of the following would be MOST important to the person responsible for managing the incident?

A. An analysis of the security logs that illustrate the sequence of events
B. An analysis of the impact of similar attacks in other organizations
C. A business case for implementing stronger logical access controls
D. A justification of corrective action taken

Correct Answer: B
Section:

QUESTION 274
Which of the following BEST indicates how well a web infrastructure protects critical information from an attacker?

A. Failed login attempts
B. Simulating a denial of service attack
C. Absence of IT audit findings
D. Penetration test

Correct Answer: D
Section:

QUESTION 275
Which of the following BEST enables a risk practitioner to enhance understanding of risk among stakeholders?

A. Key risk indicators (KRIs)
B. Risk scenarios
C. Business impact analysis (BIA)
D. Threat analysis

Correct Answer: B
Section:

QUESTION 276
Which of the following is the GREATEST concern associated with redundant data in an organization's inventory system?

A. Poor access control
B. Unnecessary data storage usage
C. Data inconsistency
D. Unnecessary costs of program changes

Correct Answer: C
Section:

QUESTION 277

What is the PRIMARY benefit of risk monitoring?

A. It reduces the number of audit findings.
B. It provides statistical evidence of control efficiency.
C. It facilitates risk-aware decision making.
D. It facilitates communication of threat levels.

Correct Answer: C
Section:

QUESTION 278
Which of the following statements describes the relationship between key risk indicators (KRIs) and key control indicators (KCIs)?

A. KRI design must precede definition of KCIs.
B. KCIs and KRIs are independent indicators and do not impact each other.
C. A decreasing trend of KRI readings will lead to changes to KCIs.
D. Both KRIs and KCIs provide insight to potential changes in the level of risk.

Correct Answer: A
Section:

QUESTION 279
Which of the following trends would cause the GREATEST concern regarding the effectiveness of an organization's user access control processes? An increase in the:

A. ratio of disabled to active user accounts.
B. percentage of users with multiple user accounts.
C. average number of access entitlements per user account.
D. average time between user transfers and access updates.

Correct Answer: D
Section:

QUESTION 280
Which of the following is the MOST important objective of an enterprise risk management (ERM) program?

A. To create a complete repository of risk to the organization
B. To create a comprehensive view of critical risk to the organization
C. To provide a bottom-up view of the most significant risk scenarios
D. To optimize costs of managing risk scenarios in the organization

Correct Answer: B
Section:

QUESTION 281
To help identify high-risk situations, an organization should:

A. continuously monitor the environment.

B. develop key performance indicators (KPIs).
C. maintain a risk matrix.
D. maintain a risk register.

Correct Answer: A
Section:

QUESTION 282
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

Correct Answer: A
Section:

QUESTION 283
Which of the following is the BEST evidence that risk management is driving business decisions in an organization?

A. Compliance breaches are addressed in a timely manner.
B. Risk ownership is identified and assigned.
C. Risk treatment options receive adequate funding.
D. Residual risk is within risk tolerance.

Correct Answer: B
Section:

QUESTION 284
A maturity model is MOST useful to an organization when it:

A. benchmarks against other organizations
B. defines a qualitative measure of risk
C. provides a reference for progress
D. provides risk metrics.

Correct Answer: C
Section:

QUESTION 285
A risk practitioner is preparing a report to communicate changes in the risk and control environment. The BEST way to engage stakeholder attention is to:

A. include detailed deviations from industry benchmarks,
B. include a summary linking information to stakeholder needs,
C. include a roadmap to achieve operational excellence,
D. publish the report on-demand for stakeholders.

Correct Answer: B
Section:

QUESTION 286
The PRIMARY advantage of involving end users in continuity planning is that they:

A. have a better understanding of specific business needs
B. can balance the overall technical and business concerns
C. can see the overall impact to the business
D. are more objective than information security management.

Correct Answer: B
Section:

QUESTION 287
Which of the following is MOST important to the effectiveness of key performance indicators (KPIs)?

A. Relevance
B. Annual review
C. Automation
D. Management approval

Correct Answer: A
Section:

QUESTION 288
Which of the following is the PRIMARY reason to adopt key control indicators (KCIs) in the risk monitoring and reporting process?

A. To provide data for establishing the risk profile
B. To provide assurance of adherence to risk management policies
C. To provide measurements on the potential for risk to occur
D. To provide assessments of mitigation effectiveness

Correct Answer: D
Section:

QUESTION 289
The PRIMARY benefit of using a maturity model is that it helps to evaluate the:

A. capability to implement new processes
B. evolution of process improvements
C. degree of compliance with policies and procedures
D. control requirements.

Correct Answer: B
Section:

QUESTION 290
Which of the following provides the BEST evidence that a selected risk treatment plan is effective?

A. Identifying key risk indicators (KRIs)
B. Evaluating the return on investment (ROI)
C. Evaluating the residual risk level
D. Performing a cost-benefit analysis

Correct Answer: D
Section:

QUESTION 291
Senior management has asked the risk practitioner for the overall residual risk level for a process that contains numerous risk scenarios. Which of the following should be provided?

A. The sum of residual risk levels for each scenario
B. The loss expectancy for aggregated risk scenarios
C. The highest loss expectancy among the risk scenarios
D. The average of anticipated residual risk levels

Correct Answer: D
Section:
Explanation:
Topic 4, Exam Pool D

QUESTION 292
Which of the following is the PRIMARY benefit of stakeholder involvement in risk scenario development?

A. Ability to determine business impact
B. Up-to-date knowledge on risk responses
C. Decision-making authority for risk treatment
D. Awareness of emerging business threats

Correct Answer: A
Section:

QUESTION 293
Which of the following is MOST helpful to understand the consequences of an IT risk event?

A. Fault tree analysis
B. Historical trend analysis
C. Root cause analysis
D. Business impact analysis (BIA)

Correct Answer: B
Section:

QUESTION 294

Which of the following is the BEST way to help ensure risk will be managed properly after a business process has been re-engineered?

A. Reassessing control effectiveness of the process
B. Conducting a post-implementation review to determine lessons learned
C. Reporting key performance indicators (KPIs) for core processes
D. Establishing escalation procedures for anomaly events

Correct Answer: A
Section:

QUESTION 295
Which of the following would be a risk practitioner's BEST course of action when a project team has accepted a risk outside the established risk appetite?

A. Reject the risk acceptance and require mitigating controls.
B. Monitor the residual risk level of the accepted risk.
C. Escalate the risk decision to the project sponsor for review.
D. Document the risk decision in the project risk register.

Correct Answer: B
Section:

QUESTION 296
When reviewing the business continuity plan (BCP) of an online sales order system, a risk practitioner notices that the recovery time objective (RTO) has a shorter lime than what is defined in the disaster recovery plan (DRP). Which of the following is the BEST way for the risk practitioner to address this concern?

A. Adopt the RTO defined in the BCR
B. Update the risk register to reflect the discrepancy.
C. Adopt the RTO defined in the DRP.
D. Communicate the discrepancy to the DR manager for follow-up.

