Isaca

Exam Questions CRISC

Certified in Risk and Information Systems Control

NEW QUESTION 1
- (Exam Topic 3)
Which of the following would be a risk practitioner's BEST course of action when a project team has accepted a risk outside the established risk appetite?

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

Answer: B

NEW QUESTION 2
- (Exam Topic 3)
Which of the following controls BEST enables an organization to ensure a complete and accurate IT asset inventory?

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

Answer: B

NEW QUESTION 3
- (Exam Topic 3)
When defining thresholds for control key performance indicators (KPIs). it is MOST helpful to align:

A. information risk assessments with enterprise risk assessments.
B. key risk indicators (KRIs) with risk appetite of the business.
C. the control key performance indicators (KPIs) with audit findings.
D. control performance with risk tolerance of business owners.

Answer: B

NEW QUESTION 4
- (Exam Topic 3)
The PRIMARY objective for requiring an independent review of an organization's IT risk management process should be to:

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

Answer: D

NEW QUESTION 5
- (Exam Topic 3)
Which of the following BEST enables an organization to determine whether external emerging risk factors will impact the organization's risk profile?

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

Answer: D

NEW QUESTION 6
- (Exam Topic 3)
Which of the following is the MAIN purpose of monitoring risk?

A. Communication
B. Risk analysis
C. Decision support
D. Benchmarking

Answer: A

NEW QUESTION 7
- (Exam Topic 3)
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

Answer: C

NEW QUESTION 8
- (Exam Topic 3)
The following is the snapshot of a recently approved IT risk register maintained by an organization's information security department.

Risk ID	Risk Title	Risk Description	Risk Submitter	Risk Owner	Control Owner(s)	Risk Likelihood Rating	Risk Impact Rating	Risk Exposure	Risk Response Type	Risk Response Description
R001	Mobile Data Theft	Laptops and mobile devices can be lost or stolen leading Internet leading to data compromise	Risk Council	End-User Computing Manager AND Inventory	IT Operations Manager AND Security Operations Manager	Low Likelihood	Very Serious	0 120	Mitigate	Purchase and acquire data encryption software for mobile
R003	Fire Hazard	A fire accident may destroy data center equipment and servers leading to loss of availability and services	Information Security Department	Data Center Facilities Manager	Facilities Manager	Low Likelihood	Serious	0 060	Transfer	Buy fire hazard insurance policy
		A disgruntled								

Significant	0 10	Low Likelihood	0 30
Serious	0 20	Likely	0 50
Very Serious	0 40	Highly Likely	0 70
Catastrophic	0 80	Near Certainty	0 90

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

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

Answer: B

NEW QUESTION 9
- (Exam Topic 3)
Which of the following would BEST indicate to senior management that IT processes are improving?

A. Changes in the number of intrusions detected
B. Changes in the number of security exceptions
C. Changes in the position in the maturity model
D. Changes to the structure of the risk register

Answer: B

NEW QUESTION 10
- (Exam Topic 3)
Which of the following is a risk practitioner's BEST recommendation to address an organization's need to secure multiple systems with limited IT resources?

A. Apply available security patches.
B. Schedule a penetration test.
C. Conduct a business impact analysis (BIA)
D. Perform a vulnerability analysis.

Answer: C

NEW QUESTION 10
- (Exam Topic 3)
Which of the following is the BEST reason to use qualitative measures to express residual risk levels related to emerging threats?

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

Answer: C

NEW QUESTION 11
- (Exam Topic 3)
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 14
- (Exam Topic 3)
When of the following provides the MOST tenable evidence that a business process control is effective?

A. Demonstration that the control is operating as designed
B. A successful walk-through of the associated risk assessment
C. Management attestation that the control is operating effectively
D. Automated data indicating that risk has been reduced

Answer: C

NEW QUESTION 15
- (Exam Topic 3)
Reviewing historical risk events is MOST useful for which of the following processes within the risk management life cycle?

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

Answer: D

NEW QUESTION 17
- (Exam Topic 3)
Which of the following BEST indicates the effectiveness of anti-malware software?

A. Number of staff hours lost due to malware attacks
B. Number of downtime hours in business critical servers
C. Number of patches made to anti-malware software
D. Number of successful attacks by malicious software

Answer: D

NEW QUESTION 22
- (Exam Topic 3)
In an organization that allows employee use of social media accounts for work purposes, which of the following is the BEST way to protect company sensitive information from being exposed?

A. Educating employees on what needs to be kept confidential
B. Implementing a data loss prevention (DLP) solution
C. Taking punitive action against employees who expose confidential data
D. Requiring employees to sign nondisclosure agreements

Answer: B

NEW QUESTION 26
- (Exam Topic 3)
Which of We following is the MOST effective control to address the risk associated with compromising data privacy within the cloud?

A. Establish baseline security configurations with the cloud service provider.
B. Require the cloud prowler 10 disclose past data privacy breaches.
C. Ensure the cloud service provider performs an annual risk assessment.
D. Specify cloud service provider liability for data privacy breaches in the contract

Answer: D

NEW QUESTION 28
- (Exam Topic 3)
Which of the following would provide the BEST evidence of an effective internal control environment/?

A. Risk assessment results
B. Adherence to governing policies

C. Regular stakeholder briefings
D. Independent audit results

Answer: D

NEW QUESTION 32
- (Exam Topic 3)
A risk practitioner identifies a database application that has been developed and implemented by the business independently of IT. Which of the following is the BEST course of action?

A. Escalate the concern to senior management.
B. Document the reasons for the exception.
C. Include the application in IT risk assessments.
D. Propose that the application be transferred to IT.

Answer: B

NEW QUESTION 37
- (Exam Topic 3)
An organization has made a decision to purchase a new IT system. During when phase of the system development life cycle (SDLC) will identified risk MOST likely lead to architecture and design trade-offs?

A. Acquisition
B. Implementation
C. Initiation
D. Operation and maintenance

Answer: C

NEW QUESTION 41
- (Exam Topic 3)
The BEST indication that risk management is effective is when risk has been reduced to meet:

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

Answer: C

NEW QUESTION 43
- (Exam Topic 3)
Which of the following BEST facilitates the mitigation of identified gaps between current and desired risk environment states?

A. Develop a risk treatment plan.
B. Validate organizational risk appetite.
C. Review results of prior risk assessments.
D. Include the current and desired states in the risk register.

Answer: A

NEW QUESTION 47
- (Exam Topic 3)
Which of the following presents the GREATEST risk to change control in business application development over the complete life cycle?

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

Answer: C

NEW QUESTION 49
- (Exam Topic 3)
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 54
- (Exam Topic 3)

An employee lost a personal mobile device that may contain sensitive corporate information. What should be the risk practitioner's recommendation?

A. Conduct a risk analysis.
B. Initiate a remote data wipe.
C. Invoke the incident response plan
D. Disable the user account.

Answer: C

NEW QUESTION 59
- (Exam Topic 3)
Which of the following is the MOST comprehensive resource for prioritizing the implementation of information systems controls?

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

Answer: C

NEW QUESTION 61
- (Exam Topic 3)
When of the following is the BEST key control indicator (KCI) to determine the effectiveness of en intrusion prevention system (IPS)?

