Isaca

Exam Questions CRISC

Certified in Risk and Information Systems Control

NEW QUESTION 1
- (Exam Topic 1)
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 m the risk register.
C. Inform senior management.
D. update the risk response plan.

Answer: A

NEW QUESTION 2
- (Exam Topic 1)
A risk practitioner is assisting with the preparation of a report on the organization s disaster recovery (DR) capabilities. Which information would have the MOST impact on the overall recovery profile?

A. The percentage of systems meeting recovery target times has increased.
B. The number of systems tested in the last year has increased.
C. The number of systems requiring a recovery plan has increased.
D. The percentage of systems with long recovery target times has decreased.

Answer: D

NEW QUESTION 3
- (Exam Topic 1)
After a high-profile systems breach at an organization s key vendor, the vendor has implemented additional mitigating controls. The vendor has voluntarily shared the following set of assessments:
After a high-profile systems breach at an organization s key vendor, the vendor has implemented additional mitigating controls. The vendor has voluntarily shared the following set of assessments:
Which of the assessments provides the MOST reliable input to evaluate residual risk in the vendor's control environment?

Type	Scope	Completed By
External audit	Financial systems and processes	Third party
Internal audit	IT security risk management	Vendor
Vendor performance scorecard	Service level agreement compliance	Organization
Regulatory examination	Information security management program	Regulator

A. External audit
B. Internal audit
C. Vendor performance scorecard
D. Regulatory examination

Answer: B

NEW QUESTION 4
- (Exam Topic 1)
A risk heat map is MOST commonly used as part of an IT risk analysis to facilitate risk:

A. identification.
B. treatment.
C. communication.
D. assessment

Answer: C

NEW QUESTION 5
- (Exam Topic 1)
A risk practitioner has determined that a key control does not meet design expectations. Which of the following should be done NEXT?

A. Document the finding in the risk register.
B. Invoke the incident response plan.
C. Re-evaluate key risk indicators.
D. Modify the design of the control.

Answer: A

NEW QUESTION 6
- (Exam Topic 1)
Malware has recently affected an organization, The MOST effective way to resolve this situation and define a comprehensive risk treatment plan would be to perform:

A. a gap analysis
B. a root cause analysis.

C. an impact assessment.
D. a vulnerability assessment.

Answer: C

NEW QUESTION 7
- (Exam Topic 1)
Which of the following is the BEST method to identify unnecessary controls?

A. Evaluating the impact of removing existing controls
B. Evaluating existing controls against audit requirements
C. Reviewing system functionalities associated with business processes
D. Monitoring existing key risk indicators (KRIs)

Answer: A

NEW QUESTION 8
- (Exam Topic 1)
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

Answer: C

NEW QUESTION 9
- (Exam Topic 1)
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

Answer: B

NEW QUESTION 10
- (Exam Topic 1)
The analysis of which of the following will BEST help validate whether suspicious network activity is malicious?

A. Logs and system events
B. Intrusion detection system (IDS) rules
C. Vulnerability assessment reports
D. Penetration test reports

Answer: B

NEW QUESTION 10
- (Exam Topic 1)
During an IT risk scenario review session, business executives question why they have been assigned ownership of IT-related risk scenarios. They feel IT risk is technical in nature and therefore should be owned by IT. Which of the following is the BEST way for the risk practitioner to address these concerns?

A. Describe IT risk scenarios in terms of business risk.
B. Recommend the formation of an executive risk council to oversee IT risk.
C. Provide an estimate of IT system downtime if IT risk materializes.
D. Educate business executives on IT risk concepts.

Answer: A

NEW QUESTION 14
- (Exam Topic 1)
A trusted third party service provider has determined that the risk of a client's systems being hacked is low. Which of the following would be the client's BEST course of action?

A. Perform their own risk assessment
B. Implement additional controls to address the risk.
C. Accept the risk based on the third party's risk assessment
D. Perform an independent audit of the third party.

Answer: C

NEW QUESTION 17
- (Exam Topic 1)

A web-based service provider with a low risk appetite for system outages is reviewing its current risk profile for online security. Which of the following observations would be MOST relevant to escalate to senior management?

A. An increase in attempted distributed denial of service (DDoS) attacks
B. An increase in attempted website phishing attacks
C. A decrease in achievement of service level agreements (SLAs)
D. A decrease in remediated web security vulnerabilities

Answer: A

NEW QUESTION 19
- (Exam Topic 1)
Which of the following is the MOST important consideration when multiple risk practitioners capture risk scenarios in a single risk register?

A. Aligning risk ownership and control ownership
B. Developing risk escalation and reporting procedures
C. Maintaining up-to-date risk treatment plans
D. Using a consistent method for risk assessment

Answer: D

NEW QUESTION 23
- (Exam Topic 1)
An application owner has specified the acceptable downtime in the event of an incident to be much lower than the actual time required for the response team to recover the application. Which of the following should be the NEXT course of action?

A. Invoke the disaster recovery plan during an incident.
B. Prepare a cost-benefit analysis of alternatives available
C. Implement redundant infrastructure for the application.
D. Reduce the recovery time by strengthening the response team.

Answer: C

NEW QUESTION 28
- (Exam Topic 1)
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

Answer: A

NEW QUESTION 31
- (Exam Topic 1)
Which of the following is the BEST indication of an effective risk management program?

A. Risk action plans are approved by senior management.
B. Residual risk is within the organizational risk appetite
C. Mitigating controls are designed and implemented.
D. Risk is recorded and tracked in the risk register

Answer: B

NEW QUESTION 36
- (Exam Topic 1)
Which of the following will BEST quantify the risk associated with malicious users in an organization?

A. Business impact analysis
B. Risk analysis
C. Threat risk assessment
D. Vulnerability assessment

Answer: A

NEW QUESTION 41
- (Exam Topic 1)
Which of the following controls will BEST detect unauthorized modification of data by a database administrator?

A. Reviewing database access rights
B. Reviewing database activity logs
C. Comparing data to input records
D. Reviewing changes to edit checks

Answer: B

NEW QUESTION 42
- (Exam Topic 1)
Which of the following should be the PRIMARY consideration when assessing the automation of control monitoring?

A. impact due to failure of control
B. Frequency of failure of control
C. Contingency plan for residual risk
D. Cost-benefit analysis of automation

Answer: D

NEW QUESTION 45
- (Exam Topic 1)
Which of the following is the MOST important characteristic of an effective risk management program?

A. Risk response plans are documented
B. Controls are mapped to key risk scenarios.
C. Key risk indicators are defined.
D. Risk ownership is assigned

Answer: D

NEW QUESTION 47
- (Exam Topic 1)
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.

Answer: B

NEW QUESTION 51
- (Exam Topic 1)
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.

Answer: C

NEW QUESTION 56
- (Exam Topic 1)
During testing, a risk practitioner finds the IT department's recovery time objective (RTO) for a key system does not align with the enterprise's business continuity plan (BCP). Which of the following should be done NEXT?

A. Report the gap to senior management
B. Consult with the IT department to update the RTO
C. Complete a risk exception form.
D. Consult with the business owner to update the BCP

Answer: A

NEW QUESTION 60
- (Exam Topic 1)
In an organization with a mature risk management program, which of the following would provide the BEST evidence that the IT risk profile is up to date?

A. Risk questionnaire
B. Risk register
C. Management assertion
D. Compliance manual

Answer: B

NEW QUESTION 65
- (Exam Topic 1)
Which of the following should be the PRIMARY input when designing IT controls?

A. Benchmark of industry standards
B. Internal and external risk reports
C. Recommendations from IT risk experts
D. Outcome of control self-assessments

Answer:

B

NEW QUESTION 68
- (Exam Topic 1)
The risk associated with an asset before controls are applied can be expressed as:

A. a function of the likelihood and impact
B. the magnitude of an impact
C. a function of the cost and effectiveness of control.
D. the likelihood of a given threat

Answer: C

NEW QUESTION 72
- (Exam Topic 1)
Which of the following is MOST helpful in identifying new risk exposures due to changes in the business environment?