Correct Answer: D
Section:

QUESTION 297
Which of the following is MOST important for maintaining the effectiveness of an IT risk register?

A. Removing entries from the register after the risk has been treated
B. Recording and tracking the status of risk response plans within the register
C. Communicating the register to key stakeholders
D. Performing regular reviews and updates to the register

Correct Answer: D
Section:

QUESTION 298
Which of the following is the MOST important consideration when developing risk strategies?

A. Organization's industry sector
B. Long-term organizational goals
C. Concerns of the business process owners
D. History of risk events

Correct Answer: B
Section:

QUESTION 299
An organization wants to grant remote access to a system containing sensitive data to an overseas third party. Which of the following should be of GREATEST concern to management?

A. Transborder data transfer restrictions
B. Differences in regional standards
C. Lack of monitoring over vendor activities
D. Lack of after-hours incident management support

Correct Answer: C
Section:

QUESTION 300
Which of the following stakeholders are typically included as part of a line of defense within the three lines of defense model?

A. Board of directors
B. Vendors
C. Regulators
D. Legal team

Correct Answer: A
Section:

QUESTION 301
Which of the following will BEST help to ensure new IT policies address the enterprise's requirements?

A. involve IT leadership in the policy development process
B. Require business users to sign acknowledgment of the poises
C. involve business owners in the pokey development process
D. Provide policy owners with greater enforcement authority

Correct Answer: B
Section:

QUESTION 302
A multinational organization is considering implementing standard background checks to' all new employees A KEY concern regarding this approach

A. fail to identity all relevant issues.
B. be too costly
C. violate laws in other countries

D. be too line consuming

Correct Answer: C
Section:

QUESTION 303
An organization's control environment is MOST effective when:

A. controls perform as intended.
B. controls operate efficiently.
C. controls are implemented consistent
D. control designs are reviewed periodically

Correct Answer: A
Section:

QUESTION 304
Who is BEST suited to provide objective input when updating residual risk to reflect the results of control effectiveness?

A. Control owner
B. Risk owner
C. Internal auditor
D. Compliance manager

Correct Answer: C
Section:

QUESTION 305
The following is the snapshot of a recently approved IT risk register maintained by an organization's information security department.

Risk ID	Risk Title	Risk Description	Risk Submitter	Risk Owner	Control Owner(s)	Risk Likelihood Rating	Risk Impact Rating	Risk Exposure	Risk Response Type	Risk Response Description
R001	Mobile Data Theft	Laptops and mobile devices can be lost or stolen leading to data compromise.	Risk Council	End-User Computing Manager AND Inventory	IT Operations Manager AND Security Operations Manager	Low Likelihood	Very Serious	0.120	Mitigate	Purchase and acquire data encryption software for mobile
R003	Fire Hazard	A fire accident may destroy data center equipment and servers leading to loss of availability and services.	Information Security Department	Data Center Facilities Manager	Facilities Manager	Low Likelihood	Serious	0.060	Transfer	Buy fire hazard insurance policy
		A disgruntled								

Significant	0.10	Low Likelihood	0.30
Serious	0.20	Likely	0.50
Very Serious	0.40	Highly Likely	0.70
Catastrophic	0.80	Near Certainty	0.90

After implementing countermeasures listed in ''Risk Response Descriptions'' for each of the Risk IDs, which of the following component of the register MUST change?

A. Risk Impact Rating
B. Risk Owner
C. Risk Likelihood Rating
D. Risk Exposure

Correct Answer: B
Section:

QUESTION 306
Of the following, who is BEST suited to assist a risk practitioner in developing a relevant set of risk scenarios?

A. Internal auditor
B. Asset owner
C. Finance manager
D. Control owner

Correct Answer: B
Section:

QUESTION 307
An organization has made a decision to purchase a new IT system. During when phase of the system development life cycle (SDLC) will identified risk MOST likely lead to architecture and design trade-offs?

A. Acquisition
B. Implementation

C. Initiation
D. Operation and maintenance

Correct Answer: C
Section:

QUESTION 308
Recovery the objectives (RTOs) should be based on

A. minimum tolerable downtime
B. minimum tolerable loss of data.
C. maximum tolerable downtime.
D. maximum tolerable loss of data

Correct Answer: C
Section:

QUESTION 309
Which of the following issues found during the review of a newly created disaster recovery plan (DRP) should be of MOST concern?

A. Some critical business applications are not included in the plan
B. Several recovery activities will be outsourced
C. The plan is not based on an internationally recognized framework
D. The chief information security officer (CISO) has not approved the plan

Correct Answer: A
Section:

QUESTION 310
Which of the following is MOST helpful in defining an early-warning threshold associated with insufficient network bandwidth''

A. Average bandwidth usage
B. Peak bandwidth usage
C. Total bandwidth usage
D. Bandwidth used during business hours

Correct Answer: A
Section:

QUESTION 311
An organization maintains independent departmental risk registers that are not automatically aggregated. Which of the following is the GREATEST concern?

A. Management may be unable to accurately evaluate the risk profile.
B. Resources may be inefficiently allocated.
C. The same risk factor may be identified in multiple areas.
D. Multiple risk treatment efforts may be initiated to treat a given risk.

Correct Answer: A
Section:

QUESTION 312
it was determined that replication of a critical database used by two business units failed. Which of the following should be of GREATEST concern1?

A. The underutilization of the replicated link
B. The cost of recovering the data
C. The lack of integrity of data
D. The loss of data confidentiality

Correct Answer: C
Section:

QUESTION 313
Which of the following contributes MOST to the effective implementation of risk responses?

A. Clear understanding of the risk
B. Comparable industry risk trends
C. Appropriate resources
D. Detailed standards and procedures

Correct Answer: A
Section:

QUESTION 314
As pan of business continuity planning, which of the following is MOST important to include m a business impact analysis (BIA)?

A. An assessment of threats to the organization
B. An assessment of recovery scenarios
C. industry standard framework
D. Documentation of testing procedures

Correct Answer: A
Section:

QUESTION 315
Which of the following would BEST mitigate an identified risk scenario?

A. Conducting awareness training
B. Executing a risk response plan
C. Establishing an organization's risk tolerance
D. Performing periodic audits

Correct Answer: C
Section:

QUESTION 316
An organization has decided to commit to a business activity with the knowledge that the risk exposure is higher than the risk appetite. Which of the following is the risk practitioner's MOST important action related to this decision?

A. Recommend risk remediation
B. Change the level of risk appetite
C. Document formal acceptance of the risk
D. Reject the business initiative

Correct Answer: C
Section:

QUESTION 317
An organization is considering outsourcing user administration controls tor a critical system. The potential vendor has offered to perform quarterly sett-audits of its controls instead of having annual independent audits. Which of the following should be of GREATEST concern to me risk practitioner?