A. Percentage of system uptime
B. Percentage of relevant threats mitigated
C. Total number of threats identified
D. Reaction time of the system to threats

Answer: B

NEW QUESTION 64
- (Exam Topic 3)
Which of the following is the BEST indicator of executive management's support for IT risk mitigation efforts?

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

Answer: B

NEW QUESTION 69
- (Exam Topic 3)
A peer review of a risk assessment finds that a relevant threat community was not included. Mitigation of the risk will require substantial changes to a software application. Which of the following is the BEST course of action?

A. Ask the business to make a budget request to remediate the problem.
B. Build a business case to remediate the fix.
C. Research the types of attacks the threat can present.
D. Determine the impact of the missing threat.

Answer: D

NEW QUESTION 73
- (Exam Topic 3)
Which of the following is the GREATEST risk associated with an environment that lacks documentation of the architecture?

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

Answer: D

NEW QUESTION 78
- (Exam Topic 3)
When developing risk scenario using a list of generic scenarios based on industry best practices, it is MOST imported to:

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

Answer: B

NEW QUESTION 80
- (Exam Topic 3)
When a risk practitioner is determining a system's criticality. it is MOST helpful to review the associated:

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

Answer: B

NEW QUESTION 84
- (Exam Topic 3)
Which element of an organization's risk register is MOST important to update following the commissioning of a new financial reporting system?

A. Key risk indicators (KRIs)
B. The owner of the financial reporting process
C. The risk rating of affected financial processes
D. The list of relevant financial controls

Answer: C

NEW QUESTION 85
- (Exam Topic 3)
An organization is analyzing the risk of shadow IT usage. Which of the following is the MOST important input into the assessment?

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

Answer: A

NEW QUESTION 88
- (Exam Topic 3)
The PRIMARY benefit of using a maturity model is that it helps to evaluate the:

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

Answer: B

NEW QUESTION 92
- (Exam Topic 3)
To help identify high-risk situations, an organization should:

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

Answer: A

NEW QUESTION 93
- (Exam Topic 3)
Who should be PRIMARILY responsible for establishing an organization's IT risk culture?

A. Business process owner
B. Executive management
C. Risk management
D. IT management

Answer: B

NEW QUESTION 98
- (Exam Topic 3)
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

Answer: D

NEW QUESTION 103
- (Exam Topic 3)
When preparing a risk status report for periodic review by senior management, it is MOST important to ensure the report includes

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

Answer: A

NEW QUESTION 106
- (Exam Topic 3)
While reviewing a contract of a cloud services vendor, it was discovered that the vendor refuses to accept liability for a sensitive data breach. Which of the following controls will BES reduce the risk associated with such a data breach?

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

Answer: B

NEW QUESTION 108
- (Exam Topic 3)
Determining if organizational risk is tolerable requires:

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

Answer: D

NEW QUESTION 113
- (Exam Topic 3)
A business unit is implementing a data analytics platform to enhance its customer relationship management (CRM) system primarily to process data that has been provided by its customers. Which of the following presents the GREATEST risk to the organization's reputation?

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

Answer: B

NEW QUESTION 118
- (Exam Topic 3)
During an acquisition, which of the following would provide the MOST useful input to the parent company's risk practitioner when developing risk scenarios for the post-acquisition phase?

A. Risk management framework adopted by each company
B. Risk registers of both companies
C. IT balanced scorecard of each company
D. Most recent internal audit findings from both companies

Answer: C

NEW QUESTION 122
- (Exam Topic 3)
An organization has used generic risk scenarios to populate its risk register. Which of the following presents the GREATEST challenge to assigning of the associated risk entries?

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

Answer: C

NEW QUESTION 123
- (Exam Topic 3)
The design of procedures to prevent fraudulent transactions within an enterprise resource planning (ERP) system should be based on:

A. stakeholder risk tolerance.
B. benchmarking criteria.

C. suppliers used by the organization.
D. the control environment.

Answer: D

NEW QUESTION 128
- (Exam Topic 3)
Which of the following is MOST important to the effectiveness of key performance indicators (KPIs)?

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

Answer: A

NEW QUESTION 130
- (Exam Topic 3)
Which of the following is the MOST important consideration when sharing risk management updates with executive management?

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

Answer: D

NEW QUESTION 131
- (Exam Topic 3)
Which of the following scenarios presents the GREATEST risk for a global organization when implementing a data classification policy?

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

Answer: D

NEW QUESTION 136
- (Exam Topic 3)
Which of the following management action will MOST likely change the likelihood rating of a risk scenario related to remote network access?

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

Answer: A

NEW QUESTION 140
- (Exam Topic 3)
Which of the following is the GREATEST risk associated with the misclassification of data?

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

Answer: A

NEW QUESTION 142
- (Exam Topic 3)
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.

Answer: B

NEW QUESTION 143
- (Exam Topic 3)
Which of the following is the BEST Key control indicator KCO to monitor the effectiveness of patch management?

A. Percentage of legacy servers out of support
B. Percentage of severs receiving automata patches
C. Number of unremediated vulnerabilities
D. Number of intrusion attempts

Answer: D

NEW QUESTION 144
- (Exam Topic 3)
Which of the following would be a risk practitioner's GREATEST concern with the use of a vulnerability scanning tool?

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

Answer: B

NEW QUESTION 146
- (Exam Topic 3)
Which of the following stakeholders are typically included as part of a line of defense within the three lines of defense model?

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

Answer: A

NEW QUESTION 150
- (Exam Topic 3)
Which of the following is the BEST way for a risk practitioner to present an annual risk management update to the board"

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

Answer: C

NEW QUESTION 155
- (Exam Topic 3)
Which of the following roles would be MOST helpful in providing a high-level view of risk related to customer data loss?

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

Answer: B

NEW QUESTION 159
- (Exam Topic 3)
A risk practitioner is utilizing a risk heat map during a risk assessment. Risk events that are coded with the same color will have a similar:

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

Answer: B

NEW QUESTION 161
- (Exam Topic 3)
Employees are repeatedly seen holding the door open for others, so that trailing employees do not have to stop and swipe their own ID badges. This behavior BEST represents:

A. a threat.
B. a vulnerability.
C. an impact
D. a control.

Answer: B

NEW QUESTION 164

- (Exam Topic 3)
Which of the following is MOST important for maintaining the effectiveness of an IT risk register?

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

Answer: D

NEW QUESTION 169
- (Exam Topic 3)
Which of the following is MOST important for mitigating ethical risk when establishing accountability for control ownership?

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

Answer: B

NEW QUESTION 172
- (Exam Topic 3)
An organization has experienced several incidents of extended network outages that have exceeded tolerance. Which of the following should be the risk practitioner's FIRST step to address this situation?

A. Recommend additional controls to address the risk.
B. Update the risk tolerance level to acceptable thresholds.
C. Update the incident-related risk trend in the risk register.
D. Recommend a root cause analysis of the incidents.

Answer: D

NEW QUESTION 177
- (Exam Topic 3)
A vulnerability assessment of a vendor-supplied solution has revealed that the software is susceptible to cross-site scripting and SQL injection attacks. Which of the following will BEST mitigate this issue?