A. Standard operating procedures
B. SWOT analysis
C. Industry benchmarking
D. Control gap analysis

Answer: B

NEW QUESTION 73
- (Exam Topic 1)
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

Answer: C

NEW QUESTION 75
- (Exam Topic 1)
Which of the following elements of a risk register is MOST likely to change as a result of change in management's risk appetite?

A. Key risk indicator (KRI) thresholds
B. Inherent risk
C. Risk likelihood and impact
D. Risk velocity

Answer: A

NEW QUESTION 80
- (Exam Topic 1)
Which of the following is the MOST important benefit of key risk indicators (KRIs)'

A. Assisting in continually optimizing risk governance
B. Enabling the documentation and analysis of trends
C. Ensuring compliance with regulatory requirements
D. Providing an early warning to take proactive actions

Answer: D

NEW QUESTION 85
- (Exam Topic 1)
Which of the following is the MOST important consideration when sharing risk management updates with executive management?

A. Using an aggregated view of organizational risk
B. Ensuring relevance to organizational goals
C. Relying on key risk indicator (KRI) data Including
D. Trend analysis of risk metrics

Answer: B

NEW QUESTION 87
- (Exam Topic 1)
An organization has allowed its cyber risk insurance to lapse while seeking a new insurance provider. The risk practitioner should report to management that the risk has been:

A. transferred
B. mitigated.
C. accepted

D. avoided

Answer: C

NEW QUESTION 90
- (Exam Topic 1)
To implement the MOST effective monitoring of key risk indicators (KRIs), which of the following needs to be in place?

A. Threshold definition
B. Escalation procedures
C. Automated data feed
D. Controls monitoring

Answer: A

NEW QUESTION 95
- (Exam Topic 1)
Which of the following would be MOST important for a risk practitioner to provide to the internal audit department during the audit planning process?

A. Closed management action plans from the previous audit
B. Annual risk assessment results
C. An updated vulnerability management report
D. A list of identified generic risk scenarios

Answer: A

NEW QUESTION 100
- (Exam Topic 1)
Which of the following is the BEST way for a risk practitioner to help management prioritize risk response?

A. Align business objectives to the risk profile.
B. Assess risk against business objectives
C. Implement an organization-specific risk taxonomy.
D. Explain risk details to management.

Answer: B

NEW QUESTION 102
- (Exam Topic 1)
Which of the following will BEST mitigate the risk associated with IT and business misalignment?

A. Establishing business key performance indicators (KPIs)
B. Introducing an established framework for IT architecture
C. Establishing key risk indicators (KRIs)
D. Involving the business process owner in IT strategy

Answer: D

NEW QUESTION 105
- (Exam Topic 1)
Which of the following would be considered a vulnerability?

A. Delayed removal of employee access
B. Authorized administrative access to HR files
C. Corruption of files due to malware
D. Server downtime due to a denial of service (DoS) attack

Answer: A

NEW QUESTION 108
- (Exam Topic 1)
A risk assessment has identified that departments have installed their own WiFi access points on the enterprise network. Which of the following would be MOST important to include in a report to senior management?

A. The network security policy
B. Potential business impact
C. The WiFi access point configuration
D. Planned remediation actions

Answer: B

NEW QUESTION 111
- (Exam Topic 1)
Which of the following would BEST ensure that identified risk scenarios are addressed?

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

Answer: A

NEW QUESTION 112
- (Exam Topic 1)
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

Answer: B

NEW QUESTION 114
- (Exam Topic 1)
Which of the following would provide the BEST guidance when selecting an appropriate risk treatment plan?

A. Risk mitigation budget
B. Business Impact analysis
C. Cost-benefit analysis
D. Return on investment

Answer: B

NEW QUESTION 118
- (Exam Topic 1)
A business unit is updating a risk register with assessment results for a key project. Which of the following is MOST important to capture in the register?

A. The team that performed the risk assessment
B. An assigned risk manager to provide oversight
C. Action plans to address risk scenarios requiring treatment
D. The methodology used to perform the risk assessment

Answer: B

NEW QUESTION 121
- (Exam Topic 1)
An audit reveals that several terminated employee accounts maintain access. Which of the following should be the FIRST step to address the risk?

A. Perform a risk assessment
B. Disable user access.
C. Develop an access control policy.
D. Perform root cause analysis.

Answer: B

NEW QUESTION 126
- (Exam Topic 1)
A risk practitioner has identified that the organization's secondary data center does not provide redundancy for a critical application. Who should have the authority to accept the associated risk?

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

Answer: C

NEW QUESTION 127
- (Exam Topic 1)
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.

Answer: C

NEW QUESTION 130

- (Exam Topic 1)
Risk management strategies are PRIMARILY adopted to:

A. take necessary precautions for claims and losses.
B. achieve acceptable residual risk levels.
C. avoid risk for business and IT assets.
D. achieve compliance with legal requirements.

Answer: B

NEW QUESTION 133
- (Exam Topic 1)
Which of the following would BEST help to ensure that suspicious network activity is identified?

A. Analyzing intrusion detection system (IDS) logs
B. Analyzing server logs
C. Using a third-party monitoring provider
D. Coordinating events with appropriate agencies

Answer: A

NEW QUESTION 136
- (Exam Topic 1)
Which of the following would BEST help minimize the risk associated with social engineering threats?

A. Enforcing employees sanctions
B. Conducting phishing exercises
C. Enforcing segregation of dunes
D. Reviewing the organization's risk appetite

Answer: B

NEW QUESTION 141
- (Exam Topic 1)
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

Answer: B

NEW QUESTION 142
- (Exam Topic 1)
Which of the following techniques would be used during a risk assessment to demonstrate to stakeholders that all known alternatives were evaluated?

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

Answer: D

NEW QUESTION 144
- (Exam Topic 1)
During the risk assessment of an organization that processes credit cards, a number of existing controls have been found to be ineffective and do not meet industry standards. The overall control environment may still be effective if:

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

Answer: A

NEW QUESTION 148
- (Exam Topic 1)
Which of the following should be the PRIMARY consideration when implementing controls for monitoring user activity logs?

A. Ensuring availability of resources for log analysis
B. Implementing log analysis tools to automate controls
C. Ensuring the control is proportional to the risk
D. Building correlations between logs collected from different sources

Answer: C

NEW QUESTION 152
- (Exam Topic 1)
A rule-based data loss prevention {DLP) tool has recently been implemented to reduce the risk of sensitive data leakage Which of the following is MOST likely to change as a result of this implementation?

A. Risk likelihood
B. Risk velocity
C. Risk appetite
D. Risk impact

Answer: A

NEW QUESTION 157
- (Exam Topic 1)
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

Answer: A

NEW QUESTION 159
- (Exam Topic 1)
Which of the following is the MOST important factor affecting risk management in an organization?

A. The risk manager's expertise
B. Regulatory requirements
C. Board of directors' expertise
D. The organization's culture

Answer: B

NEW QUESTION 160
- (Exam Topic 1)
A risk practitioner observes that hardware failure incidents have been increasing over the last few months. However, due to built-in redundancy and fault-tolerant architecture, there have been no interruptions to business operations. The risk practitioner should conclude that:

A. a root cause analysis is required
B. controls are effective for ensuring continuity
C. hardware needs to be upgraded
D. no action is required as there was no impact

Answer: A

NEW QUESTION 164
- (Exam Topic 1)
Who is the MOST appropriate owner for newly identified IT risk?

A. The manager responsible for IT operations that will support the risk mitigation efforts
B. The individual with authority to commit organizational resources to mitigate the risk
C. A project manager capable of prioritizing the risk remediation efforts
D. The individual with the most IT risk-related subject matter knowledge

Answer: B

NEW QUESTION 166
- (Exam Topic 1)
Which of the following is the PRIMARY reason for a risk practitioner to use global standards related to risk management?