A. The controls may not be properly tested
B. The vendor will not ensure against control failure
C. The vendor will not achieve best practices
D. Lack of a risk-based approach to access control

Correct Answer: D
Section:

QUESTION 318
Which of the following would BEST mitigate the ongoing risk associated with operating system (OS) vulnerabilities?

A. Temporarily mitigate the OS vulnerabilities
B. Document and implement a patching process
C. Evaluate permanent fixes such as patches and upgrades
D. Identify the vulnerabilities and applicable OS patches

Correct Answer: B
Section:

QUESTION 319
Which of the following would BEST enable a risk-based decision when considering the use of an emerging technology for data processing?

A. Gap analysis
B. Threat assessment
C. Resource skills matrix
D. Data quality assurance plan

Correct Answer: A
Section:

QUESTION 320

An organization has an approved bring your own device (BYOD) policy. Which of the following would BEST mitigate the security risk associated with the inappropriate use of enterprise applications on the devices?

A. Periodically review application on BYOD devices
B. Include BYOD in organizational awareness programs
C. Implement BYOD mobile device management (MDM) controls.
D. Enable a remote wee capability for BYOD devices

Correct Answer: C
Section:

QUESTION 321
Which key performance efficiency IKPI) BEST measures the effectiveness of an organization's disaster recovery program?

A. Number of service level agreement (SLA) violations
B. Percentage of recovery issues identified during the exercise
C. Number of total systems recovered within tie recovery point objective (RPO)
D. Percentage of critical systems recovered within tie recovery time objective (RTO)

Correct Answer: D
Section:

QUESTION 322
Which of the following will BEST help to ensure the continued effectiveness of the IT risk management function within an organization experiencing high employee turnover?

A. Well documented policies and procedures
B. Risk and issue tracking
C. An IT strategy committee
D. Change and release management

Correct Answer: B
Section:

QUESTION 323
An organization has decided to use an external auditor to review the control environment of an outsourced service provider. The BEST control criteria to evaluate the provider would be based on:

A. a recognized industry control framework
B. guidance provided by the external auditor
C. the service provider's existing controls
D. The organization's specific control requirements

Correct Answer: D
Section:

QUESTION 324
A company has recently acquired a customer relationship management (CRM) application from a certified software vendor. Which of the following will BE ST help lo prevent technical vulnerabilities from being exploded?

A. implement code reviews and Quality assurance on a regular basis

B. Verity me software agreement indemnifies the company from losses
C. Review the source coda and error reporting of the application
D. Update the software with the latest patches and updates

Correct Answer: D
Section:

QUESTION 325
Which of the following is MOST important information to review when developing plans for using emerging technologies?

A. Existing IT environment
B. IT strategic plan
C. Risk register
D. Organizational strategic plan

Correct Answer: D
Section:

QUESTION 326
What is the PRIMARY reason an organization should include background checks on roles with elevated access to production as part of its hiring process?

A. Reduce internal threats
B. Reduce exposure to vulnerabilities
C. Eliminate risk associated with personnel
D. Ensure new hires have the required skills

Correct Answer: C
Section:

QUESTION 327
Before assigning sensitivity levels to information it is MOST important to:

A. define recovery time objectives (RTOs).
B. define the information classification policy
C. conduct a sensitivity analyse
D. Identify information custodians

Correct Answer: B
Section:

QUESTION 328
An organization has used generic risk scenarios to populate its risk register. Which of the following presents the GREATEST challenge to assigning of the associated risk entries?

A. The volume of risk scenarios is too large
B. Risk aggregation has not been completed
C. Risk scenarios are not applicable
D. The risk analysts for each scenario is incomplete

Correct Answer: D
Section:

QUESTION 329
When of the following standard operating procedure (SOP) statements BEST illustrates appropriate risk register maintenance?

A. Remove risk that has been mitigated by third-party transfer
B. Remove risk that management has decided to accept
C. Remove risk only following a significant change in the risk environment
D. Remove risk when mitigation results in residual risk within tolerance levels

Correct Answer: C
Section:

QUESTION 330
Which of the blowing is MOST important when implementing an organization s security policy?

A. Obtaining management support
B. Benchmarking against industry standards
C. Assessing compliance requirements
D. Identifying threats and vulnerabilities

Correct Answer: A
Section:

QUESTION 331
A cote data center went offline abruptly for several hours affecting many transactions across multiple locations. Which of the to' owing would provide the MOST useful information to determine mitigating controls?

A. Forensic analysis
B. Risk assessment
C. Root cause analysis
D. Business impact analysis (BlA)

Correct Answer: A
Section:

QUESTION 332
A risk practitioner observed Vial a high number of pokey exceptions were approved by senior management. Which of the following is the risk practitioner's BEST course of action to determine root cause?

A. Review the risk profile
B. Review pokey change history
C. interview the control owner
D. Perform control testing

Correct Answer: C
Section:

QUESTION 333
The BEST way to mitigate the high cost of retrieving electronic evidence associated with potential litigation is to implement policies and procedures for.

A. data logging and monitoring
B. data mining and analytics
C. data classification and labeling
D. data retention and destruction

Correct Answer: C
Section:

QUESTION 334
An organization has completed a risk assessment of one of its service providers. Who should be accountable for ensuring that risk responses are implemented?

A. IT risk practitioner
B. Third -partf3ecurity team
C. The relationship owner
D. Legal representation of the business

Correct Answer: C
Section:

QUESTION 335
Which of the following would MOST likely require a risk practitioner to update the risk register?

A. An alert being reported by the security operations center.
B. Development of a project schedule for implementing a risk response
C. Completion of a project for implementing a new control
D. Engagement of a third party to conduct a vulnerability scan

Correct Answer: C
Section:

QUESTION 336
An IT risk threat analysis is BEST used to establish

A. risk scenarios
B. risk maps
C. risk appetite
D. risk ownership.

Correct Answer: A
Section:

QUESTION 337
Which of the following is a risk practitioner's MOST important responsibility in managing risk acceptance that exceeds risk tolerance?

A. Verify authorization by senior management.
B. Increase the risk appetite to align with the current risk level
C. Ensure the acceptance is set to expire over lime
D. Update the risk response in the risk register.

Correct Answer: A
Section:

QUESTION 338
Which of the following would provide the BEST evidence of an effective internal control environment/?

A. Risk assessment results
B. Adherence to governing policies
C. Regular stakeholder briefings
D. Independent audit results

Correct Answer: D
Section:

QUESTION 339
An organization is concerned that its employees may be unintentionally disclosing data through the use of social media sites. Which of the following will MOST effectively mitigate tins risk?

A. Requiring the use of virtual private networks (VPNs)
B. Establishing a data classification policy
C. Conducting user awareness training
D. Requiring employee agreement of the acceptable use policy

Correct Answer: C
Section:

QUESTION 340
Who should be responsible (of evaluating the residual risk after a compensating control has been

A. Compliance manager
B. Risk owner
C. Control owner
D. Risk practitioner

Correct Answer: D
Section:

QUESTION 341
A global company s business continuity plan (BCP) requires the transfer of its customer information....
event of a disaster. Which of the following should be the MOST important risk consideration?