A. Monitor the databases for abnormal activity
B. Approve exception to allow the software to continue operating
C. Require the software vendor to remediate the vulnerabilities
D. Accept the risk and let the vendor run the software as is

Answer: C

NEW QUESTION 178
- (Exam Topic 3)
Which of the following is the MOST appropriate action when a tolerance threshold is exceeded?

A. Communicate potential impact to decision makers.
B. Research the root cause of similar incidents.
C. Verify the response plan is adequate.
D. Increase human resources to respond in the interim.

Answer: A

NEW QUESTION 181
- (Exam Topic 3)
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 186
- (Exam Topic 3)
While reviewing the risk register, a risk practitioner notices that different business units have significant variances in inherent risk for the same risk scenario. Which of the following is the BEST course of action?

A. Update the risk register with the average of residual risk for both business units.
B. Review the assumptions of both risk scenarios to determine whether the variance is reasonable.
C. Update the risk register to ensure both risk scenarios have the highest residual risk.
D. Request that both business units conduct another review of the risk.

Answer: B

NEW QUESTION 190
- (Exam Topic 3)
Which of the following methods is an example of risk mitigation?

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

Answer: C

NEW QUESTION 194
- (Exam Topic 3)
Which of the following is the BEST indication that key risk indicators (KRIs) should be revised?

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

Answer: B

NEW QUESTION 195
- (Exam Topic 3)
Recovery the objectives (RTOs) should be based on

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

Answer: C

NEW QUESTION 199
- (Exam Topic 3)
Which of the following is MOST important to have in place to ensure the effectiveness of risk and security metrics reporting?

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

Answer: A

NEW QUESTION 202
- (Exam Topic 3)
Which of the following is MOST helpful in defining an early-warning threshold associated with insufficient network bandwidth''

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

Answer: A

NEW QUESTION 204
- (Exam Topic 3)
The acceptance of control costs that exceed risk exposure MOST likely demonstrates:

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

Answer: C

NEW QUESTION 205
- (Exam Topic 3)
Which of the following is the MOST important component in a risk treatment plan?

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

D. Treatment plan justification

Answer: D

NEW QUESTION 207
- (Exam Topic 3)
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.

Answer: D

NEW QUESTION 212
- (Exam Topic 3)
An organization must make a choice among multiple options to respond to a risk. The stakeholders cannot agree and decide to postpone the decision. Which of the following risk responses has the organization adopted?

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

Answer: D

NEW QUESTION 216
- (Exam Topic 3)
Which of the following is the MOST important objective from a cost perspective for considering aggregated risk responses in an organization?

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

Answer: C

NEW QUESTION 221
- (Exam Topic 3)
Which of the following is the GREATEST benefit when enterprise risk management (ERM) provides oversight of IT risk management?

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

Answer: A

NEW QUESTION 224
- (Exam Topic 3)
Which of the following should a risk practitioner recommend FIRST when an increasing trend of risk events and subsequent losses has been identified?

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

Answer: C

NEW QUESTION 228
- (Exam Topic 3)
An organization is implementing internet of Things (loT) technology to control temperature and lighting in its headquarters. Which of the following should be of GREATEST concern?

A. Insufficient network isolation
B. impact on network performance
C. insecure data transmission protocols
D. Lack of interoperability between sensors

Answer: D

NEW QUESTION 232
- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 236
- (Exam Topic 3)
During an internal IT audit, an active network account belonging to a former employee was identified. Which of the following is the BEST way to prevent future occurrences?

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

Answer: A

NEW QUESTION 240
- (Exam Topic 3)
Which of the following should be management's PRIMARY consideration when approving risk response action plans?

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

Answer: C

NEW QUESTION 243
- (Exam Topic 3)
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 245
- (Exam Topic 3)
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

Answer: D

NEW QUESTION 248
- (Exam Topic 3)
Which of the following will BEST help to ensure implementation of corrective action plans?

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

Answer: B

NEW QUESTION 253
- (Exam Topic 3)
Which of the following tasks should be completed prior to creating a disaster recovery plan (DRP)?

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

Answer: A

NEW QUESTION 257
- (Exam Topic 3)
Which key performance efficiency IKPI) BEST measures the effectiveness of an organization's disaster recovery program?

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

Answer: D

NEW QUESTION 262
- (Exam Topic 3)
Which of the following should be the PRIMARY goal of developing information security metrics?

A. Raising security awareness
B. Enabling continuous improvement
C. Identifying security threats
D. Ensuring regulatory compliance

Answer: B

NEW QUESTION 265
- (Exam Topic 3)
Which of the following will BEST help in communicating strategic risk priorities?

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

Answer: A

NEW QUESTION 268
- (Exam Topic 3)
A risk practitioner has been asked by executives to explain how existing risk treatment plans would affect risk posture at the end of the year. Which of the following is MOST helpful in responding to this request?

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

Answer: D

NEW QUESTION 271
- (Exam Topic 3)
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

Answer: D

NEW QUESTION 273
- (Exam Topic 3)
Which of the following will be MOST effective in uniquely identifying the originator of electronic transactions?

A. Digital signature
B. Edit checks
C. Encryption
D. Multifactor authentication

Answer: A

NEW QUESTION 277
- (Exam Topic 3)
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.

Answer: D

NEW QUESTION 279
- (Exam Topic 3)
Which of the following provides the BEST evidence that a selected risk treatment plan is effective?

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

Answer: C

NEW QUESTION 280
- (Exam Topic 3)
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.

Answer: B

NEW QUESTION 281
- (Exam Topic 3)
Which of the following is the BEST key control indicator (KCI) for risk related to IT infrastructure failure?

A. Number of times the recovery plan is reviewed
B. Number of successful recovery plan tests
C. Percentage of systems with outdated virus protection
D. Percentage of employees who can work remotely

Answer: B

NEW QUESTION 284
- (Exam Topic 3)
Which of the following should be of GREATEST concern lo a risk practitioner reviewing the implementation of an emerging technology?

A. Lack of alignment to best practices
B. Lack of risk assessment
C. Lack of risk and control procedures
D. Lack of management approval

Answer: B

NEW QUESTION 288
- (Exam Topic 3)
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

Answer: C

NEW QUESTION 293
- (Exam Topic 3)
What is the PRIMARY reason to periodically review key performance indicators (KPIs)?

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

Answer: A

NEW QUESTION 298
- (Exam Topic 3)
When evaluating a number of potential controls for treating risk, it is MOST important to consider:

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

D. risk tolerance and control complexity.

Answer: C

NEW QUESTION 303
- (Exam Topic 3)
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.

Answer: A

NEW QUESTION 307
- (Exam Topic 3)
A risk practitioner has received an updated enterprise risk management (ERM) report showing that residual risk is now within the organization's defined appetite and tolerance levels. Which of the following is the risk practitioner's BEST course of action?

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

Answer: D

NEW QUESTION 308
- (Exam Topic 3)
When reviewing a business continuity plan (BCP). which of the following would be the MOST significant deficiency?

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

Answer: B

NEW QUESTION 310
- (Exam Topic 3)
An organization wants to grant remote access to a system containing sensitive data to an overseas third party. Which of the following should be of GREATEST concern to management?

