Isaca

Exam Questions CRISC

Certified in Risk and Information Systems Control

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1
- (Exam Topic 4)
What is the MAIN benefit of using a top-down approach to develop risk scenarios?

A. It describes risk events specific to technology used by the enterprise.
B. It establishes the relationship between risk events and organizational objectives.
C. It uses hypothetical and generic risk events specific to the enterprise.
D. It helps management and the risk practitioner to refine risk scenarios.

Answer: C

NEW QUESTION 2
- (Exam Topic 4)
When classifying and prioritizing risk responses, the areas to address FIRST are those with:

A. low cost effectiveness ratios and high risk levels
B. high cost effectiveness ratios and low risk levels.
C. high cost effectiveness ratios and high risk levels
D. low cost effectiveness ratios and low risk levels.

Answer: C

NEW QUESTION 3
- (Exam Topic 4)
Which of the following should be the GREATEST concern to a risk practitioner when process documentation is incomplete?

A. Inability to allocate resources efficiently
B. Inability to identify the risk owner
C. Inability to complete the risk register
D. Inability to identify process experts

Answer: B

NEW QUESTION 4
- (Exam Topic 4)
A failed IT system upgrade project has resulted in the corruption of an organization's asset inventory database. Which of the following controls BEST mitigates the impact of this incident?

A. Encryption
B. Authentication
C. Configuration
D. Backups

Answer: D

NEW QUESTION 5
- (Exam Topic 4)
A highly regulated enterprise is developing a new risk management plan to specifically address legal and regulatory risk scenarios What should be done FIRST by IT governance to support this effort?

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

Answer: A

NEW QUESTION 6
- (Exam Topic 4)
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 7
- (Exam Topic 4)
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 8
- (Exam Topic 4)
Which of the following is the BEST way to ensure data is properly sanitized while in cloud storage?

A. Deleting the data from the file system
B. Cryptographically scrambling the data
C. Formatting the cloud storage at the block level
D. Degaussing the cloud storage media

Answer: B

NEW QUESTION 9
- (Exam Topic 4)
Which of the following is the MOST important information to cover a business continuity awareness Ira nine, program for all employees of the organization?

A. Recovery time objectives (RTOs)
B. Segregation of duties
C. Communication plan
D. Critical asset inventory

Answer: C

NEW QUESTION 10
- (Exam Topic 4)
A poster has been displayed in a data center that reads. "Anyone caught taking photographs in the data center may be subject to disciplinary action." Which of the following control types has been implemented?

A. Corrective
B. Detective
C. Deterrent
D. Preventative

Answer: A

NEW QUESTION 10
- (Exam Topic 4)
Risk appetite should be PRIMARILY driven by which of the following?

A. Enterprise security architecture roadmap
B. Stakeholder requirements
C. Legal and regulatory requirements
D. Business impact analysis (BIA)

Answer: B

NEW QUESTION 12
- (Exam Topic 4)
Which of the following key performance indicators (KPis) would BEST measure me risk of a service outage when using a Software as a Service (SaaS) vendors

A. Frequency of business continuity plan (BCP) lasting
B. Frequency and number of new software releases
C. Frequency and duration of unplanned downtime
D. Number of IT support staff available after business hours

Answer: C

NEW QUESTION 14
- (Exam Topic 4)
An organization has recently hired a large number of part-time employees. During the annual audit, it was discovered that many user IDs and passwords were documented in procedure manuals for use by the part-time employees. Which of the following BEST describes this situation?

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

Answer: B

NEW QUESTION 17

- (Exam Topic 4)
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 19
- (Exam Topic 4)
Which of the following should be of MOST concern to a risk practitioner reviewing an organization risk register after the completion of a series of risk assessments?

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

Answer: A

NEW QUESTION 22
- (Exam Topic 4)
Which of the following would be of MOST concern to a risk practitioner reviewing risk action plans for documented IT risk scenarios?

A. Individuals outside IT are managing action plans for the risk scenarios.
B. Target dates for completion are missing from some action plans.
C. Senior management approved multiple changes to several action plans.
D. Many action plans were discontinued after senior management accepted the risk.

Answer: B

NEW QUESTION 23
- (Exam Topic 4)
A risk practitioner notices a risk scenario associated with data loss at the organization's cloud provider is assigned to the provider Who should the risk scenario be reassigned to?

A. Senior management
B. Chief risk officer (CRO)
C. Vendor manager
D. Data owner

Answer: D

NEW QUESTION 25
- (Exam Topic 4)
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 27
- (Exam Topic 4)
Which of the following is PRIMARILY a risk management responsibly of the first line of defense?

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

Answer: C

NEW QUESTION 31
- (Exam Topic 4)
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 34
- (Exam Topic 4)
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 35
- (Exam Topic 4)
When establishing an enterprise IT risk management program, it is MOST important to:

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

Answer: D

NEW QUESTION 39
- (Exam Topic 4)
An organization uses one centralized single sign-on (SSO) control to cover many applications. Which of the following is the BEST course of action when a new application is added to the environment after testing of the SSO control has been completed?

A. Initiate a retest of the full control
B. Retest the control using the new application as the only sample.
C. Review the corresponding change control documentation
D. Re-evaluate the control during (he next assessment

Answer: A

NEW QUESTION 40
- (Exam Topic 4)
Which of the following is the PRIMARY reason for a risk practitioner to review an organization's IT asset inventory?

A. To plan for the replacement of assets at the end of their life cycles
B. To assess requirements for reducing duplicate assets
C. To understand vulnerabilities associated with the use of the assets
D. To calculate mean time between failures (MTBF) for the assets

Answer: C

NEW QUESTION 42
- (Exam Topic 4)
What is senior management's role in the RACI model when tasked with reviewing monthly status reports provided by risk owners?

A. Accountable
B. Informed
C. Responsible
D. Consulted

Answer: B

NEW QUESTION 46
- (Exam Topic 4)
Which of the following is the MOST effective way to help ensure accountability for managing risk?

A. Assign process owners to key risk areas.
B. Obtain independent risk assessments.
C. Assign incident response action plan responsibilities.
D. Create accurate process narratives.

Answer: A

NEW QUESTION 48
- (Exam Topic 4)
A risk practitioner has identified that the agreed recovery time objective (RTO) with a Software as a Service (SaaS) provider is longer than the business expectation. Which of the following is the risk practitioner's BEST course of action?

A. Collaborate with the risk owner to determine the risk response plan.
B. Document the gap in the risk register and report to senior management.
C. Include a right to audit clause in the service provider contract.
D. Advise the risk owner to accept the risk.

Answer: C

NEW QUESTION 50
- (Exam Topic 4)
Which of the following would BEST enable a risk-based decision when considering the use of an emerging technology for data processing?

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

Answer: A

NEW QUESTION 55
- (Exam Topic 4)
An organization has asked an IT risk practitioner to conduct an operational risk assessment on an initiative to outsource the organization's customer service operations overseas. Which of the following would MOST significantly impact management's decision?

A. Time zone difference of the outsourcing location
B. Ongoing financial viability of the outsourcing company
C. Cross-border information transfer restrictions in the outsourcing country
D. Historical network latency between the organization and outsourcing location

Answer: C

NEW QUESTION 56
- (Exam Topic 4)
Which of the following is the MOST important consideration when developing risk strategies?