A. The difference In the management practices between each company
B. The cloud computing environment is shared with another company

C. The lack of a service level agreement (SLA) in the vendor contract
D. The organizational culture differences between each country

Correct Answer: B
Section:

QUESTION 342
Which of the following is the BEST approach to mitigate the risk associated with a control deficiency?

A. Perform a business case analysis
B. Implement compensating controls.
C. Conduct a control sell-assessment (CSA)
D. Build a provision for risk

Correct Answer: C
Section:

QUESTION 343
Which of the following is PRIMARILY a risk management responsibly of the first line of defense?

A. Implementing risk treatment plans
B. Validating the status of risk mitigation efforts
C. Establishing risk policies and standards
D. Conducting independent reviews of risk assessment results

Correct Answer: C
Section:

QUESTION 344
Which of the following would be the GREATEST concern for an IT risk practitioner when an employees.....

A. The organization's structure has not been updated
B. Unnecessary access permissions have not been removed.
C. Company equipment has not been retained by IT
D. Job knowledge was not transferred to employees m the former department

Correct Answer: B
Section:

QUESTION 345
Which of the following is the BEST indication that key risk indicators (KRIs) should be revised?

A. A decrease in the number of critical assets covered by risk thresholds
B. An Increase In the number of risk threshold exceptions
C. An increase in the number of change events pending management review
D. A decrease In the number of key performance indicators (KPIs)

Correct Answer: B
Section:

QUESTION 346
In order to determining a risk is under-controlled the risk practitioner will need to

A. understand the risk tolerance
B. monitor and evaluate IT performance
C. identify risk management best practices
D. determine the sufficiency of the IT risk budget

Correct Answer: A
Section:

QUESTION 347
An organization is considering the adoption of an aggressive business strategy to achieve desired growth From a risk management perspective what should the risk practitioner do NEXT?

A. Identify new threats resorting from the new business strategy
B. Update risk awareness training to reflect current levels of risk appetite and tolerance
C. Inform the board of potential risk scenarios associated with aggressive business strategies
D. Increase the scale for measuring impact due to threat materialization

Correct Answer: A
Section:

QUESTION 348
Which of the following practices would be MOST effective in protecting personality identifiable information (Ptl) from unauthorized access m a cloud environment?

A. Apply data classification policy
B. Utilize encryption with logical access controls
C. Require logical separation of company data
D. Obtain the right to audit

Correct Answer: B
Section:

QUESTION 349
Which of the following is MOST important to the effectiveness of key performance indicators (KPIs)?

A. Management approval
B. Annual review
C. Relevance
D. Automation

Correct Answer: A
Section:

QUESTION 350
Which of the following is the MOST comprehensive resource for prioritizing the implementation of information systems controls?

A. Data classification policy
B. Emerging technology trends
C. The IT strategic plan
D. The risk register

Correct Answer: C
Section:

QUESTION 351
Which of the following will BEST help to ensure implementation of corrective action plans?

A. Establishing employee awareness training
B. Assigning accountability to risk owners
C. Selling target dates to complete actions
D. Contracting to third parties

Correct Answer: B
Section:

QUESTION 352
Which of the following would BEST facilitate the implementation of data classification requirements?

A. Implementing a data toss prevention (DLP) solution
B. Assigning a data owner
C. Scheduling periodic audits
D. Implementing technical controls over the assets

Correct Answer: B
Section:

QUESTION 353
Which of the following is MOST important for mitigating ethical risk when establishing accountability for control ownership?

A. Ensuring processes are documented to enable effective control execution
B. Ensuring regular risk messaging is Included in business communications from leadership
C. Ensuring schedules and deadlines for control-related deliverables are strictly monitored
D. Ensuring performance metrics balance business goals with risk appetiie

Correct Answer: B
Section:

QUESTION 354
Which of the following management action will MOST likely change the likelihood rating of a risk scenario related to remote network access?

A. Updating the organizational policy for remote access
B. Creating metrics to track remote connections
C. Implementing multi-factor authentication
D. Updating remote desktop software

Correct Answer: A
Section:

QUESTION 355
After the implementation of internal of Things (IoT) devices, new risk scenarios were identified. What is the PRIMARY reason to report this information to risk owners?

A. To reevaluate continued use to IoT devices
B. The add new controls to mitigate the risk
C. The recommend changes to the IoT policy
D. To confirm the impact to the risk profile

Correct Answer: D
Section:

QUESTION 356
An organization control environment is MOST effective when:

A. control designs are reviewed periodically
B. controls perform as intended.
C. controls are implemented consistently.
D. controls operate efficiently

Correct Answer: B
Section:

QUESTION 357
When is the BEST to identify risk associated with major project to determine a mitigation plan?

A. Project execution phase
B. Project initiation phase
C. Project closing phase
D. Project planning phase

Correct Answer: D
Section:

QUESTION 358
The PRIMARY objective of collecting information and reviewing documentation when performing periodic risk analysis should be to:

A. Identify new or emerging risk issues.
B. Satisfy audit requirements.
C. Survey and analyze historical risk data.

D. Understand internal and external threat agents.

Correct Answer: D
Section:

QUESTION 359
An organization is analyzing the risk of shadow IT usage. Which of the following is the MOST important input into the assessment?

A. Business benefits of shadow IT
B. Application-related expresses
C. Classification of the data
D. Volume of data

Correct Answer: A
Section:

QUESTION 360
Which of the following would be a risk practitioner's BEST recommendation upon learning of an updated cybersecurity regulation that could impact the organization?

A. Perform a gap analysis
B. Conduct system testing
C. Implement compensating controls
D. Update security policies

Correct Answer: A
Section:

QUESTION 361
It is MOST important that security controls for a new system be documented in:

A. testing requirements
B. the implementation plan.
C. System requirements
D. The security policy

Correct Answer: C
Section:

QUESTION 362
An organization is planning to move its application infrastructure from on-premises to the cloud. Which of the following is the BEST course of the actin to address the risk associated with data transfer if the relationship is terminated with the vendor?

A. Meet with the business leaders to ensure the classification of their transferred data is in place
B. Ensure the language in the contract explicitly states who is accountable for each step of the data transfer process
C. Collect requirements for the environment to ensure the infrastructure as a service (IaaS) is configured appropriately.
D. Work closely with the information security officer to ensure the company has the proper security controls in place.

Correct Answer: B
Section:

QUESTION 363
Which of the following would be the result of a significant increase in the motivation of a malicious threat actor?

A. Increase in mitigating control costs
B. Increase in risk event impact
C. Increase in risk event likelihood
D. Increase in cybersecurity premium

Correct Answer: C
Section:

QUESTION 364
Which of the following would BEST facilitate the implementation of data classification requirements?