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

Answer: C

NEW QUESTION 315
- (Exam Topic 3)
When performing a risk assessment of a new service to support a ewe Business process. which of the following should be done FRST10 ensure continuity of operations?

A. a identity conditions that may cause disruptions
B. Review incident response procedures
C. Evaluate the probability of risk events
D. Define metrics for restoring availability

Answer: A

NEW QUESTION 316
- (Exam Topic 3)
Which of the following is MOST helpful in providing an overview of an organization's risk management program?

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

Answer: C

NEW QUESTION 318

- (Exam Topic 3)
Which of the following would present the MOST significant risk to an organization when updating the incident response plan?

A. Obsolete response documentation
B. Increased stakeholder turnover
C. Failure to audit third-party providers
D. Undefined assignment of responsibility

Answer: D

NEW QUESTION 321
- (Exam Topic 3)
Winch of the following key control indicators (KCIs) BEST indicates whether security requirements are identified and managed throughout a project He cycle?

A. Number of projects going live without a security review
B. Number of employees completing project-specific security training
C. Number of security projects started in core departments
D. Number of security-related status reports submitted by project managers

Answer: D

NEW QUESTION 322
- (Exam Topic 3)
Which of the following is MOST important to compare against the corporate risk profile?

A. Industry benchmarks
B. Risk tolerance
C. Risk appetite
D. Regulatory compliance

Answer: D

NEW QUESTION 324
- (Exam Topic 3)
An application runs a scheduled job that compiles financial data from multiple business systems and updates the financial reporting system. If this job runs too long, it can delay financial reporting. Which of the following is the risk practitioner's BEST recommendation?

A. Implement database activity and capacity monitoring.
B. Ensure the business is aware of the risk.
C. Ensure the enterprise has a process to detect such situations.
D. Consider providing additional system resources to this job.

Answer: C

NEW QUESTION 329
- (Exam Topic 3)
During a risk assessment, a key external technology supplier refuses to provide control design and effectiveness information, citing confidentiality concerns. What should the risk practitioner do NEXT?

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

Answer: C

NEW QUESTION 332
- (Exam Topic 3)
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

Answer: C

NEW QUESTION 335
- (Exam Topic 3)
Which of the following provides the MOST useful information when developing a risk profile for management approval?

A. Residual risk and risk appetite
B. Strength of detective and preventative controls
C. Effectiveness and efficiency of controls
D. Inherent risk and risk tolerance

Answer: A

NEW QUESTION 337
- (Exam Topic 3)
The PRIMARY benefit associated with key risk indicators (KRIs) is that they:

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

Answer: D

NEW QUESTION 340
- (Exam Topic 3)
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 345
- (Exam Topic 3)
Which of the following is the MOST important key performance indicator (KPI) to monitor the effectiveness of disaster recovery processes?

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

Answer: D

NEW QUESTION 346
- (Exam Topic 3)
Which of the following is the BEST way to help ensure risk will be managed properly after a business process has been re-engineered?

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

Answer: A

NEW QUESTION 347
- (Exam Topic 3)
Which of the following BEST enables a risk practitioner to enhance understanding of risk among stakeholders?

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

Answer: B

NEW QUESTION 351
- (Exam Topic 3)
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

Answer: A

NEW QUESTION 353
- (Exam Topic 3)
The objective of aligning mitigating controls to risk appetite is to ensure that:

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

Answer:

D

NEW QUESTION 355
- (Exam Topic 3)
Which of the following is the BEST key performance indicator (KPI) to measure the effectiveness of an antivirus program?

A. Percentage of IT assets with current malware definitions
B. Number of false positives defected over a period of time
C. Number of alerts generated by the anti-virus software
D. Frequency of anti-vinjs software updates

Answer: A

NEW QUESTION 360
- (Exam Topic 3)
When formulating a social media policy lo address information leakage, which of the following is the MOST important concern to address?

A. Sharing company information on social media
B. Sharing personal information on social media
C. Using social media to maintain contact with business associates
D. Using social media for personal purposes during working hours

Answer: A

NEW QUESTION 364
- (Exam Topic 3)
Which of the following is the MOST effective way to incorporate stakeholder concerns when developing risk scenarios?

A. Evaluating risk impact
B. Establishing key performance indicators (KPIs)
C. Conducting internal audits
D. Creating quarterly risk reports

Answer: A

NEW QUESTION 366
- (Exam Topic 3)
Which of the following would be the GREATEST challenge when implementing a corporate risk framework for a global organization?

A. Privacy risk controls
B. Business continuity
C. Risk taxonomy
D. Management support

Answer: A

NEW QUESTION 371
- (Exam Topic 3)
When an organization is having new software implemented under contract, which of the following is key to controlling escalating costs?

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

Answer: B

NEW QUESTION 372
- (Exam Topic 3)
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.

Answer: C

NEW QUESTION 375
- (Exam Topic 3)
An organization has provided legal text explaining the rights and expected behavior of users accessing a system from geographic locations that have strong privacy regulations. Which of the following control types has been applied?

A. Detective
B. Directive
C. Preventive

D. Compensating

Answer: B

NEW QUESTION 380
- (Exam Topic 3)
The GREATEST benefit of including low-probability, high-impact events in a risk assessment is the ability to:

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

Answer: D

NEW QUESTION 382
- (Exam Topic 3)
Which of the following provides the MOST useful information to determine risk exposure following control implementations?

A. Strategic plan and risk management integration
B. Risk escalation and process for communication
C. Risk limits, thresholds, and indicators
D. Policies, standards, and procedures

Answer: C

NEW QUESTION 387
- (Exam Topic 3)
A global company s business continuity plan (BCP) requires the transfer of its customer information…. event of a disaster. Which of the following should be the MOST important risk consideration?

A. The difference In the management practices between each company
B. The cloud computing environment is shared with another company
C. The lack of a service level agreement (SLA) in the vendor contract
D. The organizational culture differences between each country

Answer: B

NEW QUESTION 389
- (Exam Topic 3)
Which of the following should be done FIRST when information is no longer required to support business objectives?

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

Answer: C

NEW QUESTION 394
- (Exam Topic 3)
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

Answer: A

NEW QUESTION 396
- (Exam Topic 3)
When a high-risk security breach occurs, which of the following would be MOST important to the person responsible for managing the incident?

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

Answer: B

NEW QUESTION 401
- (Exam Topic 3)
A newly hired risk practitioner finds that the risk register has not been updated in the past year. What is the risk practitioner's BEST course of action?

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

Answer: A

NEW QUESTION 403
- (Exam Topic 3)
An organization has recently been experiencing frequent data corruption incidents. Implementing a file corruption detection tool as a risk response strategy will help to:

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

Answer: D

NEW QUESTION 406
- (Exam Topic 3)
Which of the following findings of a security awareness program assessment would cause the GREATEST concern to a risk practitioner?

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

Answer: D

NEW QUESTION 410
- (Exam Topic 3)
Which of the following is MOST useful when communicating risk to management?

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

Answer: C

NEW QUESTION 414
- (Exam Topic 3)
Which of the following is the BEST method of creating risk awareness in an organization?