A. To build an organizational risk-aware culture
B. To continuously improve risk management processes
C. To comply with legal and regulatory requirements
D. To identify gaps in risk management practices

Answer: C

Explanation:
1. - (Exam Topic 2)
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
2. - (Exam Topic 2)
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
3. - (Exam Topic 2)
The risk associated with a high-risk vulnerability in an application is owned by the:
A. security department.
B. business unit
C. vendor.
D. IT department.
4. - (Exam Topic 2)
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 (Pll)?
A. A privacy impact assessment has not been completed.
B. Data encryption methods apply to a subset of Pll obtained.
C. The data privacy officer was not consulted.
D. Insufficient access controls are used on the loT devices.
5. - (Exam Topic 2)
Which of the following is the MOST effective control to ensure user access is maintained on a least-privilege basis?
A. User authorization
B. User recertification
C. Change log review
D. Access log monitoring
6. - (Exam Topic 2)
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
7. - (Exam Topic 2)
Risk aggregation in a complex organization will be MOST successful when:
A. using the same scales in assessing risk
B. utilizing industry benchmarks
C. using reliable qualitative data for risk Hems
D. including primarily low level risk factors
8. - (Exam Topic 2)
Which of the following is the BEST key performance indicator (KPI) to measure the effectiveness of a vulnerability management process?
A. Percentage of vulnerabilities remediated within the agreed service level
B. Number of vulnerabilities identified during the period
C. Number of vulnerabilities re-opened during the period
D. Percentage of vulnerabilities escalated to senior management
9. - (Exam Topic 2)
Which of the following approaches BEST identifies information systems control deficiencies?
A. Countermeasures analysis
B. Best practice assessment
C. Gap analysis
D. Risk assessment
10. - (Exam Topic 2)
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
11. - (Exam Topic 2)
It is MOST important for a risk practitioner to have an awareness of an organization s processes in order to:
A. perform a business impact analysis.
B. identify potential sources of risk.
C. establish risk guidelines.
D. understand control design.
12. - (Exam Topic 2)
Which of the following is the PRIMARY reason for an organization to ensure the risk register is updated regularly?
A. Risk assessment results are accessible to senior management and stakeholders.
B. Risk mitigation activities are managed and coordinated.
C. Key risk indicators (KRIs) are evaluated to validate they are still within the risk threshold.
D. Risk information is available to enable risk-based decisions.
13. - (Exam Topic 2)
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.
14. - (Exam Topic 2)
Which of the following risk register elements is MOST likely to be updated if the attack surface or exposure of an asset is reduced?
A. Likelihood rating
B. Control effectiveness
C. Assessment approach
D. Impact rating
15. - (Exam Topic 2)
Which of the following is the BEST way to determine software license compliance?
A. List non-compliant systems in the risk register.
B. Conduct periodic compliance reviews.
C. Review whistlebtower reports of noncompliance.

D. Monitor user software download activity.
16. - (Exam Topic 2)
An organization is considering modifying its system to enable acceptance of credit card payments. To reduce the risk of data exposure, which of the following should the organization do FIRST?
A. Conduct a risk assessment.
B. Update the security strategy.
C. Implement additional controls.
D. Update the risk register.
17. - (Exam Topic 2)
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.
18. - (Exam Topic 2)
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
19. - (Exam Topic 2)
Which of the following would be the BEST justification to invest in the development of a governance, risk, and compliance (GRC) solution?
A. Facilitating risk-aware decision making by stakeholders
B. Demonstrating management commitment to mitigate risk
C. Closing audit findings on a timely basis
D. Ensuring compliance to industry standards
20. - (Exam Topic 2)
An organization has granted a vendor access to its data in order to analyze customer behavior. Which of the following would be the MOST effective control to mitigate the risk of customer data leakage?
A. Enforce criminal background checks.
B. Mask customer data fields.
C. Require vendor to sign a confidentiality agreement.
D. Restrict access to customer data on a "need to know" basis.
21. - (Exam Topic 2)
When an organization's disaster recovery plan has a reciprocal agreement, which of the following risk treatment options is being applied?
A. Acceptance
B. Mitigation
C. Transfer
D. Avoidance
22. - (Exam Topic 2)
Which of the following observations would be GREATEST concern to a risk practitioner reviewing the implementation status of management action plans?
A. Management has not determined a final implementation date.
B. Management has not completed an early mitigation milestone.
C. Management has not secured resources for mitigation activities.
D. Management has not begun the implementation.
23. - (Exam Topic 2)
The PRIMARY basis for selecting a security control is:
A. to achieve the desired level of maturity.
B. the materiality of the risk.
C. the ability to mitigate risk.
D. the cost of the control.
24. - (Exam Topic 2)
Which of the following is the BEST measure of the effectiveness of an employee deprovisioning process?
A. Number of days taken to remove access after staff separation dates
B. Number of days taken for IT to remove access after receipt of HR instructions
C. Number of termination requests processed per reporting period
D. Number of days taken for HR to provide instructions to IT after staff separation dates
25. - (Exam Topic 2)
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
26. - (Exam Topic 2)
Which of the following is the BEST indicator of the effectiveness of a control monitoring program?
A. Time between control failure and failure detection
B. Number of key controls as a percentage of total control count
C. Time spent on internal control assessment reviews
D. Number of internal control failures within the measurement period
27. - (Exam Topic 2)
An organization is considering allowing users to access company data from their personal devices. Which of the following is the MOST important factor when assessing the risk?
A. Classification of the data
B. Type of device
C. Remote management capabilities
D. Volume of data
28. - (Exam Topic 2)
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)

29. - (Exam Topic 2)
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
30. - (Exam Topic 2)
An organization has engaged a third party to provide an Internet gateway encryption service that protects sensitive data uploaded to a cloud service. This is an example of risk:
A. mitigation.
B. avoidance.
C. transfer.
D. acceptance.
31. - (Exam Topic 2)
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
32. - (Exam Topic 2)
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.
33. - (Exam Topic 2)
Which of the following should be initiated when a high number of noncompliant conditions are observed during review of a control procedure?
A. Disciplinary action
B. A control self-assessment
C. A review of the awareness program
D. Root cause analysis
34. - (Exam Topic 2)
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
35. - (Exam Topic 2)
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.
36. - (Exam Topic 2)
When establishing leading indicators for the information security incident response process it is MOST important to consider the percentage of reported incidents:
A. that result in a full root cause analysis.
B. used for verification within the SLA.
C. that are verified as actual incidents.
D. resolved within the SLA.
37. - (Exam Topic 2)
Which of the following is MOST important for a risk practitioner to update when a software upgrade renders an existing key control ineffective?
A. Audit engagement letter
B. Risk profile
C. IT risk register
D. Change control documentation
38. - (Exam Topic 2)
The PRIMARY goal of a risk management program is to:
A. facilitate resource availability.
B. help ensure objectives are met.
C. safeguard corporate assets.
D. help prevent operational losses.
39. - (Exam Topic 2)
A company has located its computer center on a moderate earthquake fault. Which of the following is the MOST important consideration when establishing a contingency plan and an alternate processing site?
A. The alternative site is a hot site with equipment ready to resume processing immediately.
B. The contingency plan provides for backup media to be taken to the alternative site.
C. The contingency plan for high priority applications does not involve a shared cold site.
D. The alternative site does not reside on the same fault to matter how the distance apart.
40. - (Exam Topic 2)
Which of the following key risk indicators (KRIs) is MOST effective for monitoring risk related to a bring your own device (BYOD) program?
A. Number of users who have signed a BYOD acceptable use policy
B. Number of incidents originating from BYOD devices
C. Budget allocated to the BYOD program security controls
D. Number of devices enrolled in the BYOD program
41. - (Exam Topic 2)
Which of the following BEST indicates that an organization has implemented IT performance requirements?
A. Service level agreements
B. Vendor references
C. Benchmarking data
D. Accountability matrix
42. - (Exam Topic 2)
Which of the following is the PRIMARY reason for monitoring activities performed in a production database environment?
A. Ensuring that database changes are correctly applied