A. Assigning a data owner
B. Implementing technical control over the assets
C. Implementing a data loss prevention (DLP) solution
D. Scheduling periodic audits

Correct Answer: A
Section:

QUESTION 365
Which of the following sources is MOST relevant to reference when updating security awareness training materials?

A. Risk management framework
B. Risk register
C. Global security standards
D. Recent security incidents reported by competitors

Correct Answer: B
Section:

QUESTION 366
Which of the following should be of MOST concern to a risk practitioner reviewing an organization risk register after the completion of a series of risk assessments?

A. Several risk action plans have missed target completion dates.
B. Senior management has accepted more risk than usual.
C. Risk associated with many assets is only expressed in qualitative terms.
D. Many risk scenarios are owned by the same senior manager.

Correct Answer: A
Section:

QUESTION 367
When documenting a risk response, which of the following provides the STRONGEST evidence to support the decision?

A. Verbal majority acceptance of risk by committee
B. List of compensating controls
C. IT audit follow-up responses
D. A memo indicating risk acceptance

Correct Answer: C
Section:

QUESTION 368
Which of the following would MOST effectively reduce risk associated with an increase of online transactions on a retailer website?

A. Scalable infrastructure
B. A hot backup site
C. Transaction limits
D. Website activity monitoring

Correct Answer: C
Section:

QUESTION 369
Which of the following is the BEST method of creating risk awareness in an organization?

A. Marking the risk register available to project stakeholders
B. Ensuring senior management commitment to risk training
C. Providing regular communication to risk managers
D. Appointing the risk manager from the business units

Correct Answer: B
Section:

QUESTION 370
A bank recently incorporated Blockchain technology with the potential to impact known risk within the organization. Which of the following is the risk practitioner's BEST course of action?

A. Determine whether risk responses are still adequate.
B. Analyze and update control assessments with the new processes.
C. Analyze the risk and update the risk register as needed.
D. Conduct testing of the control that mitigate the existing risk.

Correct Answer: B
Section:

QUESTION 371
When developing risk scenario using a list of generic scenarios based on industry best practices, it is MOST imported to:

A. Assess generic risk scenarios with business users.
B. Validate the generic risk scenarios for relevance.
C. Select the maximum possible risk scenarios from the list.
D. Identify common threats causing generic risk scenarios

Correct Answer: B
Section:

QUESTION 372
Which of the following would be a risk practitioner's GREATEST concern with the use of a vulnerability scanning tool?

A. Increased time to remediate vulnerabilities
B. Inaccurate reporting of results
C. Increased number of vulnerabilities
D. Network performance degradation

Correct Answer: B
Section:

QUESTION 373
Which of the following is the PRIMARY reason to perform periodic vendor risk assessments?

A. To provide input to the organization's risk appetite
B. To monitor the vendor's control effectiveness
C. To verify the vendor's ongoing financial viability
D. To assess the vendor's risk mitigation plans

Correct Answer: B
Section:

QUESTION 374
Which of the following is the MOST important objective from a cost perspective for considering aggregated risk responses in an organization?

A. Prioritize risk response options
B. Reduce likelihood.
C. Address more than one risk response
D. Reduce impact

Correct Answer: C
Section:

QUESTION 375
Which of the following is MOST helpful in providing an overview of an organization's risk management program?

A. Risk management treatment plan
B. Risk assessment results
C. Risk management framework

D. Risk register

Correct Answer: C
Section:

QUESTION 376
Effective risk communication BEST benefits an organization by:

A. helping personnel make better-informed decisions
B. assisting the development of a risk register.
C. improving the effectiveness of IT controls.
D. increasing participation in the risk assessment process.

Correct Answer: A
Section:

QUESTION 377
Which of the following is the BEST control to minimize the risk associated with scope creep in software development?

A. An established process for project change management
B. Retention of test data and results for review purposes
C. Business managements review of functional requirements
D. Segregation between development, test, and production

Correct Answer: A
Section:

QUESTION 378
An organization has recently hired a large number of part-time employees. During the annual audit, it was discovered that many user IDs and passwords were documented in procedure manuals for use by the part-time employees. Which of the following BEST describes this situation?

A. Threat
B. Risk
C. Vulnerability
D. Policy violation

Correct Answer: B
Section:

QUESTION 379
Which of the following is MOST important to update when an organization's risk appetite changes?

A. Key risk indicators (KRIs)
B. Risk reporting methodology
C. Key performance indicators (KPIs)
D. Risk taxonomy

Correct Answer: A
Section:

QUESTION 380
The BEST key performance indicator (KPI) to measure the effectiveness of the security patching process is the percentage of patches installed:

A. by the security administration team.
B. successfully within the expected time frame.
C. successfully during the first attempt.
D. without causing an unplanned system outage.

Correct Answer: B
Section:

QUESTION 381
In order to efficiently execute a risk response action plan, it is MOST important for the emergency response team members to understand:

A. system architecture in target areas.
B. IT management policies and procedures.
C. business objectives of the organization.
D. defined roles and responsibilities.

Correct Answer: D
Section:

QUESTION 382
Which of the following is the BEST indicator of executive management's support for IT risk mitigation efforts?

A. The number of stakeholders involved in IT risk identification workshops
B. The percentage of corporate budget allocated to IT risk activities
C. The percentage of incidents presented to the board
D. The number of executives attending IT security awareness training

Correct Answer: B
Section:

QUESTION 383
Which of the following BEST enables risk-based decision making in support of a business continuity plan (BCP)?

A. Impact analysis
B. Control analysis
C. Root cause analysis
D. Threat analysis

Correct Answer: A
Section:

QUESTION 384
Which of the following is MOST important for senior management to review during an acquisition?

A. Risk appetite and tolerance
B. Risk framework and methodology
C. Key risk indicator (KRI) thresholds
D. Risk communication plan

Correct Answer: A
Section:

QUESTION 385
Senior management wants to increase investment in the organization's cybersecurity program in response to changes in the external threat landscape. Which of the following would BEST help to prioritize investment efforts?

A. Analyzing cyber intelligence reports
B. Engaging independent cybersecurity consultants
C. Increasing the frequency of updates to the risk register
D. Reviewing the outcome of the latest security risk assessment

Correct Answer: D
Section:

QUESTION 386
A recent vulnerability assessment of a web-facing application revealed several weaknesses. Which of the following should be done NEXT to determine the risk exposure?

A. Code review
B. Penetration test
C. Gap assessment
D. Business impact analysis (BIA)

Correct Answer: B
Section:

QUESTION 387
Which of the following should be of GREATEST concern when reviewing the results of an independent control assessment to determine the effectiveness of a vendor's control environment?

A. The report was provided directly from the vendor.
B. The risk associated with multiple control gaps was accepted.
C. The control owners disagreed with the auditor's recommendations.
D. The controls had recurring noncompliance.

Correct Answer: A
Section:

QUESTION 388
Which of the following is the MOST critical factor to consider when determining an organization's risk appetite?