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

Answer: B

NEW QUESTION 415
- (Exam Topic 3)
When reporting on the performance of an organization's control environment including which of the following would BEST inform stakeholders risk decision-making?

A. The audit plan for the upcoming period
B. Spend to date on mitigating control implementation
C. A report of deficiencies noted during controls testing
D. A status report of control deployment

Answer: C

NEW QUESTION 418
- (Exam Topic 3)
Which of the following is a KEY consideration for a risk practitioner to communicate to senior management evaluating the introduction of artificial intelligence (Al) solutions into the organization?

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

Answer: B

NEW QUESTION 420
- (Exam Topic 3)
Which of the following BEST enforces access control for an organization that uses multiple cloud technologies?

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

Answer: C

NEW QUESTION 423
- (Exam Topic 3)
Of the following, who is accountable for ensuing the effectiveness of a control to mitigate risk?

A. Control owner
B. Risk manager
C. Control operator
D. Risk treatment owner

Answer: A

NEW QUESTION 424
- (Exam Topic 3)
When of the following 15 MOST important when developing a business case for a proposed security investment?

A. identification of control requirements
B. Alignment to business objectives
C. Consideration of new business strategies
D. inclusion of strategy for regulatory compliance

Answer: B

NEW QUESTION 428
- (Exam Topic 3)
Which of the following practices would be MOST effective in protecting personality identifiable information (Ptl) from unauthorized access m a cloud environment?

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

Answer: B

NEW QUESTION 433
- (Exam Topic 3)
An organization has decided to postpone the assessment and treatment of several risk scenarios because stakeholders are unavailable. As a result of this decision, the risk associated with these new entries has been;

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

Answer: C

NEW QUESTION 435
- (Exam Topic 3)
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

Answer: B

NEW QUESTION 436
- (Exam Topic 3)
Which of the following is the FIRST step when conducting a business impact analysis (BIA)?

A. Identifying critical information assets
B. Identifying events impacting continuity of operations;
C. Creating a data classification scheme
D. Analyzing previous risk assessment results

Answer:

A

NEW QUESTION 437
- (Exam Topic 2)
A new policy has been published to forbid copying of data onto removable media. Which type of control has been implemented?

A. Preventive
B. Detective
C. Directive
D. Deterrent

Answer: C

NEW QUESTION 439
- (Exam Topic 2)
Which of the following is a crucial component of a key risk indicator (KRI) to ensure appropriate action is taken to mitigate risk?

A. Management intervention
B. Risk appetite
C. Board commentary
D. Escalation triggers

Answer: D

NEW QUESTION 443
- (Exam Topic 2)
A risk practitioner notices a trend of noncompliance with an IT-related control. Which of the following would BEST assist in making a recommendation to management?

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

Answer: A

NEW QUESTION 445
- (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 446
- (Exam Topic 2)
Which of the following is performed after a risk assessment is completed?

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

Answer: C

NEW QUESTION 451
- (Exam Topic 2)
The MOST important reason to aggregate results from multiple risk assessments on interdependent information systems is to:

A. establish overall impact to the organization
B. efficiently manage the scope of the assignment
C. identify critical information systems
D. facilitate communication to senior management

Answer: A

NEW QUESTION 453
- (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

Answer: C

NEW QUESTION 458
- (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.

Answer: D

NEW QUESTION 461
- (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.

Answer: A

NEW QUESTION 462
- (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

Answer: C

NEW QUESTION 463
- (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 468
- (Exam Topic 2)
Which of the following would present the GREATEST challenge when assigning accountability for control ownership?

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

Answer: D

NEW QUESTION 470
- (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.

Answer: B

NEW QUESTION 471
- (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.

Answer: C

NEW QUESTION 476
- (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

Answer: A

NEW QUESTION 479
- (Exam Topic 2)
Which of the following is MOST helpful in verifying that the implementation of a risk mitigation control has been completed as intended?

A. An updated risk register
B. Risk assessment results
C. Technical control validation
D. Control testing results

Answer: D

NEW QUESTION 481
- (Exam Topic 2)
A risk practitioner has been notified that an employee sent an email in error containing customers' personally identifiable information (Pll). Which of the following is the risk practitioner's BEST course of action?

A. Report it to the chief risk officer.
B. Advise the employee to forward the email to the phishing team.
C. follow incident reporting procedures.
D. Advise the employee to permanently delete the email.

Answer: C

NEW QUESTION 483
- (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

Answer: C

NEW QUESTION 484
- (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

Answer: D

NEW QUESTION 487
- (Exam Topic 2)
A business manager wants to leverage an existing approved vendor solution from another area within the organization. Which of the following is the risk practitioner's BEST course of action?

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

Answer: D

NEW QUESTION 488

- (Exam Topic 2)
The PRIMARY benefit of classifying information assets is that it helps to:

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

Answer: D

NEW QUESTION 491
- (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 496
- (Exam Topic 2)
Which of the following should be the PRIMARY focus of an independent review of a risk management process?

A. Accuracy of risk tolerance levels
B. Consistency of risk process results
C. Participation of stakeholders
D. Maturity of the process

Answer: B

NEW QUESTION 499
- (Exam Topic 2)
Which of the following is the MOST important reason to revisit a previously accepted risk?

A. To update risk ownership
B. To review the risk acceptance with new stakeholders
C. To ensure risk levels have not changed
D. To ensure controls are still operating effectively

Answer: C

NEW QUESTION 500
- (Exam Topic 2)
An IT operations team implements disaster recovery controls based on decisions from application owners regarding the level of resiliency needed. Who is the risk owner in this scenario?

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

Answer: C

NEW QUESTION 502
- (Exam Topic 2)
An organization is planning to outsource its payroll function to an external service provider Which of the following should be the MOST important consideration when selecting the provider?

A. Disaster recovery plan (DRP) of the system
B. Right to audit the provider
C. Internal controls to ensure data privacy
D. Transparency of key performance indicators (KPIs)

Answer: B

NEW QUESTION 505
- (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.

Answer: C

NEW QUESTION 510
- (Exam Topic 2)
A risk practitioner observes that the fraud detection controls in an online payment system do not perform as expected. Which of the following will MOST likely change as a result?

A. Impact
B. Residual risk
C. Inherent risk
D. Risk appetite

Answer: B

NEW QUESTION 515
- (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.

Answer: A

NEW QUESTION 518
- (Exam Topic 2)
Which of the following should be the PRIMARY objective of a risk awareness training program?

A. To enable risk-based decision making
B. To promote awareness of the risk governance function
C. To clarify fundamental risk management principles
D. To ensure sufficient resources are available

Answer: A

NEW QUESTION 521
- (Exam Topic 2)
A risk practitioner notices that a particular key risk indicator (KRI) has remained below its established trigger point for an extended period of time. Which of the following should be done FIRST?

A. Recommend a re-evaluation of the current threshold of the KRI.
B. Notify management that KRIs are being effectively managed.
C. Update the risk rating associated with the KRI In the risk register.
D. Update the risk tolerance and risk appetite to better align to the KRI.

Answer: A

NEW QUESTION 525
- (Exam Topic 2)
Which of the following BEST enables a proactive approach to minimizing the potential impact of unauthorized data disclosure?

A. Key risk indicators (KRIs)
B. Data backups
C. Incident response plan
D. Cyber insurance

Answer: C

NEW QUESTION 526
- (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.

Answer: C

NEW QUESTION 527
- (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.

Answer: D

NEW QUESTION 531
- (Exam Topic 2)
Which of the following is the BEST way for a risk practitioner to verify that management has addressed control issues identified during a previous external audit?

A. Interview control owners.
B. Observe the control enhancements in operation.
C. Inspect external audit documentation.
D. Review management's detailed action plans.

Answer: B

NEW QUESTION 532
- (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.

Answer: C

NEW QUESTION 533
- (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.

Answer: B

NEW QUESTION 534
- (Exam Topic 2)
Which of the following is the GREATEST concern associated with business end users developing their own applications on end user spreadsheets and database programs?

A. An IT project manager is not assigned to oversee development.
B. Controls are not applied to the applications.
C. There is a lack of technology recovery options.
D. The applications are not captured in the risk profile.

Answer: C

NEW QUESTION 537
- (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 540
- (Exam Topic 2)
Whose risk tolerance matters MOST when making a risk decision?

A. Customers who would be affected by a breach
B. Auditors, regulators and standards organizations
C. The business process owner of the exposed assets
D. The information security manager

Answer: C

NEW QUESTION 544
- (Exam Topic 2)
An organization has received notification that it is a potential victim of a cybercrime that may have compromised sensitive customer data. What should be The FIRST course of action?

A. Invoke the incident response plan.

B. Determine the business impact.
C. Conduct a forensic investigation.
D. Invoke the business continuity plan (BCP).

Answer: A

NEW QUESTION 547
- (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

Answer: B

NEW QUESTION 549
- (Exam Topic 2)
Which of the following will BEST help to ensure that information system controls are effective?

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

Answer: C

NEW QUESTION 551
- (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.

Answer: B

NEW QUESTION 552
- (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

Answer: B

NEW QUESTION 556
- (Exam Topic 2)
An internally developed payroll application leverages Platform as a Service (PaaS) infrastructure from the cloud. Who owns the related data confidentiality risk?

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

Answer: B

NEW QUESTION 559
- (Exam Topic 2)
Which of the following is the MOST important objective of embedding risk management practices into the initiation phase of the project management life cycle?

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

Answer: B

NEW QUESTION 564
- (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.

Answer: C

NEW QUESTION 569
- (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

Answer: D

NEW QUESTION 574
- (Exam Topic 2)
Which of the following would MOST likely cause a risk practitioner to reassess risk scenarios?

A. A change in the risk management policy
B. A major security incident
C. A change in the regulatory environment
D. An increase in intrusion attempts

Answer: C

NEW QUESTION 578
- (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

Answer: A

NEW QUESTION 579
- (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 583
- (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

Answer: C

NEW QUESTION 588
- (Exam Topic 2)
An organization operates in a jurisdiction where heavy fines are imposed for leakage of customer data. Which of the following provides the BEST input to assess the inherent risk impact?

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

Answer: B

NEW QUESTION 589
- (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

Answer: B

NEW QUESTION 591
- (Exam Topic 2)
To mitigate the risk of using a spreadsheet to analyze financial data, IT has engaged a third-party vendor to deploy a standard application to automate the process. Which of the following parties should own the risk associated with calculation errors?

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

Answer: A

NEW QUESTION 596
- (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 598
- (Exam Topic 2)
IT disaster recovery point objectives (RPOs) should be based on the:

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

Answer: C

NEW QUESTION 603
- (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

Answer: A

NEW QUESTION 606
- (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.

Answer: B

NEW QUESTION 610
- (Exam Topic 2)
A large organization needs to report risk at all levels for a new centralized visualization project to reduce cost and improve performance. Which of the following would MOST effectively represent the overall risk of the project to senior management?

A. Aggregated key performance indicators (KPIs)
B. Key risk indicators (KRIs)
C. Centralized risk register

D. Risk heat map

Answer: D

NEW QUESTION 614
- (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

Answer: D

NEW QUESTION 615
- (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.

Answer: A

NEW QUESTION 619
- (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.

Answer: B

NEW QUESTION 623
- (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.

Answer: C

NEW QUESTION 624
- (Exam Topic 2)
Who is responsible for IT security controls that are outsourced to an external service provider?

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

Answer: B

NEW QUESTION 628
- (Exam Topic 2)
A risk assessment has identified increased losses associated with an IT risk scenario. It is MOST important for the risk practitioner to:

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

Answer: A

NEW QUESTION 632
- (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)

Answer: C

NEW QUESTION 636
- (Exam Topic 2)
An organization has recently updated its disaster recovery plan (DRP). Which of the following would be the GREATEST risk if the new plan is not tested?

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

Answer: D

NEW QUESTION 637
- (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 (KPIs)

Answer: B

NEW QUESTION 642
- (Exam Topic 2)
Which of the following is MOST important for a risk practitioner to ensure once a risk action plan has been completed?

A. The risk owner has validated outcomes.
B. The risk register has been updated.
C. The control objectives are mapped to risk objectives.
D. The requirements have been achieved.

Answer: B

NEW QUESTION 643
- (Exam Topic 2)
An organization plans to migrate sensitive information to a public cloud infrastructure. Which of the following is the GREATEST security risk in this scenario?

A. Data may be commingled with other tenants' data.
B. System downtime does not meet the organization's thresholds.
C. The infrastructure will be managed by the public cloud administrator.
D. The cloud provider is not independently certified.

Answer: A

NEW QUESTION 648
- (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)

Answer: B

NEW QUESTION 653
- (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

Answer: B

NEW QUESTION 655
- (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

Answer: B

NEW QUESTION 660
- (Exam Topic 2)
A key risk indicator (KRI) indicates a reduction in the percentage of appropriately patched servers. Which of the following is the risk practitioner's BEST course of action?

A. Determine changes in the risk level.
B. Outsource the vulnerability management process.
C. Review the patch management process.
D. Add agenda item to the next risk committee meeting.

Answer: C

NEW QUESTION 661
- (Exam Topic 2)
Read" rights to application files in a controlled server environment should be approved by the:

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

Answer: A

NEW QUESTION 662
- (Exam Topic 2)
The GREATEST concern when maintaining a risk register is that:

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

Answer: D

NEW QUESTION 665
- (Exam Topic 2)
Which of the following BEST enables a proactive approach to minimizing the potential impact of unauthorized data disclosure?

A. Cyber insurance
B. Data backups
C. Incident response plan
D. Key risk indicators (KRIs)

Answer: D

NEW QUESTION 666
- (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

Answer: A

NEW QUESTION 669
- (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.

Answer: D

NEW QUESTION 673
- (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.

Answer: A

NEW QUESTION 676
- (Exam Topic 2)
Which of the following BEST measures the efficiency of an incident response process?

A. Number of incidents escalated to management
B. Average time between changes and updating of escalation matrix
C. Average gap between actual and agreed response times
D. Number of incidents lacking responses

Answer: C

NEW QUESTION 680
- (Exam Topic 2)
Which of the following is MOST helpful in determining the effectiveness of an organization's IT risk mitigation efforts?