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

Answer: B

NEW QUESTION 59
- (Exam Topic 4)
A MAJOR advantage of using key risk indicators (KRis) is that (hey

A. identify when risk exceeds defined thresholds
B. assess risk scenarios that exceed defined thresholds
C. identify scenarios that exceed defined risk appetite
D. help with internal control assessments concerning risk appellate

Answer: B

NEW QUESTION 63
- (Exam Topic 4)
Which of the following provides the BEST assurance of the effectiveness of vendor security controls?

A. Review vendor control self-assessments (CSA).
B. Review vendor service level agreement (SLA) metrics.
C. Require independent control assessments.
D. Obtain vendor references from existing customers.

Answer: C

NEW QUESTION 64
- (Exam Topic 4)
Which of the following would MOST likely cause management to unknowingly accept excessive risk?

A. Satisfactory audit results
B. Risk tolerance being set too low
C. Inaccurate risk ratings
D. Lack of preventive controls

Answer: C

NEW QUESTION 65

- (Exam Topic 4)
Which of the following is MOST important to consider before determining a response to a vulnerability?

A. The likelihood and impact of threat events
B. The cost to implement the risk response
C. Lack of data to measure threat events
D. Monetary value of the asset

Answer: C

NEW QUESTION 70
- (Exam Topic 4)
Which of the following resources is MOST helpful to a risk practitioner when updating the likelihood rating in the risk register?

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

Answer: D

NEW QUESTION 75
- (Exam Topic 3)
Which of the following statements describes the relationship between key risk indicators (KRIs) and key control indicators (KCIs)?

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

Answer: A

NEW QUESTION 77
- (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: D

NEW QUESTION 79
- (Exam Topic 3)
Which of the following is the BEST way to determine the potential organizational impact of emerging privacy regulations?

A. Evaluate the security architecture maturity.
B. Map the new requirements to the existing control framework.
C. Charter a privacy steering committee.
D. Conduct a privacy impact assessment (PIA).

Answer: D

NEW QUESTION 83
- (Exam Topic 3)
During a risk treatment plan review, a risk practitioner finds the approved risk action plan has not been completed However, there were other risk mitigation actions implemented. Which of the fallowing is the BEST course of action?

A. Review the cost-benefit of mitigating controls
B. Mark the risk status as unresolved within the risk register
C. Verify the sufficiency of mitigating controls with the risk owner
D. Update the risk register with implemented mitigating actions

Answer: A

NEW QUESTION 88
- (Exam Topic 3)
Winch of the following can be concluded by analyzing the latest vulnerability report for the it infrastructure?

A. Likelihood of a threat
B. Impact of technology risk
C. Impact of operational risk
D. Control weakness

Answer: C

NEW QUESTION 90
- (Exam Topic 3)
Which type of indicators should be developed to measure the effectiveness of an organization's firewall rule set?

A. Key risk indicators (KRIs)
B. Key management indicators (KMIs)
C. Key performance indicators (KPIs)
D. Key control indicators (KCIs)

Answer: D

NEW QUESTION 91
- (Exam Topic 3)
Which of the following is MOST important to include in a risk assessment of an emerging technology?

A. Risk response plans
B. Risk and control ownership
C. Key controls
D. Impact and likelihood ratings

Answer: D

NEW QUESTION 94
- (Exam Topic 3)
When reviewing a report on the performance of control processes, it is MOST important to verify whether the:

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

Answer: D

NEW QUESTION 95
- (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 98
- (Exam Topic 3)
Which of the following is the BEST method for assessing control effectiveness against technical vulnerabilities that could be exploited to compromise an information system?

A. Vulnerability scanning
B. Systems log correlation analysis
C. Penetration testing
D. Monitoring of intrusion detection system (IDS) alerts

Answer: C

NEW QUESTION 99
- (Exam Topic 3)
Which of the following is the BEST indicator of the effectiveness of IT risk management processes?

A. Percentage of business users completing risk training
B. Percentage of high-risk scenarios for which risk action plans have been developed
C. Number of key risk indicators (KRIs) defined
D. Time between when IT risk scenarios are identified and the enterprise's response

Answer: B

NEW QUESTION 100
- (Exam Topic 3)
Which of the following will help ensure the elective decision-making of an IT risk management committee?

A. Key stakeholders are enrolled as members
B. Approved minutes ate forwarded to senior management
C. Committee meets at least quarterly
D. Functional overlap across the business is minimized

Answer:

D

NEW QUESTION 102
- (Exam Topic 3)
The PRIMARY purpose of using a framework for risk analysis is to:

A. improve accountability
B. improve consistency
C. help define risk tolerance
D. help develop risk scenarios.

Answer: B

NEW QUESTION 103
- (Exam Topic 3)
An organization has detected unauthorized logins to its client database servers. Which of the following should be of GREATEST concern?

A. Potential increase in regulatory scrutiny
B. Potential system downtime
C. Potential theft of personal information
D. Potential legal risk

Answer: C

NEW QUESTION 108
- (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 113
- (Exam Topic 3)
Which of the following is an IT business owner's BEST course of action following an unexpected increase in emergency changes?

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

Answer: B

NEW QUESTION 116
- (Exam Topic 3)
Which of the following should be an element of the risk appetite of an organization?

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

Answer: B

NEW QUESTION 121
- (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 126
- (Exam Topic 3)
A service provider is managing a client’s servers. During an audit of the service, a noncompliant control is discovered that will not be resolved before the next audit because the client cannot afford the downtime required to correct the issue. The service provider’s MOST appropriate action would be to:

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

D. ask the client to document the formal risk acceptance for the provider

Answer: D

NEW QUESTION 131
- (Exam Topic 3)
An organizations chief technology officer (CTO) has decided to accept the risk associated with the potential loss from a denial-of-service (DoS) attack. In this situation, the risk practitioner's BEST course of action is to:

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

Answer: A

NEW QUESTION 132
- (Exam Topic 3)
An IT department has provided a shared drive for personnel to store information to which all employees have access. Which of the following parties is accountable for the risk of potential loss of confidential information?

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

Answer: D

NEW QUESTION 134
- (Exam Topic 3)
Which of the following is the MOST important technology control to reduce the likelihood of fraudulent payments committed internally?

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

Answer: B

NEW QUESTION 139
- (Exam Topic 3)
Which of the following is the BEST recommendation to senior management when the results of a risk and control assessment indicate a risk scenario can only be partially mitigated?

A. Implement controls to bring the risk to a level within appetite and accept the residual risk.
B. Implement a key performance indicator (KPI) to monitor the existing control performance.
C. Accept the residual risk in its entirety and obtain executive management approval.
D. Separate the risk into multiple components and avoid the risk components that cannot be mitigated.

Answer: C

NEW QUESTION 141
- (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 143
- (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 144
- (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 145
- (Exam Topic 3)
Which of the following is MOST important for an organization to update following a change in legislation requiring notification to individuals impacted by data breaches?

A. Insurance coverage
B. Security awareness training
C. Policies and standards
D. Risk appetite and tolerance

Answer: C

NEW QUESTION 149
- (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 151
- (Exam Topic 3)
Which of the following statements BEST illustrates the relationship between key performance indicators (KPIs) and key control indicators (KCIs)?

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

Answer: B

NEW QUESTION 155
- (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 157
- (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 162
- (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 164
- (Exam Topic 3)
A risk practitioner has been asked to advise management on developing a log collection and correlation strategy. Which of the following should be the MOST important consideration when developing this strategy?