A. Fiscal management practices
B. Business maturity
C. Budget for implementing security
D. Management culture

Correct Answer: D
Section:

QUESTION 389
Which of the following is the MOST important key performance indicator (KPI) to monitor the effectiveness of disaster recovery processes?

A. Percentage of IT systems recovered within the mean time to restore (MTTR) during the disaster recovery test
B. Percentage of issues arising from the disaster recovery test resolved on time
C. Percentage of IT systems included in the disaster recovery test scope
D. Percentage of IT systems meeting the recovery time objective (RTO) during the disaster recovery test

Correct Answer: D
Section:

QUESTION 390
An organization wants to launch a campaign to advertise a new product Using data analytics, the campaign can be targeted to reach potential customers. Which of the following should be of GREATEST concern to the risk practitioner?

A. Data minimization
B. Accountability
C. Accuracy
D. Purpose limitation

Correct Answer: D
Section:

QUESTION 391
A risk practitioner is utilizing a risk heat map during a risk assessment. Risk events that are coded with the same color will have a similar:

A. risk score
B. risk impact
C. risk response
D. risk likelihood.

Correct Answer: B
Section:

QUESTION 392
A recent risk workshop has identified risk owners and responses for newly identified risk scenarios. Which of the following should be the risk practitioner's NEXT step?

A. Develop a mechanism for monitoring residual risk.
B. Update the risk register with the results.

C. Prepare a business case for the response options.
D. Identify resources for implementing responses.

Correct Answer: C
Section:

QUESTION 393
The objective of aligning mitigating controls to risk appetite is to ensure that:

A. exposures are reduced to the fullest extent
B. exposures are reduced only for critical business systems
C. insurance costs are minimized
D. the cost of controls does not exceed the expected loss.

Correct Answer: D
Section:

QUESTION 394
An organization has decided to postpone the assessment and treatment of several risk scenarios because stakeholders are unavailable. As a result of this decision, the risk associated with these new entries has been;

A. mitigated
B. deferred
C. accepted.
D. transferred

Correct Answer: C
Section:

QUESTION 395
When a risk practitioner is determining a system's criticality. it is MOST helpful to review the associated:

A. process flow.
B. business impact analysis (BIA).
C. service level agreement (SLA).
D. system architecture.

Correct Answer: B
Section:

QUESTION 396
When evaluating a number of potential controls for treating risk, it is MOST important to consider:

A. risk appetite and control efficiency.
B. inherent risk and control effectiveness.
C. residual risk and cost of control.
D. risk tolerance and control complexity.

Correct Answer: C
Section:

QUESTION 397
Which of the following is the MOST effective way to reduce potential losses due to ongoing expense fraud?

A. Implement user access controls
B. Perform regular internal audits
C. Develop and communicate fraud prevention policies
D. Conduct fraud prevention awareness training.

Correct Answer: A
Section:

QUESTION 398
An organization is participating in an industry benchmarking study that involves providing customer transaction records for analysis Which of the following is the MOST important control to ensure the privacy of customer information?

A. Nondisclosure agreements (NDAs)
B. Data anonymization
C. Data cleansing
D. Data encryption

Correct Answer: C
Section:

QUESTION 399
Which of the following is the BEST way for a risk practitioner to present an annual risk management update to the board''

A. A summary of risk response plans with validation results
B. A report with control environment assessment results
C. A dashboard summarizing key risk indicators (KRIs)
D. A summary of IT risk scenarios with business cases

Correct Answer: C
Section:

QUESTION 400
Which of the following is MOST important to promoting a risk-aware culture?

A. Regular testing of risk controls
B. Communication of audit findings
C. Procedures for security monitoring
D. Open communication of risk reporting

Correct Answer: D
Section:

QUESTION 401
The BEST metric to demonstrate that servers are configured securely is the total number of servers:

A. exceeding availability thresholds
B. experiencing hardware failures
C. exceeding current patching standards.
D. meeting the baseline for hardening.

Correct Answer: D
Section:

QUESTION 402
A risk practitioner has collaborated with subject matter experts from the IT department to develop a large list of potential key risk indicators (KRIs) for all IT operations within the organization of the following, who should review the completed list and select the appropriate KRIs for implementation?

A. IT security managers
B. IT control owners
C. IT auditors
D. IT risk owners

Correct Answer: D
Section:

QUESTION 403
If preventive controls cannot be Implemented due to technology limitations, which of the following should be done FIRST to reduce risk7

A. Evaluate alternative controls.
B. Redefine the business process to reduce the risk.
C. Develop a plan to upgrade technology.
D. Define a process for monitoring risk.

Correct Answer: A
Section:

QUESTION 404
Which of the following resources is MOST helpful to a risk practitioner when updating the likelihood rating in the risk register?

A. Risk control assessment
B. Audit reports with risk ratings
C. Penetration test results
D. Business impact analysis (BIA)

Correct Answer: D
Section:

QUESTION 405
A segregation of duties control was found to be ineffective because it did not account for all applicable functions when evaluating access. Who is responsible for ensuring the control is designed to effectively address risk?

A. Risk manager
B. Control owner
C. Control tester
D. Risk owner

Correct Answer: B
Section:

QUESTION 406
Which of the following would be the BEST way for a risk practitioner to validate the effectiveness of a patching program?

A. Conduct penetration testing.
B. Interview IT operations personnel.
C. Conduct vulnerability scans.
D. Review change control board documentation.

Correct Answer: C
Section:

QUESTION 407
The BEST indicator of the risk appetite of an organization is the

A. regulatory environment of the organization
B. risk management capability of the organization
C. board of directors' response to identified risk factors
D. importance assigned to IT in meeting strategic goals

Correct Answer: B
Section:

QUESTION 408
Which of the following is the BEST method to mitigate the risk of an unauthorized employee viewing confidential data in a database''

A. Implement role-based access control
B. Implement a data masking process
C. Include sanctions in nondisclosure agreements (NDAs)
D. Install a data loss prevention (DLP) tool

Correct Answer: A
Section:

QUESTION 409
Which of the following is the BEST approach for an organization in a heavily regulated industry to comprehensively test application functionality?

A. Use production data in a non-production environment
B. Use masked data in a non-production environment

C. Use test data in a production environment
D. Use anonymized data in a non-production environment

Correct Answer: D
Section:

QUESTION 410
An organization has agreed to a 99% availability for its online services and will not accept availability that falls below 98.5%. This is an example of:

A. risk mitigation.
B. risk evaluation.
C. risk appetite.
D. risk tolerance.

Correct Answer: C
Section:

QUESTION 411
Which of the following is the PRIMARY purpose of creating and documenting control procedures?

A. To facilitate ongoing audit and control testing
B. To help manage risk to acceptable tolerance levels
C. To establish and maintain a control inventory
D. To increase the likelihood of effective control operation

Correct Answer: D
Section:

QUESTION 412
Of the following, who is responsible for approval when a change in an application system is ready for release to production?