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

Answer: D

NEW QUESTION 683
- (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.

Answer: D

NEW QUESTION 686
- (Exam Topic 2)
An upward trend in which of the following metrics should be of MOST concern?

A. Number of business change management requests
B. Number of revisions to security policy
C. Number of security policy exceptions approved
D. Number of changes to firewall rules

Answer: C

NEW QUESTION 691
- (Exam Topic 2)
Which of the following BEST indicates effective information security incident management?

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

Answer: C

NEW QUESTION 694
- (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.

Answer:

D

NEW QUESTION 696
- (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 699
- (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.

Answer: B

NEW QUESTION 700
- (Exam Topic 2)
An organization has decided to outsource a web application, and customer data will be stored in the vendor's public cloud. To protect customer data, it is MOST important to ensure which of the following?

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

Answer: D

NEW QUESTION 701
- (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

Answer: D

NEW QUESTION 705
- (Exam Topic 2)
Which of the following can be used to assign a monetary value to risk?

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

Answer: A

NEW QUESTION 710
- (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

Answer: B

NEW QUESTION 715
- (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.

Answer: D

NEW QUESTION 716
- (Exam Topic 2)
IT stakeholders have asked a risk practitioner for IT risk profile reports associated with specific departments to allocate resources for risk mitigation. The BEST way to address this request would be to use:

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

Answer: D

NEW QUESTION 718
- (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 721
- (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 723
- (Exam Topic 3)
Which of the following is the GREATEST benefit for an organization with a strong risk awareness culture?

A. Reducing the involvement by senior management
B. Using more risk specialists
C. Reducing the need for risk policies and guidelines
D. Discussing and managing risk as a team

Answer: D

NEW QUESTION 727
- (Exam Topic 3)
An organization outsources the processing of us payroll data A risk practitioner identifies a control weakness at the third party trial exposes the payroll data. Who should own this risk?

A. The third party's IT operations manager
B. The organization's process owner
C. The third party's chief risk officer (CRO)
D. The organization's risk practitioner

Answer: B

NEW QUESTION 728
- (Exam Topic 3)
Which of the following is the PRIMARY benefit of stakeholder involvement in risk scenario development?

A. Ability to determine business impact

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

Answer: A

NEW QUESTION 733
- (Exam Topic 3)
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.

Answer: B

NEW QUESTION 737
- (Exam Topic 3)
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.

Answer: B

NEW QUESTION 741
- (Exam Topic 3)
An organization is conducting a review of emerging risk. Which of the following is the BEST input for this exercise?

A. Audit reports
B. Industry benchmarks
C. Financial forecasts
D. Annual threat reports

Answer: B

NEW QUESTION 743
- (Exam Topic 3)
Analyzing trends in key control indicators (KCIs) BEST enables a risk practitioner to proactively identify impacts on an organization's:

A. risk classification methods
B. risk-based capital allocation
C. risk portfolio
D. risk culture

Answer: C

NEW QUESTION 747
- (Exam Topic 3)
The MOST important reason for implementing change control procedures is to ensure:

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

Answer: A

NEW QUESTION 752
- (Exam Topic 3)
Which of the following approaches BEST identifies information systems control deficiencies?

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

Answer: C

NEW QUESTION 753
- (Exam Topic 3)
A company has recently acquired a customer relationship management (CRM) application from a certified software vendor. Which of the following will BE ST help

lo prevent technical vulnerabilities from being exploded?

A. implement code reviews and Quality assurance on a regular basis
B. Verity me software agreement indemnifies the company from losses
C. Review the source coda and error reporting of the application
D. Update the software with the latest patches and updates

Answer: D

NEW QUESTION 754
- (Exam Topic 3)
A risk practitioner has collaborated with subject matter experts from the IT department to develop a large list of potential key risk indicators (KRIs) for all IT operations within the organization Of the following, who should review the completed list and select the appropriate KRIs for implementation?

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

Answer: D

NEW QUESTION 755
- (Exam Topic 3)
A recent risk workshop has identified risk owners and responses for newly identified risk scenarios. Which of the following should be the risk practitioner's NEXT step?

A. Develop a mechanism for monitoring residual risk.
B. Update the risk register with the results.
C. Prepare a business case for the response options.
D. Identify resources for implementing responses.

Answer: C

NEW QUESTION 760
- (Exam Topic 3)
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.

Answer: B

NEW QUESTION 764
- (Exam Topic 3)
Which of the following is the MOST important consideration for protecting data assets m a Business application system?

A. Application controls are aligned with data classification lutes
B. Application users are periodically trained on proper data handling practices
C. Encrypted communication is established between applications and data servers
D. Offsite encrypted backups are automatically created by the application

Answer: A

NEW QUESTION 767
- (Exam Topic 3)
An organization is planning to move its application infrastructure from on-premises to the cloud. Which of the following is the BEST course of the actin to address the risk associated with data transfer if the relationship is terminated with the vendor?

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

Answer: B

NEW QUESTION 768
- (Exam Topic 3)
The PRIMARY objective of collecting information and reviewing documentation when performing periodic risk analysis should be to:

A. Identify new or emerging risk issues.
B. Satisfy audit requirements.
C. Survey and analyze historical risk data.
D. Understand internal and external threat agents.

Answer: D

NEW QUESTION 772
- (Exam Topic 3)
An organization has decided to commit to a business activity with the knowledge that the risk exposure is higher than the risk appetite. Which of the following is the risk practitioner's MOST important action related to this decision?

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

Answer: C

NEW QUESTION 773
- (Exam Topic 3)
A cote data center went offline abruptly for several hours affecting many transactions across multiple locations. Which of the to" owing would provide the MOST useful information to determine mitigating controls?

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

Answer: A

NEW QUESTION 778
- (Exam Topic 3)
Which of the following BEST enables risk-based decision making in support of a business continuity plan (BCP)?

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

Answer: A

NEW QUESTION 783
- (Exam Topic 3)
Which of the following BEST mitigates the risk of sensitive personal data leakage from a software development environment?

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

Answer: C

NEW QUESTION 788
- (Exam Topic 3)
Senior management has asked the risk practitioner for the overall residual risk level for a process that contains numerous risk scenarios. Which of the following should be provided?

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

Answer: D

NEW QUESTION 793
- (Exam Topic 3)
Several newly identified risk scenarios are being integrated into an organization's risk register. The MOST appropriate risk owner would be the individual who:

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

Answer: C

NEW QUESTION 798
- (Exam Topic 3)
Of the following, who is BEST suited to assist a risk practitioner in developing a relevant set of risk scenarios?

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

D. Control owner

Answer: B

NEW QUESTION 801
- (Exam Topic 3)
Which of the following BEST protects an organization against breaches when using a software as a service (SaaS) application?

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

Answer: B

NEW QUESTION 803
- (Exam Topic 3)
Which of the following is the GREATEST benefit of identifying appropriate risk owners?

A. Accountability is established for risk treatment decisions
B. Stakeholders are consulted about risk treatment options
C. Risk owners are informed of risk treatment options
D. Responsibility is established for risk treatment decisions.

Answer: A

NEW QUESTION 806
- (Exam Topic 3)
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.

Answer: C

NEW QUESTION 810
- (Exam Topic 2)
An organization is making significant changes to an application. At what point should the application risk profile be updated?

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

Answer: D

NEW QUESTION 813
- (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

Answer: B

NEW QUESTION 815
- (Exam Topic 2)
Which of the following is MOST effective in continuous risk management process improvement?

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

Answer: A

NEW QUESTION 816
- (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

Answer: D

NEW QUESTION 820
- (Exam Topic 2)
An IT risk practitioner is evaluating an organization's change management controls over the last six months. The GREATEST concern would be an increase in:

A. rolled back changes below management's thresholds.
B. change-related exceptions per month.
C. the average implementation time for changes.
D. number of user stories approved for implementation.

Answer: B

NEW QUESTION 822
- (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 826
- (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 828
- (Exam Topic 2)
After migrating a key financial system to a new provider, it was discovered that a developer could gain access to the production environment. Which of the following is the BEST way to mitigate the risk in this situation?

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

Answer: B

NEW QUESTION 832
- (Exam Topic 2)
Which of the following should be the PRIMARY recipient of reports showing the progress of a current IT risk mitigation project?

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

Answer: A

NEW QUESTION 836
- (Exam Topic 2)
The FIRST task when developing a business continuity plan should be to:

A. determine data backup and recovery availability at an alternate site.
B. identify critical business functions and resources.
C. define roles and responsibilities for implementation.
D. identify recovery time objectives (RTOs) for critical business applications.

Answer: B

NEW QUESTION 841

- (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

Answer: D

NEW QUESTION 842
- (Exam Topic 2)
Which of the following is MOST important to review when determining whether a potential IT service provider's control environment is effective?

A. Independent audit report
B. Control self-assessment
C. MOST important to update when an
D. Service level agreements (SLAs)

Answer: A

NEW QUESTION 847
- (Exam Topic 2)
An external security audit has reported multiple findings related to control noncompliance. Which of the following would be MOST important for the risk practitioner to communicate to senior management?

A. A recommendation for internal audit validation
B. Plans for mitigating the associated risk
C. Suggestions for improving risk awareness training
D. The impact to the organization's risk profile

Answer: D

NEW QUESTION 850
- (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

Answer: A

NEW QUESTION 853
- (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

Answer: D

NEW QUESTION 854
- (Exam Topic 2)
An organization has completed a project to implement encryption on all databases that host customer data. Which of the following elements of the risk register should be updated the reflect this change?

A. Risk likelihood
B. Inherent risk
C. Risk appetite
D. Risk tolerance

Answer: B

NEW QUESTION 856
- (Exam Topic 2)
Which of the following would BEST enable a risk practitioner to embed risk management within the organization?

A. Provide risk management feedback to key stakeholders.
B. Collect and analyze risk data for report generation.
C. Monitor and prioritize risk data according to the heat map.
D. Engage key stakeholders in risk management practices.

Answer: D

NEW QUESTION 859
- (Exam Topic 2)
An organization is considering adopting artificial intelligence (AI). Which of the following is the risk practitioner's MOST important course of action?

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

Answer: C

NEW QUESTION 862
- (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

Answer: A

NEW QUESTION 864
- (Exam Topic 2)
Which of the following is MOST important to ensure when continuously monitoring the performance of a client-facing application?

A. Objectives are confirmed with the business owne
B. Control owners approve control changes.
C. End-user acceptance testing has been conducte
D. Performance information in the log is encrypte

Answer: D

NEW QUESTION 865
- (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

Answer: D

NEW QUESTION 867
- (Exam Topic 2)
Which of the following would be a weakness in procedures for controlling the migration of changes to production libraries?

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

Answer: A

NEW QUESTION 872
- (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

Answer: B

NEW QUESTION 876
- (Exam Topic 1)
Which of the following should be the HIGHEST priority when developing a risk response?

A. The risk response addresses the risk with a holistic view.
B. The risk response is based on a cost-benefit analysis.

C. The risk response is accounted for in the budget.
D. The risk response aligns with the organization's risk appetite.

Answer: D

NEW QUESTION 878
- (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 882
- (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 885
- (Exam Topic 1)
The MOST important characteristic of an organization s policies is to reflect the organization's:

A. risk assessment methodology.
B. risk appetite.
C. capabilities
D. asset value.

Answer: B

NEW QUESTION 887
- (Exam Topic 1)
Which of the following would be the BEST recommendation if the level of risk in the IT risk profile has decreased and is now below management's risk appetite?

A. Optimize the control environment.
B. Realign risk appetite to the current risk level.
C. Decrease the number of related risk scenarios.
D. Reduce the risk management budget.

Answer: A

NEW QUESTION 891
- (Exam Topic 1)
Which of the following is the BEST way to validate the results of a vulnerability assessment?

A. Perform a penetration test.
B. Review security logs.
C. Conduct a threat analysis.
D. Perform a root cause analysis.

Answer: A

NEW QUESTION 893
- (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 898
- (Exam Topic 1)
A key risk indicator (KRI) is reported to senior management on a periodic basis as exceeding thresholds, but each time senior management has decided to take no

action to reduce the risk. Which of the following is the MOST likely reason for senior management's response?

A. The underlying data source for the KRI is using inaccurate data and needs to be corrected.
B. The KRI is not providing useful information and should be removed from the KRI inventory.
C. The KRI threshold needs to be revised to better align with the organization s risk appetite
D. Senior management does not understand the KRI and should undergo risk training.

Answer: C

NEW QUESTION 903
- (Exam Topic 1)
Reviewing results from which of the following is the BEST way to identify information systems control deficiencies?

A. Vulnerability and threat analysis
B. Control remediation planning
C. User acceptance testing (UAT)
D. Control self-assessment (CSA)

Answer: D

NEW QUESTION 907
- (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 912
- (Exam Topic 1)
Whether the results of risk analyses should be presented in quantitative or qualitative terms should be based PRIMARILY on the:

A. requirements of management.
B. specific risk analysis framework being used.
C. organizational risk tolerance
D. results of the risk assessment.

Answer: A

NEW QUESTION 915
- (Exam Topic 1)
The PRIMARY objective of testing the effectiveness of a new control before implementation is to:

A. ensure that risk is mitigated by the control.
B. measure efficiency of the control process.
C. confirm control alignment with business objectives.
D. comply with the organization's policy.

Answer: C

NEW QUESTION 919
- (Exam Topic 1)
In addition to the risk register, what should a risk practitioner review to develop an understanding of the organization's risk profile?

A. The control catalog
B. The asset profile
C. Business objectives
D. Key risk indicators (KRIs)

Answer: C

NEW QUESTION 921
- (Exam Topic 1)
Which of the following is the MOST important requirement for monitoring key risk indicators (KRIs) using log analysis?

A. Obtaining logs m an easily readable format
B. Providing accurate logs m a timely manner
C. Collecting logs from the entire set of IT systems
D. implementing an automated log analysis tool

Answer: B

NEW QUESTION 922

- (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 926
.....

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