A. Ensuring time synchronization of log sources.
B. Ensuring the inclusion of external threat intelligence log sources.
C. Ensuring the inclusion of all computing resources as log sources.
D. Ensuring read-write access to all log sources

Answer: A

NEW QUESTION 167
- (Exam Topic 3)
Which of the following should be included in a risk scenario to be used for risk analysis?

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

Answer: B

NEW QUESTION 169
- (Exam Topic 3)
Which of the following scenarios represents a threat?

A. Connecting a laptop to a free, open, wireless access point (hotspot)
B. Visitors not signing in as per policy
C. Storing corporate data in unencrypted form on a laptop
D. A virus transmitted on a USB thumb drive

Answer: D

NEW QUESTION 174
- (Exam Topic 3)
The PRIMARY reason to have risk owners assigned to entries in the risk register is to ensure:

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

Answer: A

NEW QUESTION 179
- (Exam Topic 3)
The PRIMARY benefit of conducting continuous monitoring of access controls is the ability to identify:

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

Answer: B

NEW QUESTION 182
- (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 184
- (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 188
- (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 190
- (Exam Topic 3)
Which of the following is the MOST important objective of an enterprise risk management (ERM) program?

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

Answer: B

NEW QUESTION 193
- (Exam Topic 3)
Which of the following provides the MOST useful information when determining if a specific control should be implemented?

A. Business impact analysis (BIA)
B. Cost-benefit analysis
C. Attribute analysis
D. Root cause analysis

Answer: B

NEW QUESTION 197
- (Exam Topic 3)
Which of the following roles is BEST suited to help a risk practitioner understand the impact of IT-related events on business objectives?

A. IT management
B. Internal audit
C. Process owners
D. Senior management

Answer: C

NEW QUESTION 200
- (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: D

NEW QUESTION 202
- (Exam Topic 3)
A risk manager has determined there is excessive risk with a particular technology. Who is the BEST person to own the unmitigated risk of the technology?

A. IT system owner
B. Chief financial officer
C. Chief risk officer
D. Business process owner

Answer: D

NEW QUESTION 204
- (Exam Topic 3)
Which of The following is the BEST way to confirm whether appropriate automated controls are in place within a recently implemented system?

A. Perform a post-implementation review.
B. Conduct user acceptance testing.

C. Review the key performance indicators (KPIs).
D. Interview process owners.

Answer: C

NEW QUESTION 208
- (Exam Topic 3)
The PRIMARY goal of conducting a business impact analysis (BIA) as part of an overall continuity planning process is to:

A. obtain the support of executive management.
B. map the business processes to supporting IT and other corporate resources.
C. identify critical business processes and the degree of reliance on support services.
D. document the disaster recovery process.

Answer: C

NEW QUESTION 213
- (Exam Topic 3)
An organization is preparing to transfer a large number of customer service representatives to the sales department. Of the following, who is responsible for mitigating the risk associated with residual system access?

A. IT service desk manager
B. Sales manager
C. Customer service manager
D. Access control manager

Answer: D

NEW QUESTION 217
- (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 218
- (Exam Topic 3)
The risk associated with an asset after controls are applied can be expressed as:

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

Answer: C

NEW QUESTION 220
- (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 224
- (Exam Topic 3)
Which of the following practices MOST effectively safeguards the processing of personal data?

A. Personal data attributed to a specific data subject is tokenized.
B. Data protection impact assessments are performed on a regular basis.
C. Personal data certifications are performed to prevent excessive data collection.
D. Data retention guidelines are documented, established, and enforced.

Answer: B

NEW QUESTION 229
- (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 233
- (Exam Topic 3)
Key risk indicators (KRIs) are MOST useful during which of the following risk management phases?

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

Answer: A

NEW QUESTION 234
- (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 237
- (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 239
- (Exam Topic 3)
Which of the following is MOST important when considering risk in an enterprise risk management (ERM) process?

A. Financial risk is given a higher priority.
B. Risk with strategic impact is included.
C. Security strategy is given a higher priority.
D. Risk identified by industry benchmarking is included.

Answer: B

NEW QUESTION 242
- (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 247
- (Exam Topic 3)
Legal and regulatory risk associated with business conducted over the Internet is driven by:

A. the jurisdiction in which an organization has its principal headquarters
B. international law and a uniform set of regulations.
C. the laws and regulations of each individual country
D. international standard-setting bodies.

Answer: C

NEW QUESTION 252
- (Exam Topic 3)

Winch of the following is the BEST evidence of an effective risk treatment plan?

A. The inherent risk is below the asset residual risk.
B. Remediation cost is below the asset business value
C. The risk tolerance threshold s above the asset residual
D. Remediation is completed within the asset recovery time objective (RTO)

Answer: B

NEW QUESTION 257
- (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 259
- (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 260
- (Exam Topic 3)
Which of the following BEST indicates the risk appetite and tolerance level (or the risk associated with business interruption caused by IT system failures?

A. Mean time to recover (MTTR)
B. IT system criticality classification
C. Incident management service level agreement (SLA)
D. Recovery time objective (RTO)

Answer: D

NEW QUESTION 264
- (Exam Topic 3)
An organization moved its payroll system to a Software as a Service (SaaS) application. A new data privacy regulation stipulates that data can only be processed within the country where it is collected. Which of the following should be done FIRST when addressing this situation?

A. Analyze data protection methods.
B. Understand data flows.
C. Include a right-to-audit clause.
D. Implement strong access controls.

Answer: B

NEW QUESTION 267
- (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 272
- (Exam Topic 3)
Which of the following data would be used when performing a business impact analysis (BIA)?

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

Answer: D

NEW QUESTION 276
- (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 280
- (Exam Topic 3)
The PRIMARY advantage of involving end users in continuity planning is that they:

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

Answer: B

NEW QUESTION 281
- (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 286
- (Exam Topic 3)
In an organization dependent on data analytics to drive decision-making, which of the following would BEST help to minimize the risk associated with inaccurate data?

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

Answer: B

NEW QUESTION 289
- (Exam Topic 3)
Who should be accountable for monitoring the control environment to ensure controls are effective?

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

Answer: A

NEW QUESTION 293
- (Exam Topic 3)
Which of the following is the PRIMARY objective of providing an aggregated view of IT risk to business management?

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

Answer: B

NEW QUESTION 294
- (Exam Topic 3)
To communicate the risk associated with IT in business terms, which of the following MUST be defined?

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

Answer:

C

NEW QUESTION 296
- (Exam Topic 3)
Which of the following should be a risk practitioner's PRIMARY focus when tasked with ensuring organization records are being retained for a sufficient period of time to meet legal obligations?

A. Data duplication processes
B. Data archival processes
C. Data anonymization processes
D. Data protection processes

Answer: B

NEW QUESTION 300
- (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 304
- (Exam Topic 3)
Which of the following is the BEST source for identifying key control indicators (KCIs)?

A. Privileged user activity monitoring controls
B. Controls mapped to organizational risk scenarios
C. Recent audit findings of control weaknesses
D. A list of critical security processes

Answer: B

NEW QUESTION 305
- (Exam Topic 3)
Which of the following would be MOST helpful when communicating roles associated with the IT risk management process?

A. Skills matrix
B. Job descriptions
C. RACI chart
D. Organizational chart

Answer: A

NEW QUESTION 306
- (Exam Topic 3)
Who is BEST suited to determine whether a new control properly mitigates data loss risk within a system?