A. Information security officer
B. IT risk manager
C. Business owner
D. Chief risk officer (CRO)

Correct Answer: C
Section:

QUESTION 413
During a risk assessment, a key external technology supplier refuses to provide control design and effectiveness information, citing confidentiality concerns. What should the risk practitioner do NEXT?

A. Escalate the non-cooperation to management
B. Exclude applicable controls from the assessment.
C. Review the supplier's contractual obligations.
D. Request risk acceptance from the business process owner.

Correct Answer: C
Section:

QUESTION 414
Which of the following findings of a security awareness program assessment would cause the GREATEST concern to a risk practitioner?

A. The program has not decreased threat counts.
B. The program has not considered business impact.
C. The program has been significantly revised
D. The program uses non-customized training modules.

Correct Answer: D
Section:

QUESTION 415
Which of the following is the MOST important concern when assigning multiple risk owners for an identified risk?

A. Accountability may not be clearly defined.
B. Risk ratings may be inconsistently applied.
C. Different risk taxonomies may be used.
D. Mitigation efforts may be duplicated.

Correct Answer: A
Section:

QUESTION 416
When preparing a risk status report for periodic review by senior management, it is MOST important to ensure the report includes

A. risk exposure in business terms
B. a detailed view of individual risk exposures
C. a summary of incidents that have impacted the organization.
D. recommendations by an independent risk assessor.

Correct Answer: A
Section:

QUESTION 417
Which of the following is the MAIN benefit to an organization using key risk indicators (KRIs)?

A. KRIs assist in the preparation of the organization's risk profile.
B. KRIs signal that a change in the control environment has occurred.
C. KRIs provide a basis to set the risk appetite for an organization
D. KRIs provide an early warning that a risk threshold is about to be reached.

Correct Answer: D
Section:

QUESTION 418
Which of the following is the PRIMARY reason for sharing risk assessment reports with senior stakeholders?

A. To support decision-making for risk response
B. To hold risk owners accountable for risk action plans
C. To secure resourcing for risk treatment efforts
D. To enable senior management to compile a risk profile

Correct Answer: A
Section:

QUESTION 419
Which of the following BEST enables effective IT control implementation?

A. Key risk indicators (KRIs)
B. Documented procedures
C. Information security policies
D. Information security standards

Correct Answer: B
Section:

QUESTION 420
Which of the following should be the FIRST consideration when establishing a new risk governance program?

A. Developing an ongoing awareness and training program
B. Creating policies and standards that are easy to comprehend
C. Embedding risk management into the organization
D. Completing annual risk assessments on critical resources

Correct Answer: B
Section:

QUESTION 421
When establishing an enterprise IT risk management program, it is MOST important to:

A. review alignment with the organizations strategy.
B. understand the organization's information security policy.
C. validate the organization's data classification scheme.
D. report identified IT risk scenarios to senior management.

Correct Answer: D
Section:

QUESTION 422
An organization has operations in a location that regularly experiences severe weather events. Which of the following would BEST help to mitigate the risk to operations?

A. Prepare a cost-benefit analysis to evaluate relocation.
B. Prepare a disaster recovery plan (DRP).
C. Conduct a business impact analysis (BIA) for an alternate location.
D. Develop a business continuity plan (BCP).

Correct Answer: D
Section:

QUESTION 423
Which of the following is the MAIN benefit to an organization using key risk indicators (KRIs)?

A. KRIs provide an early warning that a risk threshold is about to be reached.
B. KRIs signal that a change in the control environment has occurred.
C. KRIs provide a basis to set the risk appetite for an organization.
D. KRIs assist in the preparation of the organization's risk profile.

Correct Answer: A
Section:

QUESTION 424
What is the BEST recommendation to reduce the risk associated with potential system compromise when a vendor stops releasing security patches and updates for a business-critical legacy system?

A. Segment the system on its own network.
B. Ensure regular backups take place.
C. Virtualize the system in the cloud.
D. Install antivirus software on the system.

Correct Answer: A
Section:

QUESTION 425
Which of the following would provide the MOST helpful input to develop risk scenarios associated with hosting an organization's key IT applications in a cloud environment?

A. Reviewing the results of independent audits
B. Performing a site visit to the cloud provider's data center
C. Performing a due diligence review
D. Conducting a risk workshop with key stakeholders

Correct Answer: D
Section:

QUESTION 426
A newly incorporated enterprise needs to secure its information assets From a governance perspective which of the following should be done FIRST?

A. Define information retention requirements and policies
B. Provide information security awareness training
C. Establish security management processes and procedures

D. Establish an inventory of information assets

Correct Answer: D
Section:

QUESTION 427
A highly regulated enterprise is developing a new risk management plan to specifically address legal and regulatory risk scenarios What should be done FIRST by IT governance to support this effort?

A. Request a regulatory risk reporting methodology
B. Require critical success factors (CSFs) for IT risks.
C. Establish IT-specific compliance objectives
D. Communicate IT key risk indicators (KRIs) and triggers

Correct Answer: A
Section:

QUESTION 428
Business management is seeking assurance from the CIO that IT has a plan in place for early identification of potential issues that could impact the delivery of a new application Which of the following is the BEST way to increase the chances of a successful delivery'?

A. Implement a release and deployment plan
B. Conduct comprehensive regression testing.
C. Develop enterprise-wide key risk indicators (KRIs)
D. Include business management on a weekly risk and issues report

Correct Answer: D
Section:

QUESTION 429
A root because analysis indicates a major service disruption due to a lack of competency of newly hired IT system administrators Who should be accountable for resolving the situation?

A. HR training director
B. Business process owner
C. HR recruitment manager
D. Chief information officer (CIO)

Correct Answer: C
Section:

QUESTION 430
Which of the following is the BEST way to determine whether system settings are in alignment with control baselines?

A. Configuration validation
B. Control attestation
C. Penetration testing
D. Internal audit review

Correct Answer: A
Section:

QUESTION 431
A recent big data project has resulted in the creation of an application used to support important investment decisions. Which of the following should be of GREATEST concern to the risk practitioner?

A. Data quality
B. Maintenance costs
C. Data redundancy
D. System integration

Correct Answer: A
Section:

QUESTION 432
Which of the following presents the GREATEST challenge to managing an organization's end-user devices?

A. Incomplete end-user device inventory
B. Unsupported end-user applications
C. Incompatible end-user devices
D. Multiple end-user device models

Correct Answer: A
Section:

QUESTION 433
Which of the following is the result of a realized risk scenario?

A. Technical event
B. Threat event
C. Vulnerability event
D. Loss event

Correct Answer: D
Section:

QUESTION 434
Which of the following is the MOST important outcome of a business impact analysis (BIA)?

A. Understanding and prioritization of critical processes
B. Completion of the business continuity plan (BCP)
C. Identification of regulatory consequences
D. Reduction of security and business continuity threats

Correct Answer: A
Section:

QUESTION 435
Senior management is deciding whether to share confidential data with the organization's business partners. The BEST course of action for a risk practitioner would be to submit a report to senior management containing the:

A. possible risk and suggested mitigation plans.
B. design of controls to encrypt the data to be shared.
C. project plan for classification of the data.
D. summary of data protection and privacy legislation.