B. Enforcing that changes are authorized
C. Deterring illicit actions of database administrators
D. Preventing system developers from accessing production data
43. - (Exam Topic 2)
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
44. - (Exam Topic 2)
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.
45. - (Exam Topic 2)
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.
46. - (Exam Topic 2)
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
47. - (Exam Topic 2)
Which of the following approaches would BEST help to identify relevant risk scenarios?
A. Engage line management in risk assessment workshops.
B. Escalate the situation to risk leadership.
C. Engage internal audit for risk assessment workshops.
D. Review system and process documentation.
48. - (Exam Topic 2)
Which of the following is the MOST important consideration when selecting either a qualitative or quantitative risk analysis?
A. Expertise in both methodologies
B. Maturity of the risk management program
C. Time available for risk analysis
D. Resources available for data analysis
49. - (Exam Topic 2)
Which of the following BEST contributes to the implementation of an effective risk response action plan?
A. An IT tactical plan
B. Disaster recovery and continuity testing
C. Assigned roles and responsibilities
D. A business impact analysis
50. - (Exam Topic 2)
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
51. - (Exam Topic 2)
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
52. - (Exam Topic 2)
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
53. - (Exam Topic 2)
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
54. - (Exam Topic 2)
Which of the following is the GREATEST benefit to an organization when updates to the risk register are made promptly after the completion of a risk assessment?
A. Improved senior management communication
B. Optimized risk treatment decisions
C. Enhanced awareness of risk management
D. Improved collaboration among risk professionals
55. - (Exam Topic 2)
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.
56. - (Exam Topic 2)
Which of the following is the GREATEST concern when an organization uses a managed security service provider as a firewall administrator?
A. Exposure of log data
B. Lack of governance
C. Increased number of firewall rules
D. Lack of agreed-upon standards
57. - (Exam Topic 2)
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.
58. - (Exam Topic 2)
Which of the following methods would BEST contribute to identifying obscure risk scenarios?
A. Brainstorming sessions
B. Control self-assessments
C. Vulnerability analysis
D. Monte Carlo analysis
59. - (Exam Topic 2)
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.
60. - (Exam Topic 2)
An organization is planning to acquire a new financial system. Which of the following stakeholders would provide the MOST relevant information for analyzing the risk associated with the new IT solution?
A. Project sponsor
B. Process owner
C. Risk manager
D. Internal auditor
61. - (Exam Topic 2)
Which of The following will BEST communicate the importance of risk mitigation initiatives to senior management?
A. Business case
B. Balanced scorecard
C. Industry standards
D. Heat map
62. - (Exam Topic 2)
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
63. - (Exam Topic 2)
Which of the following is MOST important to enable well-informed cybersecurity risk decisions?
A. Determine and understand the risk rating of scenarios.
B. Conduct risk assessment peer reviews.
C. Identify roles and responsibilities for security controls.
D. Engage a third party to perform a risk assessment.
64. - (Exam Topic 2)
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
65. - (Exam Topic 2)
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.
66. - (Exam Topic 2)
The PRIMARY reason for periodic penetration testing of Internet-facing applications is to:
A. ensure policy and regulatory compliance.
B. assess the proliferation of new threats.
C. verify Internet firewall control settings.
D. identify vulnerabilities in the system.
67. - (Exam Topic 2)
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.
68. - (Exam Topic 2)
An organization has outsourced its backup and recovery procedures to a third-party cloud provider. Which of the following is the risk practitioner s BEST course of action?
A. Accept the risk and document contingency plans for data disruption.
B. Remove the associated risk scenario from the risk register due to avoidance.
C. Mitigate the risk with compensating controls enforced by the third-party cloud provider.
D. Validate the transfer of risk and update the register to reflect the change.
69. - (Exam Topic 2)

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.
70. - (Exam Topic 2)
The MAIN purpose of having a documented risk profile is to:
A. comply with external and internal requirements.
B. enable well-informed decision making.
C. prioritize investment projects.
D. keep the risk register up-to-date.
71. - (Exam Topic 2)
Which of the following will provide the BEST measure of compliance with IT policies?
A. Evaluate past policy review reports.
B. Conduct regular independent reviews.
C. Perform penetration testing.
D. Test staff on their compliance responsibilities.
72. - (Exam Topic 2)
Which of the following should be a risk practitioner s MOST important consideration when developing IT risk scenarios?
A. The impact of controls on the efficiency of the business in delivering services
B. Linkage of identified risk scenarios with enterprise risk management
C. Potential threats and vulnerabilities that may have an impact on the business
D. Results of network vulnerability scanning and penetration testing
73. - (Exam Topic 2)
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.
74. - (Exam Topic 2)
The risk associated with data loss from a website which contains sensitive customer information is BEST owned by:
A. the third-party website manager
B. the business process owner
C. IT security
D. the compliance manager
75. - (Exam Topic 2)
When presenting risk, the BEST method to ensure that the risk is measurable against the organization's risk appetite is through the use of a:
A. risk map
B. cause-and-effect diagram
C. maturity model
D. technology strategy plan.
76. - (Exam Topic 2)
Which of the following is the MAIN reason for analyzing risk scenarios?
A. Identifying additional risk scenarios
B. Updating the heat map
C. Assessing loss expectancy
D. Establishing a risk appetite
77. - (Exam Topic 2)
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
78. - (Exam Topic 2)
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.
79. - (Exam Topic 2)
The MAIN goal of the risk analysis process is to determine the:
A. potential severity of impact
B. frequency and magnitude of loss
C. control deficiencies
D. threats and vulnerabilities
80. - (Exam Topic 2)
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
81. - (Exam Topic 2)
Which of the following would be of GREATEST assistance when justifying investment in risk response strategies?
A. Total cost of ownership
B. Resource dependency analysis
C. Cost-benefit analysis
D. Business impact analysis
82. - (Exam Topic 2)
Which of the following is the MOST effective way to help ensure an organization's current risk scenarios are relevant?
A. Adoption of industry best practices
B. Involvement of stakeholders in risk assessment
C. Review of risk scenarios by independent parties

D. Documentation of potential risk in business cases
83. - (Exam Topic 2)
After mapping generic risk scenarios to organizational security policies, the NEXT course of action should be to:
A. record risk scenarios in the risk register for analysis.
B. validate the risk scenarios for business applicability.
C. reduce the number of risk scenarios to a manageable set.
D. perform a risk analysis on the risk scenarios.
84. - (Exam Topic 2)
Accountability for a particular risk is BEST represented in a:
A. risk register.
B. risk catalog
C. risk scenario
D. RACI matrix.
85. - (Exam Topic 2)
The PRIMARY purpose of a maturity model is to compare the:
A. current state of key processes to their desired state.
B. actual KPIs with target KPIs.
C. organization to industry best practices.
D. organization to peers.
86. - (Exam Topic 2)
The BEST way to test the operational effectiveness of a data backup procedure is to:
A. conduct an audit of files stored offsite.
B. interview employees to compare actual with expected procedures.
C. inspect a selection of audit trails and backup logs.
D. demonstrate a successful recovery from backup files.
87. - (Exam Topic 2)
An organization is measuring the effectiveness of its change management program to reduce the number of unplanned production changes. Which of the following would be the BEST metric to determine if the program is performing as expected?
A. Decrease in the time to move changes to production
B. Ratio of emergency fixes to total changes
C. Ratio of system changes to total changes
D. Decrease in number of changes without a fallback plan
88. - (Exam Topic 2)
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
89. - (Exam Topic 2)
Which of the following should management consider when selecting a risk mitigation option?
A. Maturity of the enterprise architecture
B. Cost of control implementation
C. Reliability of key performance indicators (KPIs)
D. Reliability of key risk indicators (KPIs)
90. - (Exam Topic 2)
Which of the following indicates an organization follows IT risk management best practice?
A. The risk register template uses an industry standard.
B. The risk register is regularly updated.
C. All fields in the risk register have been completed.
D. Controls are listed against risk entries in the register.
91. - (Exam Topic 2)
An organization's risk tolerance should be defined and approved by which of the following?
A. The chief risk officer (CRO)
B. The board of directors
C. The chief executive officer (CEO)
D. The chief information officer (CIO)
92. - (Exam Topic 2)
Which of The following is the BEST way to confirm whether appropriate automated controls are in place within a recently implemented system?
A. Perform a post-implementation review.
B. Conduct user acceptance testing.
C. Review the key performance indicators (KPIs).
D. Interview process owners.
93. - (Exam Topic 2)
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
94. - (Exam Topic 2)
The PRIMARY benefit of conducting continuous monitoring of access controls is the ability to identify:
A. inconsistencies between security policies and procedures
B. possible noncompliant activities that lead to data disclosure
C. leading or lagging key risk indicators (KRIs)
D. unknown threats to undermine existing access controls
95. - (Exam Topic 2)
Which of the following should be the MAIN consideration when validating an organization's risk appetite?
A. Comparison against regulations
B. Maturity of the risk culture
C. Capacity to withstand loss
D. Cost of risk mitigation options
96. - (Exam Topic 2)
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.
97. - (Exam Topic 2)
Which of the following is MOST helpful in identifying gaps between the current and desired state of the IT risk environment?
A. Analyzing risk appetite and tolerance levels
B. Assessing identified risk and recording results in the risk register
C. Evaluating risk scenarios and assessing current controls
D. Reviewing guidance from industry best practices and standards
98. - (Exam Topic 2)
When communicating changes in the IT risk profile, which of the following should be included to BEST enable stakeholder decision making?
A. List of recent incidents affecting industry peers
B. Results of external attacks and related compensating controls
C. Gaps between current and desired states of the control environment
D. Review of leading IT risk management practices within the industry
99. - (Exam Topic 2)
The purpose of requiring source code escrow in a contractual agreement is to:
A. ensure that the source code is valid and exists.
B. ensure that the source code is available if the vendor ceases to exist.
C. review the source code for adequacy of controls.
D. ensure the source code is available when bugs occur.
100. - (Exam Topic 2)
Which of the following is the MOST important consideration when performing a risk assessment of a fire suppression system within a data center?
A. Insurance coverage
B. Onsite replacement availability
C. Maintenance procedures
D. Installation manuals
101. - (Exam Topic 2)
Which of the following could BEST detect an in-house developer inserting malicious functions into a web-based application?
A. Segregation of duties
B. Code review
C. Change management
D. Audit modules
102. - (Exam Topic 2)
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.
103. - (Exam Topic 2)
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
104. - (Exam Topic 2)
Which of the following is the PRIMARY role of a data custodian in the risk management process?
A. Performing periodic data reviews according to policy
B. Reporting and escalating data breaches to senior management
C. Being accountable for control design
D. Ensuring data is protected according to the classification
105. - (Exam Topic 2)
The annualized loss expectancy (ALE) method of risk analysis:
A. helps in calculating the expected cost of controls
B. uses qualitative risk rankings such as low. medium and high.
C. can be used m a cost-benefit analysts
D. can be used to determine the indirect business impact.
106. - (Exam Topic 2)
An organization has outsourced its lease payment process to a service provider who lacks evidence of compliance with a necessary regulatory standard. Which risk treatment was adopted by the organization?
A. Acceptance
B. Transfer
C. Mitigation
D. Avoidance
107. - (Exam Topic 2)
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.
108. - (Exam Topic 2)
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.
109. - (Exam Topic 2)
The risk associated with inadvertent disclosure of database records from a public cloud service provider (CSP) would MOST effectively be reduced by:
A. encrypting the data
B. including a nondisclosure clause in the CSP contract
C. assessing the data classification scheme

D. reviewing CSP access privileges
110. - (Exam Topic 2)
Which of the following would BEST help secure online financial transactions from improper users?
A. Review of log-in attempts
B. Multi-level authorization
C. Periodic review of audit trails
D. Multi-factor authentication
111. - (Exam Topic 2)
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
112. - (Exam Topic 2)
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.
113. - (Exam Topic 2)
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
114. - (Exam Topic 2)
Which of the following would be of GREATEST concern to a risk practitioner reviewing current key risk indicators (KRIs)?
A. The KRIs' source data lacks integrity.
B. The KRIs are not automated.
C. The KRIs are not quantitative.
D. The KRIs do not allow for trend analysis.
115. - (Exam Topic 2)
Which of the following is MOST likely to be impacted as a result of a new policy which allows staff members to remotely connect to the organization's IT systems via personal or public computers?
A. Risk appetite
B. Inherent risk
C. Key risk indicator (KRI)
D. Risk tolerance
116. - (Exam Topic 2)
A control owner identifies that the organization's shared drive contains personally identifiable information (Pll) 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.
117. - (Exam Topic 2)
An organization has four different projects competing for funding to reduce overall IT risk. Which project should management defer?

Project Name	Initial Risk Rating	Residual Risk R
Alpha	High	Medium
Bravo	High	Low
Charlie	High	High

A. Project Charlie
B. Project Bravo
C. Project Alpha
D. Project Delta
118. - (Exam Topic 2)
Which of the following is the BEST way to identify changes in the risk profile of an organization?
A. Monitor key risk indicators (KRIs).
B. Monitor key performance indicators (KPIs).
C. Interview the risk owner.
D. Conduct a gap analysis
119. - (Exam Topic 2)
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
120. - (Exam Topic 2)
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
121. - (Exam Topic 2)
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
122. - (Exam Topic 2)

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
123. - (Exam Topic 2)
Performing a background check on a new employee candidate before hiring is an example of what type of control?
A. Detective
B. Compensating
C. Corrective
D. Preventive
124. - (Exam Topic 2)
Which of the following provides the MOST important information to facilitate a risk response decision?
A. Audit findings
B. Risk appetite
C. Key risk indicators
D. Industry best practices
125. - (Exam Topic 2)
Which of the following can be interpreted from a single data point on a risk heat map?
A. Risk tolerance
B. Risk magnitude
C. Risk response
D. Risk appetite
126. - (Exam Topic 2)
Which of the following is the BEST approach for performing a business impact analysis (BIA) of a supply-chain management application?
A. Reviewing the organization's policies and procedures
B. Interviewing groups of key stakeholders
C. Circulating questionnaires to key internal stakeholders
D. Accepting IT personnel s view of business issues
127. - (Exam Topic 2)
A business unit has decided to accept the risk of implementing an off-the-shelf, commercial software package that uses weak password controls. The BEST course of action would be to:
A. obtain management approval for policy exception.
B. develop an improved password software routine.
C. select another application with strong password controls.
D. continue the implementation with no changes.
128. - (Exam Topic 2)
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
129. - (Exam Topic 2)
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
130. - (Exam Topic 2)
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
131. - (Exam Topic 2)
Which of the following is MOST commonly compared against the risk appetite?
A. IT risk
B. Inherent risk
C. Financial risk
D. Residual risk
132. - (Exam Topic 2)
The MOST effective approach to prioritize risk scenarios is by:
A. assessing impact to the strategic plan.
B. aligning with industry best practices.
C. soliciting input from risk management experts.
D. evaluating the cost of risk response.
133. - (Exam Topic 2)
An identified high probability risk scenario involving a critical, proprietary business function has an annualized cost of control higher than the annual loss expectancy. Which of the following is the BEST risk response?
A. Mitigate
B. Accept
C. Transfer
D. Avoid
134. - (Exam Topic 2)
Which of the following should a risk practitioner do FIRST when an organization decides to use a cloud service?
A. Review the vendor selection process and vetting criteria.
B. Assess whether use of service falls within risk tolerance thresholds.
C. Establish service level agreements (SLAs) with the vendor.
D. Check the contract for appropriate security risk and control provisions.
135. - (Exam Topic 2)
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.
136. - (Exam Topic 2)
Which of the following is the PRIMARY role of the board of directors in corporate risk governance?
A. Approving operational strategies and objectives
B. Monitoring the results of actions taken to mitigate risk
C. Ensuring the effectiveness of the risk management program
D. Ensuring risk scenarios are identified and recorded in the risk register
137. - (Exam Topic 2)
Prudent business practice requires that risk appetite not exceed:
A. inherent risk.
B. risk tolerance.
C. risk capacity.
D. residual risk.
138. - (Exam Topic 2)
Which of the following would BEST help identify the owner for each risk scenario in a risk register?
A. Determining which departments contribute most to risk
B. Allocating responsibility for risk factors equally to asset owners
C. Mapping identified risk factors to specific business processes
D. Determining resource dependency of assets
139. - (Exam Topic 2)
Which of the following will BEST support management repotting on risk?
A. Risk policy requirements
B. A risk register
C. Control self-assessment
D. Key performance Indicators
140. - (Exam Topic 2)
An organization has introduced risk ownership to establish clear accountability for each process. To ensure effective risk ownership, it is MOST important that:
A. senior management has oversight of the process.
B. process ownership aligns with IT system ownership.
C. segregation of duties exists between risk and process owners.
D. risk owners have decision-making authority.
141. - (Exam Topic 2)
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
142. - (Exam Topic 2)
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
143. - (Exam Topic 2)
Which of The following would offer the MOST insight with regard to an organization's risk culture?
A. Risk management procedures
B. Senior management interviews
C. Benchmark analyses
D. Risk management framework
144. - (Exam Topic 2)
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.
145. - (Exam Topic 2)
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
146. - (Exam Topic 2)
Which of the following provides The MOST useful information when determining a risk management program's maturity level?
A. Risk assessment results
B. A recently reviewed risk register
C. Key performance indicators (KPIs)
D. The organization's risk framework
147. - (Exam Topic 2)
Which of the following is the PRIMARY reason to update a risk register with risk assessment results?
A. To communicate the level and priority of assessed risk to management
B. To provide a comprehensive inventory of risk across the organization
C. To assign a risk owner to manage the risk
D. To enable the creation of action plans to address nsk
148. - (Exam Topic 2)
Which of the following would MOST likely result in updates to an IT risk appetite statement?
A. External audit findings
B. Feedback from focus groups
C. Self-assessment reports
D. Changes in senior management

149. - (Exam Topic 2)
Which of the following BEST indicates that an organizations risk management program is effective?
A. Fewer security incidents have been reported.
B. The number of audit findings has decreased.
C. Residual risk is reduced.
D. inherent risk Is unchanged.
150. - (Exam Topic 2)
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.
151. - (Exam Topic 2)
Which of the following approaches will BEST help to ensure the effectiveness of risk awareness training?
A. Piloting courses with focus groups
B. Using reputable third-party training programs
C. Reviewing content with senior management
D. Creating modules for targeted audiences
152. - (Exam Topic 2)
A monthly payment report is generated from the enterprise resource planning (ERP) software to validate data against the old and new payroll systems. What is the BEST way to mitigate the risk associated with data integrity loss in the new payroll system after data migration?
A. Compare new system reports with functional requirements.
B. Compare encrypted data with checksums.
C. Compare results of user acceptance testing (UAT) with the testing criteria.
D. Compare processing output from both systems using the previous month's data.
153. - (Exam Topic 2)
Which of The following is the MOST relevant information to include in a risk management strategy?
A. Quantified risk triggers
B. Cost of controls
C. Regulatory requirements
D. Organizational goals
154. - (Exam Topic 2)
An organization learns of a new ransomware attack affecting organizations worldwide. Which of the following should be done FIRST to reduce the likelihood of infection from the attack?
A. Identify systems that are vulnerable to being exploited by the attack.
B. Confirm with the antivirus solution vendor whether the next update will detect the attack.
C. Verify the data backup process and confirm which backups are the most recent ones available.
D. Obtain approval for funding to purchase a cyber insurance plan.
155. - (Exam Topic 2)
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.
156. - (Exam Topic 2)
Which of the following is the MAIN benefit of involving stakeholders in the selection of key risk indicators (KRIs)?
A. Improving risk awareness
B. Obtaining buy-in from risk owners
C. Leveraging existing metrics
D. Optimizing risk treatment decisions
157. - (Exam Topic 2)
When assessing the maturity level of an organization's risk management framework, which of the following deficiencies should be of GREATEST concern to a risk practitioner?
A. Unclear organizational risk appetite
B. Lack of senior management participation
C. Use of highly customized control frameworks
D. Reliance on qualitative analysis methods
158. - (Exam Topic 2)
When reporting risk assessment results to senior management, which of the following is MOST important to include to enable risk-based decision making?
A. Risk action plans and associated owners
B. Recent audit and self-assessment results
C. Potential losses compared to treatment cost
D. A list of assets exposed to the highest risk
159. - (Exam Topic 2)
Which of the following BEST confirms the existence and operating effectiveness of information systems controls?
A. Self-assessment questionnaires completed by management
B. Review of internal audit and third-party reports
C. Management review and sign-off on system documentation
D. First-hand direct observation of the controls in operation
160. - (Exam Topic 2)
Which of the following is the BEST indication that an organization's risk management program has not reached the desired maturity level?
A. Significant increases in risk mitigation budgets
B. Large fluctuations in risk ratings between assessments
C. A steady increase in the time to recover from incidents
D. A large number of control exceptions
161. - (Exam Topic 2)
Which of the following presents the GREATEST challenge for an IT risk practitioner who wants to report on trends in historical IT risk levels?
A. Qualitative measures for potential loss events
B. Changes in owners for identified IT risk scenarios
C. Changes in methods used to calculate probability
D. Frequent use of risk acceptance as a treatment option
162. - (Exam Topic 2)
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.
163. - (Exam Topic 2)
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
164. - (Exam Topic 2)
Which of the following should an organization perform to forecast the effects of a disaster?
A. Develop a business impact analysis (6IA).
B. Define recovery time objectives (RTO).
C. Analyze capability maturity model gaps.
D. Simulate a disaster recovery.
165. - (Exam Topic 2)
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.
166. - (Exam Topic 2)
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
167. - (Exam Topic 2)
A new regulator/ requirement imposes severe fines for data leakage involving customers' personally identifiable information (Pll). The risk practitioner has recommended avoiding the risk. Which of the following actions would BEST align with this recommendation?
A. Reduce retention periods for Pll data.
B. Move Pll to a highly-secured outsourced site.
C. Modify business processes to stop collecting Pll.
D. Implement strong encryption for Pll.
168. - (Exam Topic 2)
Which stakeholders are PRIMARILY responsible for determining enterprise IT risk appetite?
A. Audit and compliance management
B. The chief information officer (CIO) and the chief financial officer (CFO)
C. Enterprise risk management and business process owners
D. Executive management and the board of directors
169. - (Exam Topic 2)
Which of the following is the BEST course of action when risk is found to be above the acceptable risk appetite?
A. Review risk tolerance levels
B. Maintain the current controls.
C. Analyze the effectiveness of controls.
D. Execute the risk response plan
170. - (Exam Topic 2)
Which of the following is the BEST key performance indicator (KPI) to measure the effectiveness of an anti-virus program?
A. Frequency of anti-virus software updates
B. Number of alerts generated by the anti-virus software
C. Number of false positives detected over a period of time
D. Percentage of IT assets with current malware definitions
171. - (Exam Topic 2)
Which of the following BEST supports the communication of risk assessment results to stakeholders?
A. Monitoring of high-risk areas
B. Classification of risk profiles
C. Periodic review of the risk register
D. Assignment of risk ownership
172. - (Exam Topic 2)
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
173. - (Exam Topic 2)
Which of the following is MOST critical to the design of relevant risk scenarios?
A. The scenarios are based on past incidents.
B. The scenarios are linked to probable organizational situations.
C. The scenarios are mapped to incident management capabilities.
D. The scenarios are aligned with risk management capabilities.
174. - (Exam Topic 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
175. - (Exam Topic 2)
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

176. - (Exam Topic 2)
Which of the following is the GREATEST concern associated with the transmission of healthcare data across the internet?
A. Unencrypted data
B. Lack of redundant circuits
C. Low bandwidth connections
D. Data integrity
177. - (Exam Topic 2)
Which of the following is the MOST important consideration when identifying stakeholders to review risk scenarios developed by a risk analyst? The reviewers are:
A. accountable for the affected processes.
B. members of senior management.
C. authorized to select risk mitigation options.
D. independent from the business operations.
178. - (Exam Topic 2)
A risk practitioner recently discovered that sensitive data from the production environment is required for testing purposes in non-production environments. Which of the following i the BEST recommendation to address this situation?
A. Enable data encryption in the test environment
B. Implement equivalent security in the test environment.
C. Prevent the use of production data for test purposes
D. Mask data before being transferred to the test environment.
179. - (Exam Topic 2)
Which of the following provides The BEST information when determining whether to accept residual risk of a critical system to be implemented?
A. Single loss expectancy (SLE)
B. Cost of the information system
C. Availability of additional compensating controls
D. Potential business impacts are within acceptable levels
180. - (Exam Topic 2)
A risk owner has accepted a high-impact risk because the control was adversely affecting process efficiency. Before updating the risk register, it is MOST important for the risk practitioner to:
A. ensure suitable insurance coverage is purchased.
B. negotiate with the risk owner on control efficiency.
C. reassess the risk to confirm the impact.
D. obtain approval from senior management.
181. - (Exam Topic 2)
Which of the following is the BEST indication of the effectiveness of a business continuity program?
A. Business continuity tests are performed successfully and issues are addressed.
B. Business impact analyses are reviewed and updated in a timely manner.
C. Business continuity and disaster recovery plans are regularly updated.
D. Business units are familiar with the business continuity plans and process.
182. - (Exam Topic 2)
Which of the following IT key risk indicators (KRIs) provides management with the BEST feedback on IT capacity?
A. Trends in IT resource usage
B. Trends in IT maintenance costs
C. Increased resource availability
D. Increased number of incidents
183. - (Exam Topic 2)
During an IT department reorganization, the manager of a risk mitigation action plan was replaced. The new manager has begun implementing a new control after identifying a more effective option. Which of the following is the risk practitioner's BEST course of action?
A. Communicate the decision to the risk owner for approval
B. Seek approval from the previous action plan manager.
C. Identify an owner for the new control.
D. Modify the action plan in the risk register.
184. - (Exam Topic 2)
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
185. - (Exam Topic 2)
What should a risk practitioner do FIRST upon learning a risk treatment owner has implemented a different control than what was specified in the IT risk action plan?
A. Seek approval from the control owner.
B. Update the action plan in the risk register.
C. Reassess the risk level associated with the new control.
D. Validate that the control has an established testing method.
186. - (Exam Topic 2)
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.
187. - (Exam Topic 2)
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
188. - (Exam Topic 2)
Which of the following is the MOST important consideration when determining whether to accept residual risk after security controls have been implemented on a critical system?
A. Cost versus benefit of additional mitigating controls
B. Annualized loss expectancy (ALE) for the system
C. Frequency of business impact
D. Cost of the Information control system

189. - (Exam Topic 2)
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)
190. - (Exam Topic 2)
During a control review, the control owner states that an existing control has deteriorated over time. What is the BEST recommendation to the control owner?
A. Implement compensating controls to reduce residual risk
B. Escalate the issue to senior management
C. Discuss risk mitigation options with the risk owner.
D. Certify the control after documenting the concern.
191. - (Exam Topic 2)
The MOST significant benefit of using a consistent risk ranking methodology across an organization is that it enables:
A. allocation of available resources
B. clear understanding of risk levels
C. assignment of risk to the appropriate owners
D. risk to be expressed in quantifiable terms
192. - (Exam Topic 2)
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.
193. - (Exam Topic 2)
A risk practitioner has learned that an effort to implement a risk mitigation action plan has stalled due to lack of funding. The risk practitioner should report that the associated risk has been:
A. mitigated
B. accepted
C. avoided
D. deferred
194. - (Exam Topic 2)
Which of the following is the BEST approach for determining whether a risk action plan is effective?
A. Comparing the remediation cost against budget
B. Assessing changes in residual risk
C. Assessing the inherent risk
D. Monitoring changes of key performance indicators
195. - (Exam Topic 2)
The maturity of an IT risk management program is MOST influenced by:
A. the organization's risk culture
B. benchmarking results against similar organizations
C. industry-specific regulatory requirements
D. expertise available within the IT department
196. - (Exam Topic 2)
Which of the following is an IT business owner's BEST course of action following an unexpected increase in emergency changes?
A. Evaluating the impact to control objectives
B. Conducting a root cause analysis
C. Validating the adequacy of current processes
D. Reconfiguring the IT infrastructure
197. - (Exam Topic 2)
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
198. - (Exam Topic 2)
A bank has outsourced its statement printing function to an external service provider. Which of the follow

NEW QUESTION 168
- (Exam Topic 2)
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)

Answer: A

NEW QUESTION 173
- (Exam Topic 2)
Which of the following is the BEST key performance indicator (KPI) for determining how well an IT policy is aligned to business requirements?

A. Total cost to support the policy
B. Number of exceptions to the policy
C. Total cost of policy breaches
D. Number of inquiries regarding the policy

Answer: C

NEW QUESTION 177
- (Exam Topic 2)
A maturity model will BEST indicate:

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

Answer: B

NEW QUESTION 182
- (Exam Topic 2)
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.

Answer: C

NEW QUESTION 187
- (Exam Topic 2)
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

Answer: B

NEW QUESTION 190
- (Exam Topic 2)
Who is PRIMARILY accountable for risk treatment decisions?

A. Risk owner
B. Business manager
C. Data owner
D. Risk manager

Answer: B

NEW QUESTION 191
- (Exam Topic 2)
Which of the following is the PRIMARY responsibility of the first line of defense related to computer-enabled fraud?

A. Providing oversight of risk management processes
B. Implementing processes to detect and deter fraud
C. Ensuring that risk and control assessments consider fraud
D. Monitoring the results of actions taken to mitigate fraud

Answer: C

NEW QUESTION 195
- (Exam Topic 2)
The BEST key performance indicator (KPI) to measure the effectiveness of a vulnerability remediation program is the number of:

A. vulnerability scans.
B. recurring vulnerabilities.
C. vulnerabilities remediated,
D. new vulnerabilities identified.

Answer: C

NEW QUESTION 198
- (Exam Topic 2)
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.

Answer:

A

NEW QUESTION 203
- (Exam Topic 2)
An organization's financial analysis department uses an in-house forecasting application for business projections. Who is responsible for defining access roles to protect the sensitive data within this application?

A. IT risk manager
B. IT system owner
C. Information security manager
D. Business owner

Answer: D

NEW QUESTION 205
- (Exam Topic 2)
Mapping open risk issues to an enterprise risk heat map BEST facilitates:

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

Answer: D

NEW QUESTION 210
- (Exam Topic 2)
Which of the following is MOST important for an organization to have in place when developing a risk management framework?

A. A strategic approach to risk including an established risk appetite
B. A risk-based internal audit plan for the organization
C. A control function within the risk management team
D. An organization-wide risk awareness training program

Answer: A

NEW QUESTION 213
- (Exam Topic 2)
Which of the following should be a risk practitioner's NEXT action after identifying a high probability of data loss in a system?

A. Enhance the security awareness program.
B. Increase the frequency of incident reporting.
C. Purchase cyber insurance from a third party.
D. Conduct a control assessment.

Answer: D

NEW QUESTION 214
- (Exam Topic 2)
Which of the following is the MOST important input when developing risk scenarios?

A. Key performance indicators
B. Business objectives
C. The organization's risk framework
D. Risk appetite

Answer: B

NEW QUESTION 216
- (Exam Topic 2)
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 anal/sis 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

Answer: A

NEW QUESTION 220
- (Exam Topic 2)
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.

Answer: C

NEW QUESTION 223
- (Exam Topic 2)
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

Answer: A

NEW QUESTION 228
- (Exam Topic 2)
The BEST key performance indicator (KPI) for monitoring adherence to an organization's user accounts provisioning practices is the percentage of:

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

Answer: A

NEW QUESTION 230
- (Exam Topic 2)
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

Answer: B

NEW QUESTION 234
- (Exam Topic 2)
An organization with a large number of applications wants to establish a security risk assessment program. Which of the following would provide the MOST useful information when determining the frequency of risk assessments?

A. Feedback from end users
B. Results of a benchmark analysis
C. Recommendations from internal audit
D. Prioritization from business owners

Answer: D

NEW QUESTION 237
- (Exam Topic 2)
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

Answer: A

NEW QUESTION 239
- (Exam Topic 2)
Management has required information security awareness training to reduce the risk associated with credential compromise. What is the BEST way to assess the effectiveness of the training?

A. Conduct social engineering testing.
B. Audit security awareness training materials.
C. Administer an end-of-training quiz.
D. Perform a vulnerability assessment.

Answer: A

NEW QUESTION 243
- (Exam Topic 2)

Which of the following would be MOST relevant to stakeholders regarding ineffective control implementation?

A. Threat to IT
B. Number of control failures
C. Impact on business
D. Risk ownership

Answer: C

NEW QUESTION 245
- (Exam Topic 2)
A control owner responsible for the access management process has developed a machine learning model to automatically identify excessive access privileges. What is the risk practitioner's BEST course of action?

A. Review the design of the machine learning model against control objectives.
B. Adopt the machine learning model as a replacement for current manual access reviews.
C. Ensure the model assists in meeting regulatory requirements for access controls.
D. Discourage the use of emerging technologies in key processes.

Answer: A

NEW QUESTION 248
- (Exam Topic 2)
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)

Answer: D

NEW QUESTION 252
- (Exam Topic 2)
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

Answer: C

NEW QUESTION 256
- (Exam Topic 2)
Which of the following BEST helps to balance the costs and benefits of managing IT risk?

A. Prioritizing risk responses
B. Evaluating risk based on frequency and probability
C. Considering risk factors that can be quantified
D. Managing the risk by using controls

Answer: A

NEW QUESTION 258
- (Exam Topic 2)
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

Answer: D

NEW QUESTION 260
- (Exam Topic 2)
During the initial risk identification process for a business application, it is MOST important to include which of the following stakeholders?

A. Business process owners
B. Business process consumers
C. Application architecture team
D. Internal audit

Answer: A

NEW QUESTION 262
- (Exam Topic 2)
Which of the following is a KEY responsibility of the second line of defense?

A. Implementing control activities
B. Monitoring control effectiveness
C. Conducting control self-assessments
D. Owning risk scenarios

Answer: B

NEW QUESTION 267
- (Exam Topic 2)
When updating a risk register with the results of an IT risk assessment, the risk practitioner should log:

A. high impact scenarios.
B. high likelihood scenarios.
C. treated risk scenarios.
D. known risk scenarios.

Answer: D

NEW QUESTION 269
- (Exam Topic 2)
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

Answer: C

NEW QUESTION 274
- (Exam Topic 2)
The PRIMARY purpose of using control metrics is to evaluate the:

A. amount of risk reduced by compensating controls.
B. amount of risk present in the organization.
C. variance against objectives.
D. number of incidents.

Answer: C

NEW QUESTION 279
- (Exam Topic 2)
Which of the following should be included in a risk assessment report to BEST facilitate senior management's understanding of the results?

A. Benchmarking parameters likely to affect the results
B. Tools and techniques used by risk owners to perform the assessments
C. A risk heat map with a summary of risk identified and assessed
D. The possible impact of internal and external risk factors on the assessment results

Answer: C

NEW QUESTION 281
- (Exam Topic 2)
What can be determined from the risk scenario chart?

Project Name	Initial Risk Rating	Residual Risk Rating	Project Cost
Sierra	Medium	Low	Low
Tango	Medium	Low	Medium
Uniform	High	High	High
Victor	High	Medium	Medium

A. Relative positions on the risk map
B. Risk treatment options
C. Capability of enterprise to implement
D. The multiple risk factors addressed by a chosen response

Answer: A

NEW QUESTION 284
- (Exam Topic 2)
Which of The following is the PRIMARY consideration when establishing an organization's risk management methodology?

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

Answer: A

NEW QUESTION 285
- (Exam Topic 2)
Following a significant change to a business process, a risk practitioner believes the associated risk has been reduced. The risk practitioner should advise the risk owner to FIRST

A. review the key risk indicators.
B. conduct a risk analysis.
C. update the risk register
D. reallocate risk response resources.

Answer: B

NEW QUESTION 288
- (Exam Topic 2)
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.

Answer: B

NEW QUESTION 293
- (Exam Topic 2)
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

Answer: A

NEW QUESTION 297
- (Exam Topic 2)
A risk practitioner is reviewing the status of an action plan to mitigate an emerging IT risk and finds the risk level has increased. The BEST course of action would be to:

A. implement the planned controls and accept the remaining risk.
B. suspend the current action plan in order to reassess the risk.
C. revise the action plan to include additional mitigating controls.
D. evaluate whether selected controls are still appropriate.

Answer: D

NEW QUESTION 301
- (Exam Topic 2)
A software developer has administrative access to a production application. Which of the following should be of GREATEST concern to a risk practitioner?

A. The administrative access does not allow for activity log monitoring.
B. The administrative access does not follow password management protocols.
C. The administrative access represents a deviation from corporate policy.
D. The administrative access represents a segregation of duties conflict.

Answer: D

NEW QUESTION 303
- (Exam Topic 2)
Which of the following is MOST important for an organization that wants to reduce IT operational risk?

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

Answer: D

NEW QUESTION 305
- (Exam Topic 2)
Which of the following is the MOST effective way to mitigate identified risk scenarios?

A. Assign ownership of the risk response plan
B. Provide awareness in early detection of risk.
C. Perform periodic audits on identified risk.
D. areas Document the risk tolerance of the organization.

Answer: A

NEW QUESTION 309
- (Exam Topic 2)
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

Answer: D

NEW QUESTION 314
- (Exam Topic 2)
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.

Answer: D

NEW QUESTION 318
- (Exam Topic 2)
An IT organization is replacing the customer relationship management (CRM) system. Who should own the risk associated with customer data leakage caused by insufficient IT security controls for the new system?

A. Chief information security officer
B. Business process owner
C. Chief risk officer
D. IT controls manager

Answer: B

NEW QUESTION 321
- (Exam Topic 2)
Which of the following criteria is MOST important when developing a response to an attack that would compromise data?

A. The recovery time objective (RTO)
B. The likelihood of a recurring attack
C. The organization's risk tolerance
D. The business significance of the information

Answer: D

NEW QUESTION 325
- (Exam Topic 2)
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.

Answer: D

NEW QUESTION 326
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

CRISC Practice Exam Features:

* CRISC Questions and Answers Updated Frequently

* CRISC Practice Questions Verified by Expert Senior Certified Staff

* CRISC Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* CRISC Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year