A. Data owner
B. Control owner
C. Risk owner
D. System owner

Answer: B

NEW QUESTION 308
- (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 313
- (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 315
- (Exam Topic 3)
Which of the following BEST represents a critical threshold value for a key control indicator (KCI)?

A. The value at which control effectiveness would fail
B. Thresholds benchmarked to peer organizations
C. A typical operational value
D. A value that represents the intended control state

Answer: A

NEW QUESTION 320
- (Exam Topic 3)
Which of the following controls BEST helps to ensure that transaction data reaches its destination?

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

Answer: B

NEW QUESTION 325
- (Exam Topic 3)
All business units within an organization have the same risk response plan for creating local disaster recovery plans. In an effort to achieve cost effectiveness, the BEST course of action would be to:

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

Answer: D

NEW QUESTION 328
- (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 333
- (Exam Topic 4)
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 334
- (Exam Topic 4)
Which of the following situations presents the GREATEST challenge to creating a comprehensive IT risk profile of an organization?

A. Manual vulnerability scanning processes
B. Organizational reliance on third-party service providers
C. Inaccurate documentation of enterprise architecture (EA)
D. Risk-averse organizational risk appetite

Answer: D

NEW QUESTION 336
- (Exam Topic 4)
Which of the following would provide the MOST helpful input to develop risk scenarios associated with hosting an organization's key IT applications in a cloud

environment?

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

Answer: D

NEW QUESTION 337
- (Exam Topic 4)
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 341
- (Exam Topic 4)
An information security audit identified a risk resulting from the failure of an automated control Who is responsible for ensuring the risk register is updated accordingly?

A. The risk practitioner
B. The risk owner
C. The control owner
D. The audit manager

Answer: A

NEW QUESTION 342
- (Exam Topic 4)
Which of the following BEST enables a risk practitioner to understand management's approach to organizational risk?

A. Organizational structure and job descriptions
B. Risk appetite and risk tolerance
C. Industry best practices for risk management
D. Prior year's risk assessment results

Answer: B

NEW QUESTION 346
- (Exam Topic 4)
An organization has agreed to a 99% availability for its online services and will not accept availability that falls below 98.5%. This is an example of:

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

Answer: C

NEW QUESTION 351
- (Exam Topic 4)
An organization maintains independent departmental risk registers that are not automatically aggregated. Which of the following is the GREATEST concern?

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

Answer: A

NEW QUESTION 352
- (Exam Topic 4)
Which of the following is the BEST approach to mitigate the risk associated with a control deficiency?

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

Answer: C

NEW QUESTION 355
- (Exam Topic 4)
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 357
- (Exam Topic 4)
Which of the following has the GREATEST influence on an organization's risk appetite?

A. Threats and vulnerabilities
B. Internal and external risk factors
C. Business objectives and strategies
D. Management culture and behavior

Answer: D

NEW QUESTION 360
- (Exam Topic 4)
Which of the following would BEST facilitate the implementation of data classification requirements?

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

Answer: A

NEW QUESTION 363
- (Exam Topic 4)
Which of the following activities BEST facilitates effective risk management throughout the organization?

A. Reviewing risk-related process documentation
B. Conducting periodic risk assessments
C. Performing a business impact analysis (BIA)
D. Performing frequent audits

Answer: B

NEW QUESTION 367
- (Exam Topic 4)
When implementing an IT risk management program, which of the following is the BEST time to evaluate current control effectiveness?

A. Before defining a framework
B. During the risk assessment
C. When evaluating risk response
D. When updating the risk register

Answer: B

NEW QUESTION 369
- (Exam Topic 4)
Which of the following is the MOST effective way 10 identify an application backdoor prior to implementation'?

A. User acceptance testing (UAT)
B. Database activity monitoring
C. Source code review
D. Vulnerability analysis

Answer: B

NEW QUESTION 374
- (Exam Topic 4)
Which of the following BEST enables effective IT control implementation?

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

Answer: B

NEW QUESTION 376
- (Exam Topic 4)
Which of the following contributes MOST to the effective implementation of risk responses?

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

Answer: A

NEW QUESTION 380
- (Exam Topic 4)
An organization is concerned that its employees may be unintentionally disclosing data through the use of social media sites. Which of the following will MOST effectively mitigate tins risk?

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

Answer: C

NEW QUESTION 385
- (Exam Topic 4)
As pan of business continuity planning, which of the following is MOST important to include m a business impact analysis (BIA)?

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

Answer: A

NEW QUESTION 386
- (Exam Topic 4)
A zero-day vulnerability has been discovered in a globally used brand of hardware server that allows hackers to gain access to affected IT systems. Which of the following is MOST likely to change as a result of this situation?

A. Control effectiveness
B. Risk appetite
C. Risk likelihood
D. Key risk indicator (KRI)

Answer: C

NEW QUESTION 389
- (Exam Topic 4)
Who is MOST important lo include in the assessment of existing IT risk scenarios?

A. Technology subject matter experts
B. Business process owners
C. Business users of IT systems
D. Risk management consultants

Answer: C

NEW QUESTION 392
- (Exam Topic 4)
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 395
- (Exam Topic 4)
Which of the following should be used as the PRIMARY basis for evaluating the state of an organization's cloud computing environment against leading practices?

A. The cloud environment's capability maturity model
B. The cloud environment's risk register
C. The cloud computing architecture

D. The organization's strategic plans for cloud computing

Answer: A

NEW QUESTION 396
- (Exam Topic 4)
One of an organization's key IT systems cannot be patched because the patches interfere with critical business application functionalities. Which of the following would be the risk practitioner's BEST recommendation?

A. Additional mitigating controls should be identified.
B. The system should not be used until the application is changed
C. The organization's IT risk appetite should be adjusted.
D. The associated IT risk should be accepted by management.

Answer: A

NEW QUESTION 399
- (Exam Topic 4)
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 401
- (Exam Topic 4)
Which of the following is the PRIMARY reason for an organization to include an acceptable use banner when users log in?

A. To reduce the likelihood of insider threat
B. To eliminate the possibility of insider threat
C. To enable rapid discovery of insider threat
D. To reduce the impact of insider threat

Answer: A

NEW QUESTION 405
- (Exam Topic 4)
When confirming whether implemented controls are operating effectively, which of the following is MOST important to review?

A. Results of benchmarking studies
B. Results of risk assessments
C. Number of emergency change requests
D. Maturity model

Answer: B

NEW QUESTION 406
- (Exam Topic 4)
Which of the following observations from a third-party service provider review would be of GREATEST concern to a risk practitioner?

A. Service level agreements (SLAs) have not been met over the last quarter.
B. The service contract is up for renewal in less than thirty days.
C. Key third-party personnel have recently been replaced.
D. Monthly service charges are significantly higher than industry norms.

Answer: C

NEW QUESTION 408
- (Exam Topic 4)
To define the risk management strategy which of the following MUST be set by the board of directors?

A. Operational strategies
B. Risk governance
C. Annualized loss expectancy (ALE)
D. Risk appetite

Answer: B

NEW QUESTION 409
- (Exam Topic 4)
An organization wants to launch a campaign to advertise a new product Using data analytics, the campaign can be targeted to reach potential customers. Which of the following should be of GREATEST concern to the risk practitioner?

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

Answer: D

NEW QUESTION 413
- (Exam Topic 4)
Which of the blowing is MOST important when implementing an organization s security policy?

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

Answer: A

NEW QUESTION 414
- (Exam Topic 4)
Which of the following is the MOST effective way to reduce potential losses due to ongoing expense fraud?

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

Answer: A

NEW QUESTION 418
- (Exam Topic 4)
An organization recently configured a new business division Which of the following is MOST likely to be affected?

A. Risk profile
B. Risk culture
C. Risk appetite
D. Risk tolerance

Answer: A

NEW QUESTION 420
- (Exam Topic 4)
An organization retains footage from its data center security camera for 30 days when the policy requires 90-day retention The business owner challenges whether the situation is worth remediating Which of the following is the risk manager s BEST response'

A. Identify the regulatory bodies that may highlight this gap
B. Highlight news articles about data breaches
C. Evaluate the risk as a measure of probable loss
D. Verify if competitors comply with a similar policy

Answer: B

NEW QUESTION 421
- (Exam Topic 4)
Which of the following would be the result of a significant increase in the motivation of a malicious threat actor?

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

Answer: C

NEW QUESTION 423
- (Exam Topic 4)
Which of the following is MOST helpful in identifying loss magnitude during risk analysis of a new system?

A. Recovery time objective (RTO)
B. Cost-benefit analysis
C. Business impact analysis (BIA)
D. Cyber insurance coverage

Answer: C

NEW QUESTION 427

- (Exam Topic 4)
An organization has experienced a cyber attack that exposed customer personally identifiable information (Pll) and caused extended outages of network services. Which of the following stakeholders are MOST important to include in the cyber response team to determine response actions?

A. Security control owners based on control failures
B. Cyber risk remediation plan owners
C. Risk owners based on risk impact
D. Enterprise risk management (ERM) team

Answer: C

NEW QUESTION 430
- (Exam Topic 4)
Which of the following should be of GREATEST concern when reviewing the results of an independent control assessment to determine the effectiveness of a vendor's control environment?

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

Answer: A

NEW QUESTION 433
- (Exam Topic 4)
Which of the following is MOST important for successful incident response?

A. The quantity of data logged by the attack control tools
B. Blocking the attack route immediately
C. The ability to trace the source of the attack
D. The timeliness of attack recognition

Answer: D

NEW QUESTION 437
- (Exam Topic 4)
Which of the following is the PRIMARY objective of maintaining an information asset inventory?

A. To provide input to business impact analyses (BIAs)
B. To protect information assets
C. To facilitate risk assessments
D. To manage information asset licensing

Answer: B

NEW QUESTION 442
- (Exam Topic 4)
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 444
- (Exam Topic 4)
In order to efficiently execute a risk response action plan, it is MOST important for the emergency response team members to understand:

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

Answer: D

NEW QUESTION 446
- (Exam Topic 4)
The cost of maintaining a control has grown to exceed the potential loss. Which of the following BEST describes this situation?

A. Insufficient risk tolerance
B. Optimized control management
C. Effective risk management
D. Over-controlled environment

Answer: B

NEW QUESTION 451
- (Exam Topic 4)
Which of the following is the BEST way to determine whether system settings are in alignment with control baselines?

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

Answer: A

NEW QUESTION 453
- (Exam Topic 4)
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 455
- (Exam Topic 4)
Which of the following proposed benefits is MOST likely to influence senior management approval to reallocate budget for a new security initiative?

A. Reduction in the number of incidents
B. Reduction in inherent risk
C. Reduction in residual risk
D. Reduction in the number of known vulnerabilities

Answer: B

NEW QUESTION 456
- (Exam Topic 4)
Which of the following would be the BEST way for a risk practitioner to validate the effectiveness of a patching program?

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

Answer: C

NEW QUESTION 460
- (Exam Topic 4)
Which of the following is a risk practitioner's BEST recommendation upon learning that an employee inadvertently disclosed sensitive data to a vendor?

A. Enroll the employee in additional security training.
B. Invoke the incident response plan.
C. Conduct an internal audit.
D. Instruct the vendor to delete the data.

Answer: B

NEW QUESTION 462
- (Exam Topic 4)
Before assigning sensitivity levels to information it is MOST important to:

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

Answer: B

NEW QUESTION 467
- (Exam Topic 4)
Which of the following is the result of a realized risk scenario?

A. Threat event
B. Vulnerability event
C. Technical event
D. Loss event

Answer:

D

NEW QUESTION 471
- (Exam Topic 4)
A risk practitioner has established that a particular control is working as desired, but the annual cost of maintenance has increased and now exceeds the expected annual loss exposure. The result is that the control is:

A. mature
B. ineffective.
C. optimized.
D. inefficient.

Answer: B

NEW QUESTION 473
- (Exam Topic 4)
After an annual risk assessment is completed, which of the following would be MOST important to communicate to stakeholders?

A. A decrease in threats
B. A change in the risk profile
C. An increase in reported vulnerabilities
D. An increase in identified risk scenarios

Answer: B

NEW QUESTION 477
- (Exam Topic 4)
A risk practitioner has identified that the agreed recovery time objective (RTO) with a Software as a Service (SaaS) provider is longer than the business expectation. Which ot the following is the risk practitioner's BEST course of action?

A. Collaborate with the risk owner to determine the risk response plan.
B. Document the gap in the risk register and report to senior management.
C. Include a right to audit clause in the service provider contract.
D. Advise the risk owner to accept the risk.

Answer: A

NEW QUESTION 482
- (Exam Topic 4)
Who is the BEST person to the employee personal data?

A. Human resources (HR) manager
B. System administrator
C. Data privacy manager
D. Compliance manager

Answer: A

NEW QUESTION 485
- (Exam Topic 4)
Of the following, who is responsible for approval when a change in an application system is ready for release to production?

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

Answer: C

NEW QUESTION 488
- (Exam Topic 4)
Which of the following should be accountable for ensuring that media containing financial information are adequately destroyed per an organization's data disposal policy?

A. Compliance manager
B. Data architect
C. Data owner
D. Chief information officer (CIO)

Answer: C

NEW QUESTION 491
- (Exam Topic 4)
An organization has decided to use an external auditor to review the control environment of an outsourced service provider. The BEST control criteria to evaluate the provider would be based on:

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

Answer: D

NEW QUESTION 493
- (Exam Topic 4)
It is MOST important that security controls for a new system be documented in:

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

Answer: C

NEW QUESTION 494
- (Exam Topic 4)
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 495
- (Exam Topic 4)
Which of the following is the ULTIMATE goal of conducting a privacy impact analysis (PIA)?

A. To identify gaps in data protection controls
B. To develop a customer notification plan
C. To identify personally identifiable information (PII)
D. To determine gaps in data identification processes

Answer: A

NEW QUESTION 498
- (Exam Topic 4)
Which of the following is MOST important to determine as a result of a risk assessment?

A. Process ownership
B. Risk appetite statement
C. Risk tolerance levels
D. Risk response options

Answer: D

NEW QUESTION 499
- (Exam Topic 4)
Which of the following is the GREATEST benefit of a three lines of defense structure?

A. An effective risk culture that empowers employees to report risk
B. Effective segregation of duties to prevent internal fraud
C. Clear accountability for risk management processes
D. Improved effectiveness and efficiency of business operations

Answer: C

NEW QUESTION 502
- (Exam Topic 4)
What should be the PRIMARY consideration related to data privacy protection when there are plans for a business initiative to make use of personal information?

A. Do not collect or retain data that is not needed.
B. Redact data where possible.
C. Limit access to the personal data.
D. Ensure all data is encrypted at rest and during transit.

Answer: D

NEW QUESTION 505
- (Exam Topic 4)

Which of the following should be the PRIMARY input to determine risk tolerance?

A. Regulatory requirements
B. Organizational objectives
C. Annual loss expectancy (ALE)
D. Risk management costs

Answer: C

NEW QUESTION 508
- (Exam Topic 4)
An organization recently implemented a machine learning-based solution to monitor IT usage and analyze user behavior in an effort to detect internal fraud. Which of the following is MOST likely to be reassessed as a result of this initiative?

A. Risk likelihood
B. Risk culture
C. Risk appetite
D. Risk capacity

Answer: A

NEW QUESTION 509
- (Exam Topic 4)
Which of the following should be a risk practitioner's NEXT step after learning of an incident that has affected a competitor?

A. Activate the incident response plan.
B. Implement compensating controls.
C. Update the risk register.
D. Develop risk scenarios.

Answer: A

NEW QUESTION 514
- (Exam Topic 4)
After entering a large number of low-risk scenarios into the risk register, it is MOST important for the risk practitioner to:

A. prepare a follow-up risk assessment.
B. recommend acceptance of the risk scenarios.
C. reconfirm risk tolerance levels.
D. analyze changes to aggregate risk.

Answer: D

NEW QUESTION 519
- (Exam Topic 4)
During a risk assessment, a risk practitioner learns that an IT risk factor is adequately mitigated by compensating controls in an associated business process. Which of the following would enable the MOST effective management of the residual risk?

A. Schedule periodic reviews of the compensating controls' effectiveness.
B. Report the use of compensating controls to senior management.
C. Recommend additional IT controls to further reduce residual risk.
D. Request that ownership of the compensating controls is reassigned to IT

Answer: A

NEW QUESTION 521
- (Exam Topic 4)
Which of the following should be the PRIMARY basis for prioritizing risk responses?

A. The impact of the risk
B. The replacement cost of the business asset
C. The cost of risk mitigation controls
D. The classification of the business asset

Answer: A

NEW QUESTION 523
- (Exam Topic 4)
Which of the following would BEST mitigate the ongoing risk associated with operating system (OS) vulnerabilities?

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

Answer: B

NEW QUESTION 526
- (Exam Topic 4)
Which of the following is MOST important when determining risk appetite?

A. Assessing regulatory requirements
B. Benchmarking against industry standards
C. Gaining management consensus
D. Identifying risk tolerance

Answer: C

NEW QUESTION 531
- (Exam Topic 4)
The following is the snapshot of a recently approved IT risk register maintained by an organization's information security department.

Risk ID	Risk Title	Risk Description	Risk Submitter	Risk Owner	Control Owner(s)	Risk Likelihood Rating	Risk Impact Rating	Risk Exposure	Risk Response Type	Risk Response Description
R001	Mobile Data Theft	Laptops and mobile devices can be lost or stolen leading to data compromise	Risk Council	End-User Computing Manager AND Inventory Manager	IT Operations Manager AND Security Operations	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 536
- (Exam Topic 4)
Which of the following is MOST important for an organization to consider when developing its IT strategy?

A. IT goals and objectives
B. Organizational goals and objectives
C. The organization's risk appetite statement
D. Legal and regulatory requirements

Answer: C

NEW QUESTION 539
- (Exam Topic 3)
Which of the following will be the GREATEST concern when assessing the risk profile of an organization?

A. The risk profile was not updated after a recent incident
B. The risk profile was developed without using industry standards.
C. The risk profile was last reviewed two years ago.
D. The risk profile does not contain historical loss data.

Answer: A

NEW QUESTION 542
- (Exam Topic 3)
Which of the following BEST indicates that an organization has implemented IT performance requirements?

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

Answer: A

NEW QUESTION 545
- (Exam Topic 3)
Which of the following would BEST mitigate the risk associated with reputational damage from inappropriate use of social media sites by employees?

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

Answer: D

NEW QUESTION 550
- (Exam Topic 3)
A chief information officer (CIO) has identified risk associated with shadow systems being maintained by business units to address specific functionality gaps in the organization's enterprise resource planning (ERP) system. What is the BEST way to reduce this risk going forward?

A. Align applications to business processes.
B. Implement an enterprise architecture (EA).
C. Define the software development life cycle (SDLC).
D. Define enterprise-wide system procurement requirements.

Answer: B

NEW QUESTION 551
- (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 552
- (Exam Topic 3)
Which of the following should be the MOST important consideration for senior management when developing a risk response strategy?

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

Answer: A

NEW QUESTION 554
- (Exam Topic 3)
Which of the following BEST indicates that additional or improved controls ate needed m the environment?

A. Management, has decreased organisational risk appetite
B. The risk register and portfolio do not include all risk scenarios
C. merging risk scenarios have been identified
D. Risk events and losses exceed risk tolerance

Answer: D

NEW QUESTION 555
- (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 559
- (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 562
- (Exam Topic 3)
An organization's risk register contains a large volume of risk scenarios that senior management considers overwhelming. Which of the following would BEST help to improve the risk register?

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

Answer: D

NEW QUESTION 564
- (Exam Topic 3)
The BEST way to determine the likelihood of a system availability risk scenario is by assessing the:

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

Answer: D

NEW QUESTION 569
- (Exam Topic 3)
Which of the following provides the BEST measurement of an organization's risk management maturity level?

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

Answer: C

NEW QUESTION 570
- (Exam Topic 3)
The BEST key performance indicator (KPI) to measure the effectiveness of a backup process would be the number of:

A. resources to monitor backups
B. restoration monitoring reports
C. backup recovery requests
D. recurring restore failures

Answer: D

NEW QUESTION 574
- (Exam Topic 3)
Which of the following is the BEST indicator of an effective IT security awareness program?

A. Decreased success rate of internal phishing tests
B. Decreased number of reported security incidents
C. Number of disciplinary actions issued for security violations
D. Number of employees that complete security training

Answer: A

NEW QUESTION 576
- (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 579
- (Exam Topic 3)
Which of the following is the GREATEST benefit to an organization when updates to the risk register are made promptly after the completion of a risk assessment?

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

Answer: B

NEW QUESTION 581
- (Exam Topic 3)
Which of the following is MOST important when developing risk scenarios?

A. Reviewing business impact analysis (BIA)
B. Collaborating with IT audit
C. Conducting vulnerability assessments
D. Obtaining input from key stakeholders

Answer: D

NEW QUESTION 583
- (Exam Topic 3)
Which of the following BEST indicates the efficiency of a process for granting access privileges?

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

Answer: C

NEW QUESTION 588
- (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 592
- (Exam Topic 3)
A maturity model is MOST useful to an organization when it:

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

Answer: C

NEW QUESTION 593
- (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 595
- (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 600
- (Exam Topic 3)
Which of the following is the BEST way for an organization to enable risk treatment decisions?

A. Allocate sufficient funds for risk remediation.
B. Promote risk and security awareness.
C. Establish clear accountability for risk.
D. Develop comprehensive policies and standards.

Answer: C

NEW QUESTION 605
- (Exam Topic 3)
Which of the following is the MOST common concern associated with outsourcing to a service provider?

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

Answer: C

NEW QUESTION 606
- (Exam Topic 3)
In response to the threat of ransomware, an organization has implemented cybersecurity awareness activities. The risk practitioner's BEST recommendation to further reduce the impact of ransomware attacks would be to implement:

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

Answer: B

NEW QUESTION 610
- (Exam Topic 3)
Which of me following is MOST helpful to mitigate the risk associated with an application under development not meeting business objectives?

A. Identifying tweets that may compromise enterprise architecture (EA)
B. Including diverse Business scenarios in user acceptance testing (UAT)
C. Performing risk assessments during the business case development stage
D. Including key stakeholders in review of user requirements

Answer: D

NEW QUESTION 611
- (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 613
- (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 614
- (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 619
- (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 620
- (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 621
- (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 624
- (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 629
- (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 631
- (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 633
- (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 634
- (Exam Topic 3)
An IT risk practitioner has been asked to regularly report on the overall status and effectiveness of the IT risk management program. Which of the following is MOST useful for this purpose?

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

Answer: A

NEW QUESTION 635
- (Exam Topic 2)
An audit reveals that there are changes in the environment that are not reflected in the risk profile. Which of the following is the BEST course of action?

A. Review the risk identification process.
B. Inform the risk scenario owners.
C. Create a risk awareness communication plan.
D. Update the risk register.

Answer: A

NEW QUESTION 637
- (Exam Topic 2)
A key risk indicator (KRI) threshold has reached the alert level, indicating data leakage incidents are highly probable. What should be the risk practitioner's FIRST course of action?

A. Update the KRI threshold.
B. Recommend additional controls.
C. Review incident handling procedures.
D. Perform a root cause analysis.

Answer: D

NEW QUESTION 642
- (Exam Topic 2)
Which of the following is MOST helpful in developing key risk indicator (KRI) thresholds?

A. Loss expectancy information
B. Control performance predictions
C. IT service level agreements (SLAs)
D. Remediation activity progress

Answer: A

NEW QUESTION 646
- (Exam Topic 2)
When collecting information to identify IT-related risk, a risk practitioner should FIRST focus on IT:

A. risk appetite.
B. security policies
C. process maps.
D. risk tolerance level

Answer: B

NEW QUESTION 649
- (Exam Topic 2)
Controls should be defined during the design phase of system development because:

A. it is more cost-effective to determine controls in the early design phase.

B. structured analysis techniques exclude identification of controls.
C. structured programming techniques require that controls be designed before coding begins.
D. technical specifications are defined during this phase.

Answer: A

NEW QUESTION 650
- (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 652
- (Exam Topic 2)
A control owner responsible for the access management process has developed a machine learning model to automatically identify excessive access privileges. What is the risk practitioner's BEST course of action?

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

Answer: A

NEW QUESTION 655
- (Exam Topic 2)
Which of the following key risk indicators (KRIs) is MOST effective for monitoring risk related to a bring your own device (BYOD) program?

A. Number of users who have signed a BYOD acceptable use policy
B. Number of incidents originating from BYOD devices
C. Budget allocated to the BYOD program security controls
D. Number of devices enrolled in the BYOD program

Answer: D

NEW QUESTION 657
- (Exam Topic 2)
Which of the following is MOST important when defining controls?

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

Answer: C

NEW QUESTION 661
- (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 665
- (Exam Topic 2)
During a risk assessment, the risk practitioner finds a new risk scenario without controls has been entered into the risk register. Which of the following is the MOST appropriate action?

A. Include the new risk scenario in the current risk assessment.
B. Postpone the risk assessment until controls are identified.
C. Request the risk scenario be removed from the register.
D. Exclude the new risk scenario from the current risk assessment

Answer: A

NEW QUESTION 670
- (Exam Topic 2)
Which of the following is the BEST key performance indicator (KPI) to measure the effectiveness of an anti-virus program?

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

Answer: C

NEW QUESTION 673
- (Exam Topic 2)
An organization has granted a vendor access to its data in order to analyze customer behavior. Which of the following would be the MOST effective control to mitigate the risk of customer data leakage?

A. Enforce criminal background checks.
B. Mask customer data fields.
C. Require vendor to sign a confidentiality agreement.
D. Restrict access to customer data on a "need to know" basis.

Answer: D

NEW QUESTION 678
- (Exam Topic 2)
After identifying new risk events during a project, the project manager s NEXT step should be to:

A. determine if the scenarios need 10 be accepted or responded to.
B. record the scenarios into the risk register.
C. continue with a qualitative risk analysis.
D. continue with a quantitative risk analysis.

Answer: B

NEW QUESTION 683
- (Exam Topic 2)
Who should be responsible for strategic decisions on risk management?

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

Answer: B

NEW QUESTION 686
- (Exam Topic 2)
Which of the following is a KEY outcome of risk ownership?

A. Risk responsibilities are addressed.
B. Risk-related information is communicated.
C. Risk-oriented tasks are defined.
D. Business process risk is analyzed.

Answer: A

NEW QUESTION 691
- (Exam Topic 2)
Which of the following statements in an organization's current risk profile report is cause for further action by senior management?

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

Answer: B

NEW QUESTION 692
- (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 697
- (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 701
- (Exam Topic 2)
What is the MOST important consideration when aligning IT risk management with the enterprise risk management (ERM) framework?

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

Answer: B

NEW QUESTION 705
- (Exam Topic 2)
An IT organization is replacing the customer relationship management (CRM) system. Who should own the risk associated with customer data leakage caused by insufficient IT security controls for the new system?

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

Answer: B

NEW QUESTION 706
- (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 709
- (Exam Topic 2)
Which of the following is the BEST key performance indicator (KPI) for determining how well an IT policy is aligned to business requirements?

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

Answer: C

NEW QUESTION 712
- (Exam Topic 2)
Which of the following BEST promotes commitment to controls?

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

Answer: A

NEW QUESTION 713
- (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 717
- (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 719
- (Exam Topic 2)
Which of the following is MOST influential when management makes risk response decisions?

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

Answer: A

NEW QUESTION 723
- (Exam Topic 2)
Which of the following is the BEST way to ensure ongoing control effectiveness?

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

Answer: C

NEW QUESTION 726
- (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 727
- (Exam Topic 2)
A risk owner has identified a risk with high impact and very low likelihood. The potential loss is covered by insurance. Which of the following should the risk practitioner do NEXT?

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

Answer: C

NEW QUESTION 732
- (Exam Topic 2)
Which of the following provides the BEST evidence that risk responses have been executed according to their risk action plans?

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

Answer: D

NEW QUESTION 736
- (Exam Topic 2)
Which of the following is MOST critical to the design of relevant risk scenarios?

A. The scenarios are based on past incidents.
B. The scenarios are linked to probable organizational situations.
C. The scenarios are mapped to incident management capabilities.
D. The scenarios are aligned with risk management capabilities.

Answer: B

NEW QUESTION 740
- (Exam Topic 2)
Which of the following is MOST likely to be impacted as a result of a new policy which allows staff members to remotely connect to the organization's IT systems via personal or public computers?

A. Risk appetite
B. Inherent risk
C. Key risk indicator (KRI)
D. Risk tolerance

Answer: B

NEW QUESTION 743
- (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 745
- (Exam Topic 2)
Which of the following is the MAIN benefit of involving stakeholders in the selection of key risk indicators (KRIs)?

A. Improving risk awareness
B. Obtaining buy-in from risk owners
C. Leveraging existing metrics
D. Optimizing risk treatment decisions

Answer: B

NEW QUESTION 746
- (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 748
- (Exam Topic 2)
Which of the following should an organization perform to forecast the effects of a disaster?

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

Answer: A

NEW QUESTION 751
- (Exam Topic 2)
A risk practitioner recently discovered that sensitive data from the production environment is required for testing purposes in non-production environments. Which of the following i the BEST recommendation to address this situation?

A. Enable data encryption in the test environment
B. Implement equivalent security in the test environment.
C. Prevent the use of production data for test purposes
D. Mask data before being transferred to the test environment.

Answer: B

NEW QUESTION 755

- (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 756
- (Exam Topic 2)
Which of the following would qualify as a key performance indicator (KPI)?

A. Aggregate risk of the organization
B. Number of identified system vulnerabilities
C. Number of exception requests processed in the past 90 days
D. Number of attacks against the organization's website

Answer: B

NEW QUESTION 758
- (Exam Topic 2)
Which of the following will be MOST effective to mitigate the risk associated with the loss of company data stored on personal devices?

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

Answer: C

NEW QUESTION 763
- (Exam Topic 2)
Which of the following should management consider when selecting a risk mitigation option?

A. Maturity of the enterprise architecture
B. Cost of control implementation
C. Reliability of key performance indicators (KPIs)
D. Reliability of key risk indicators (KPIs)

Answer: B

NEW QUESTION 764
- (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 769
- (Exam Topic 2)
Which of the following is the MOST important consideration when determining whether to accept residual risk after security controls have been implemented on a critical system?

A. Cost versus benefit of additional mitigating controls
B. Annualized loss expectancy (ALE) for the system
C. Frequency of business impact
D. Cost of the Information control system

Answer: A

NEW QUESTION 774
- (Exam Topic 2)
Which of the following BEST supports the communication of risk assessment results to stakeholders?

A. Monitoring of high-risk areas
B. Classification of risk profiles
C. Periodic review of the risk register
D. Assignment of risk ownership

Answer: D

NEW QUESTION 778
- (Exam Topic 2)
Which of the following should be the MAIN consideration when validating an organization's risk appetite?

A. Comparison against regulations
B. Maturity of the risk culture
C. Capacity to withstand loss
D. Cost of risk mitigation options

Answer: B

NEW QUESTION 782
- (Exam Topic 2)
Which of the following is the BEST indicator of the effectiveness of a control monitoring program?

A. Time between control failure and failure detection
B. Number of key controls as a percentage of total control count
C. Time spent on internal control assessment reviews
D. Number of internal control failures within the measurement period

Answer: A

NEW QUESTION 784
- (Exam Topic 2)
Which of the following is the MOST important consideration when performing a risk assessment of a fire suppression system within a data center?

A. Insurance coverage
B. Onsite replacement availability
C. Maintenance procedures
D. Installation manuals

Answer: C

NEW QUESTION 785
- (Exam Topic 2)
Which of the following is the MOST important input when developing risk scenarios?

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

Answer: B

NEW QUESTION 789
- (Exam Topic 2)
Which of the following would BEST enable mitigation of newly identified risk factors related to internet of Things (IoT)?

A. Introducing control procedures early in the life cycle
B. Implementing IoT device software monitoring
C. Performing periodic risk assessments of IoT
D. Performing secure code reviews

Answer: A

NEW QUESTION 790
- (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 794
- (Exam Topic 2)
Which of the following would MOST likely result in updates to an IT risk appetite statement?

A. External audit findings
B. Feedback from focus groups
C. Self-assessment reports
D. Changes in senior management

Answer: D

NEW QUESTION 797
- (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 799
- (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 802
- (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 806
- (Exam Topic 2)
From a risk management perspective, which of the following is the PRIMARY benefit of using automated system configuration validation tools?

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

Answer: C

NEW QUESTION 809
- (Exam Topic 2)
Which of the following BEST facilitates the development of effective IT risk scenarios?

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

Answer: A

NEW QUESTION 814
- (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 818
- (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 823
- (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 826
- (Exam Topic 2)
Which of the following is MOST important for a risk practitioner to consider when evaluating plans for changes to IT services?

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

Answer: B

NEW QUESTION 829
- (Exam Topic 2)
The PRIMARY purpose of vulnerability assessments is to:

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

Answer: D

NEW QUESTION 834
- (Exam Topic 2)
An organization's HR department has implemented a policy requiring staff members to take a minimum of five consecutive days leave per year to mitigate the risk of malicious insider activities. Which of the following is the BEST key performance indicator (KPI) of the effectiveness of this policy?

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

Answer: B

NEW QUESTION 839
- (Exam Topic 2)
A new regulator/ requirement imposes severe fines for data leakage involving customers' personally identifiable information (Pll). The risk practitioner has recommended avoiding the risk. Which of the following actions would BEST align with this recommendation?

A. Reduce retention periods for Pll data.
B. Move Pll to a highly-secured outsourced site.
C. Modify business processes to stop collecting Pll.
D. Implement strong encryption for Pll.

Answer: C

NEW QUESTION 844
- (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 848
- (Exam Topic 2)

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

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

Answer: A

NEW QUESTION 852
- (Exam Topic 2)
Which of the following is MOST important for an organization to have in place when developing a risk management framework?

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

Answer: A

NEW QUESTION 853
- (Exam Topic 2)
An organization has outsourced its lease payment process to a service provider who lacks evidence of compliance with a necessary regulatory standard. Which risk treatment was adopted by the organization?

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

Answer: A

NEW QUESTION 857
- (Exam Topic 2)
For no apparent reason, the time required to complete daily processing for a legacy application is approaching a risk threshold. Which of the following activities should be performed FIRST?

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

Answer: D

NEW QUESTION 862
- (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 864
- (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 869
- (Exam Topic 2)
A control owner has completed a year-long project To strengthen existing controls. It is MOST important for the risk practitioner to:

A. update the risk register to reflect the correct level of residual risk.
B. ensure risk monitoring for the project is initiated.
C. conduct and document a business impact analysis (BIA).
D. verify cost-benefit of the new controls being implemented.

Answer: A

NEW QUESTION 873
- (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 875
- (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 878
- (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 880
- (Exam Topic 2)
A payroll manager discovers that fields in certain payroll reports have been modified without authorization. Which of the following control weaknesses could have contributed MOST to this problem?

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

Answer: B

NEW QUESTION 881
- (Exam Topic 2)
An organization's financial analysis department uses an in-house forecasting application for business projections. Who is responsible for defining access roles to protect the sensitive data within this application?

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

Answer: D

NEW QUESTION 886
- (Exam Topic 2)
Which of the following methods would BEST contribute to identifying obscure risk scenarios?

A. Brainstorming sessions
B. Control self-assessments
C. Vulnerability analysis
D. Monte Carlo analysis

Answer: A

NEW QUESTION 890
- (Exam Topic 2)
Which of the following will MOST improve stakeholders' understanding of the effect of a potential threat?

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

D. Establishing metrics to assess the effectiveness of the responses

Answer: C

NEW QUESTION 893
- (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 898
- (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 900
.....

Relate Links

100% Pass Your CRISC Exam with Exambible Prep Materials

https://www.exambible.com/CRISC-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/