Correct Answer: A
Section:

QUESTION 436
Which of the following is MOST important for successful incident response?

A. The quantity of data logged by the attack control tools
B. Blocking the attack route immediately
C. The ability to trace the source of the attack
D. The timeliness of attack recognition

Correct Answer: D
Section:

QUESTION 437
Which of The following BEST represents the desired risk posture for an organization?

A. Inherent risk is lower than risk tolerance.
B. Operational risk is higher than risk tolerance.
C. Accepted risk is higher than risk tolerance.
D. Residual risk is lower than risk tolerance.

Correct Answer: D
Section:

QUESTION 438
An organization is adopting blockchain for a new financial system. Which of the following should be the GREATEST concern for a risk practitioner evaluating the system's production readiness?

A. Limited organizational knowledge of the underlying technology
B. Lack of commercial software support
C. Varying costs related to implementation and maintenance
D. Slow adoption of the technology across the financial industry

Correct Answer: A
Section:

QUESTION 439
Which of the following should be the PRIMARY basis for prioritizing risk responses?

A. The impact of the risk
B. The replacement cost of the business asset
C. The cost of risk mitigation controls
D. The classification of the business asset

Correct Answer: A
Section:

QUESTION 440
Risk appetite should be PRIMARILY driven by which of the following?

A. Enterprise security architecture roadmap
B. Stakeholder requirements
C. Legal and regulatory requirements
D. Business impact analysis (BIA)

Correct Answer: B
Section:

QUESTION 441
What is the MAIN benefit of using a top-down approach to develop risk scenarios?

A. It describes risk events specific to technology used by the enterprise.
B. It establishes the relationship between risk events and organizational objectives.
C. It uses hypothetical and generic risk events specific to the enterprise.
D. It helps management and the risk practitioner to refine risk scenarios.

Correct Answer: C
Section:

QUESTION 442
A zero-day vulnerability has been discovered in a globally used brand of hardware server that allows hackers to gain access to affected IT systems. Which of the following is MOST likely to change as a result of this situation?

A. Control effectiveness
B. Risk appetite
C. Risk likelihood
D. Key risk indicator (KRI)

Correct Answer: C
Section:

QUESTION 443
When developing a response plan to address security incidents regarding sensitive data loss, it is MOST important

A. revalidate current key risk indicators (KRIs).
B. revise risk management procedures.
C. review the data classification policy.

D. revalidate existing risk scenarios.

Correct Answer: C
Section:

QUESTION 444
Which of the following potential scenarios associated with the implementation of a new database technology presents the GREATEST risk to an organization?

A. The organization may not have a sufficient number of skilled resources.
B. Application and data migration cost for backups may exceed budget.
C. Data may not be recoverable due to system failures.
D. The database system may not be scalable in the future.

Correct Answer: B
Section:

QUESTION 445
After entering a large number of low-risk scenarios into the risk register, it is MOST important for the risk practitioner to:

A. prepare a follow-up risk assessment.
B. recommend acceptance of the risk scenarios.
C. reconfirm risk tolerance levels.
D. analyze changes to aggregate risk.

Correct Answer: D
Section:

QUESTION 446
Which of the following provides the MOST reliable evidence of a control's effectiveness?

A. A risk and control self-assessment
B. Senior management's attestation
C. A system-generated testing report
D. detailed process walk-through

Correct Answer: D
Section:

QUESTION 447
Which of the following BEST reduces the risk associated with the theft of a laptop containing sensitive information?

A. Cable lock
B. Data encryption
C. Periodic backup
D. Biometrics access control

Correct Answer: B

Section:

QUESTION 448
An organization has asked an IT risk practitioner to conduct an operational risk assessment on an initiative to outsource the organization's customer service operations overseas. Which of the following would MOST significantly impact management's decision?

A. Time zone difference of the outsourcing location
B. Ongoing financial viability of the outsourcing company
C. Cross-border information transfer restrictions in the outsourcing country
D. Historical network latency between the organization and outsourcing location

Correct Answer: C
Section:

QUESTION 449
Which of the following is the MOST effective way for a large and diversified organization to minimize risk associated with unauthorized software on company devices?

A. Scan end points for applications not included in the asset inventory.
B. Prohibit the use of cloud-based virtual desktop software.
C. Conduct frequent reviews of software licenses.
D. Perform frequent internal audits of enterprise IT infrastructure.

Correct Answer: A
Section:

QUESTION 450
Which of the following BEST facilitates the identification of appropriate key performance indicators (KPIs) for a risk management program?

A. Reviewing control objectives
B. Aligning with industry best practices
C. Consulting risk owners
D. Evaluating KPIs in accordance with risk appetite

Correct Answer: C
Section:

QUESTION 451
Which of the following is a risk practitioner's BEST recommendation upon learning that an employee inadvertently disclosed sensitive data to a vendor?

A. Enroll the employee in additional security training.
B. Invoke the incident response plan.
C. Conduct an internal audit.
D. Instruct the vendor to delete the data.

Correct Answer: B
Section:

QUESTION 452
Which of the following is the BEST method to maintain a common view of IT risk within an organization?

A. Collecting data for IT risk assessment
B. Establishing and communicating the IT risk profile
C. Utilizing a balanced scorecard
D. Performing and publishing an IT risk analysis

Correct Answer: C
Section:

QUESTION 453
Which of the following is the MOST important information to cover a business continuity awareness Ira nine, program for all employees of the organization?

A. Recovery time objectives (RTOs)
B. Segregation of duties
C. Communication plan
D. Critical asset inventory

Correct Answer: C
Section:

QUESTION 454
Which of the following is the BEST approach for selecting controls to minimize risk?

A. Industry best practice review
B. Risk assessment
C. Cost-benefit analysis
D. Control-effectiveness evaluation

Correct Answer: C
Section:

QUESTION 455
The MAIN reason for prioritizing IT risk responses is to enable an organization to:

A. determine the risk appetite.
B. determine the budget.
C. define key performance indicators (KPIs).
D. optimize resource utilization.

Correct Answer: C
Section:

QUESTION 456
An organization has experienced a cyber attack that exposed customer personally identifiable information (PII) and caused extended outages of network services. Which of the following stakeholders are MOST important to include in the cyber response team to determine response actions?

A. Security control owners based on control failures
B. Cyber risk remediation plan owners
C. Risk owners based on risk impact
D. Enterprise risk management (ERM) team

Correct Answer: C
Section:

QUESTION 457
Which of the following is the PRIMARY reason for a risk practitioner to review an organization's IT asset inventory?

A. To plan for the replacement of assets at the end of their life cycles
B. To assess requirements for reducing duplicate assets
C. To understand vulnerabilities associated with the use of the assets
D. To calculate mean time between failures (MTBF) for the assets

Correct Answer: C
Section: