Exam Questions CRISC

Certified in Risk and Information Systems Control

https://www.2passeasy.com/dumps/CRISC/

NEW QUESTION 1
- (Exam Topic 1)
Which of the following is the FIRST step in managing the risk associated with the leakage of confidential data?

A. Maintain and review the classified data inventor.
B. Implement mandatory encryption on data
C. Conduct an awareness program for data owners and users.
D. Define and implement a data classification policy

Answer: D

NEW QUESTION 2
- (Exam Topic 1)
Which of the following is the BEST course of action to reduce risk impact?

A. Create an IT security policy.
B. Implement corrective measures.
C. Implement detective controls.
D. Leverage existing technology

Answer: B

NEW QUESTION 3
- (Exam Topic 1)
A control for mitigating risk in a key business area cannot be implemented immediately. Which of the following is the risk practitioner's BEST course of action when a compensating control needs to be applied?

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

Answer: A

NEW QUESTION 4
- (Exam Topic 1)
Which of the following BEST provides an early warning that network access of terminated employees is not being revoked in accordance with the service level agreement (SLA)?

A. Updating multi-factor authentication
B. Monitoring key access control performance indicators
C. Analyzing access control logs for suspicious activity
D. Revising the service level agreement (SLA)

Answer: B

NEW QUESTION 5
- (Exam Topic 1)
From a business perspective, which of the following is the MOST important objective of a disaster recovery test?

A. The organization gains assurance it can recover from a disaster
B. Errors are discovered in the disaster recovery process.
C. All business critical systems are successfully tested.
D. All critical data is recovered within recovery time objectives (RTOs).

Answer: B

NEW QUESTION 6
- (Exam Topic 1)
Establishing and organizational code of conduct is an example of which type of control?

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

Answer: B

NEW QUESTION 7
- (Exam Topic 1)
Which of the following is the MOST important consideration when selecting key risk indicators (KRIs) to monitor risk trends over time?

A. Ongoing availability of data
B. Ability to aggregate data
C. Ability to predict trends

D. Availability of automated reporting systems

Answer: C

NEW QUESTION 8
- (Exam Topic 1)
After a high-profile systems breach at an organization s key vendor, the vendor has implemented additional mitigating controls. The vendor has voluntarily shared the following set of assessments:
After a high-profile systems breach at an organization s key vendor, the vendor has implemented additional mitigating controls. The vendor has voluntarily shared the following set of assessments:
Which of the assessments provides the MOST reliable input to evaluate residual risk in the vendor's control environment?

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

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

Answer: B

NEW QUESTION 9
- (Exam Topic 1)
Which of the following will BEST help mitigate the risk associated with malicious functionality in outsourced application development?

A. Perform an m-depth code review with an expert
B. Validate functionality by running in a test environment
C. Implement a service level agreement.
D. Utilize the change management process.

Answer: C

NEW QUESTION 10
- (Exam Topic 1)
Which of the following is the BEST way to identify changes to the risk landscape?

A. Internal audit reports
B. Access reviews
C. Threat modeling
D. Root cause analysis

Answer: C

NEW QUESTION 10
- (Exam Topic 1)
A risk heat map is MOST commonly used as part of an IT risk analysis to facilitate risk:

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

Answer: C

NEW QUESTION 14
- (Exam Topic 1)
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 16
- (Exam Topic 1)
The head of a business operations department asks to review the entire IT risk register. Which of the following would be the risk manager s BEST approach to this request before sharing the register?

A. Escalate to senior management
B. Require a nondisclosure agreement.
C. Sanitize portions of the register
D. Determine the purpose of the request

Answer: D

NEW QUESTION 18
- (Exam Topic 1)
A risk practitioner has determined that a key control does not meet design expectations. Which of the following should be done NEXT?

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

Answer: A

NEW QUESTION 23
- (Exam Topic 1)
Which of the following roles would be MOST helpful in providing a high-level view of risk related to customer data loss?

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

Answer: A

NEW QUESTION 28
- (Exam Topic 1)
A risk practitioner is summarizing the results of a high-profile risk assessment sponsored by senior management. The BEST way to support risk-based decisions by senior management would be to:

A. map findings to objectives.
B. provide a quantified detailed analysts.
C. recommend risk tolerance thresholds.
D. quantify key risk indicators (KRIs).

Answer: A

NEW QUESTION 33
- (Exam Topic 1)
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 38
- (Exam Topic 1)
Which of the following is the BEST indication of an improved risk-aware culture following the implementation of a security awareness training program for all employees?

A. A reduction in the number of help desk calls
B. An increase in the number of identified system flaws
C. A reduction in the number of user access resets
D. An increase in the number of incidents reported

Answer: B

NEW QUESTION 39
- (Exam Topic 1)
Periodically reviewing and updating a risk register with details on identified risk factors PRIMARILY helps to:

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

Answer: C

NEW QUESTION 42
- (Exam Topic 1)
A contract associated with a cloud service provider MUST include:

A. ownership of responsibilities.
B. a business recovery plan.
C. provision for source code escrow.
D. the providers financial statements.

Answer: A

NEW QUESTION 45
- (Exam Topic 1)
During an IT risk scenario review session, business executives question why they have been assigned ownership of IT-related risk scenarios. They feel IT risk is technical in nature and therefore should be owned by IT. Which of the following is the BEST way for the risk practitioner to address these concerns?

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

Answer: A

NEW QUESTION 46
- (Exam Topic 1)
Which of the following is the MAIN reason to continuously monitor IT-related risk?

A. To redefine the risk appetite and risk tolerance levels based on changes in risk factors
B. To update the risk register to reflect changes in levels of identified and new IT-related risk
C. To ensure risk levels are within acceptable limits of the organization's risk appetite and risk tolerance
D. To help identify root causes of incidents and recommend suitable long-term solutions

Answer: C

NEW QUESTION 50
- (Exam Topic 1)
Which of the following risk management practices BEST facilitates the incorporation of IT risk scenarios into the enterprise-wide risk register?

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

Answer: D

NEW QUESTION 52
- (Exam Topic 1)
The PRIMARY benefit of maintaining an up-to-date risk register is that it helps to:

A. implement uniform controls for common risk scenarios.
B. ensure business unit risk is uniformly distributed.
C. build a risk profile for management review.
D. quantify the organization's risk appetite.

Answer: C

NEW QUESTION 55
- (Exam Topic 1)
Which of the following should be the HIGHEST priority when developing a risk response?

A. The risk response addresses the risk with a holistic view.
B. The risk response is based on a cost-benefit analysis.
C. The risk response is accounted for in the budget.
D. The risk response aligns with the organization's risk appetite.

Answer: D

NEW QUESTION 60
- (Exam Topic 1)
Calculation of the recovery time objective (RTO) is necessary to determine the:

A. time required to restore files.
B. point of synchronization
C. priority of restoration.
D. annual loss expectancy (ALE).

Answer:

A

NEW QUESTION 64
- (Exam Topic 1)
Which of the following is the MOST important requirement for monitoring key risk indicators (KRIs) using log analysis?

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

Answer: B

NEW QUESTION 68
- (Exam Topic 1)
Which of the following is the BEST metric to demonstrate the effectiveness of an organization's change management process?

A. Increase in the frequency of changes
B. Percent of unauthorized changes
C. Increase in the number of emergency changes
D. Average time to complete changes

Answer: B

NEW QUESTION 73
- (Exam Topic 1)
An application owner has specified the acceptable downtime in the event of an incident to be much lower than the actual time required for the response team to recover the application. Which of the following should be the NEXT course of action?

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

Answer: C

NEW QUESTION 75
- (Exam Topic 1)
The PRIMARY advantage of implementing an IT risk management framework is the:

A. establishment of a reliable basis for risk-aware decision making.
B. compliance with relevant legal and regulatory requirements.
C. improvement of controls within the organization and minimized losses.
D. alignment of business goals with IT objectives.

Answer: A

NEW QUESTION 77
- (Exam Topic 1)
Which of the following is the BEST approach to use when creating a comprehensive set of IT risk scenarios?

A. Derive scenarios from IT risk policies and standards.
B. Map scenarios to a recognized risk management framework.
C. Gather scenarios from senior management.
D. Benchmark scenarios against industry peers.

Answer: A

NEW QUESTION 79
- (Exam Topic 1)
The PRIMARY objective for selecting risk response options is to:

A. reduce risk 10 an acceptable level.
B. identify compensating controls.
C. minimize residual risk.
D. reduce risk factors.

Answer: A

NEW QUESTION 84
- (Exam Topic 1)
A risk practitioner discovers several key documents detailing the design of a product currently in development have been posted on the Internet. What should be the risk practitioner's FIRST course of action?

A. invoke the established incident response plan.
B. Inform internal audit.

C. Perform a root cause analysis
D. Conduct an immediate risk assessment

Answer: A

NEW QUESTION 89
- (Exam Topic 1)
Which of the following is the BEST indication of an effective risk management program?

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

Answer: B

NEW QUESTION 91
- (Exam Topic 1)
Which of the following will BEST quantify the risk associated with malicious users in an organization?

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

Answer: A

NEW QUESTION 95
- (Exam Topic 1)
Which of the following is the PRIMARY factor in determining a recovery time objective (RTO)?

A. Cost of offsite backup premises
B. Cost of downtime due to a disaster
C. Cost of testing the business continuity plan
D. Response time of the emergency action plan

Answer: B

NEW QUESTION 98
- (Exam Topic 1)
Reviewing results from which of the following is the BEST way to identify information systems control deficiencies?

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

Answer: D

NEW QUESTION 99
- (Exam Topic 1)
Which of the following is the MOST important consideration when developing an organization's risk taxonomy?

A. Leading industry frameworks
B. Business context
C. Regulatory requirements
D. IT strategy

Answer: C

NEW QUESTION 102
- (Exam Topic 1)
Which of the following is MOST important to understand when determining an appropriate risk assessment approach?

A. Complexity of the IT infrastructure
B. Value of information assets
C. Management culture
D. Threats and vulnerabilities

Answer: A

NEW QUESTION 104
- (Exam Topic 1)
Which of the following is MOST important when developing key performance indicators (KPIs)?

A. Alignment to risk responses
B. Alignment to management reports
C. Alerts when risk thresholds are reached
D. Identification of trends

Answer: C

NEW QUESTION 108
- (Exam Topic 1)
Which of the following controls will BEST detect unauthorized modification of data by a database administrator?

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

Answer: B

NEW QUESTION 110
- (Exam Topic 1)
Which of the following provides the BEST evidence of the effectiveness of an organization's account provisioning process?

A. User provisioning
B. Role-based access controls
C. Security log monitoring
D. Entitlement reviews

Answer: B

NEW QUESTION 113
- (Exam Topic 1)
Which of the following is the GREATEST benefit of incorporating IT risk scenarios into the corporate risk register?

A. Corporate incident escalation protocols are established.
B. Exposure is integrated into the organization's risk profile.
C. Risk appetite cascades to business unit management
D. The organization-wide control budget is expanded.

Answer: B

NEW QUESTION 115
- (Exam Topic 1)
The number of tickets to rework application code has significantly exceeded the established threshold. Which of the following would be the risk practitioner s BEST recommendation?

A. Perform a root cause analysis
B. Perform a code review
C. Implement version control software.
D. Implement training on coding best practices

Answer: A

NEW QUESTION 117
- (Exam Topic 1)
Which of the following is the MAIN reason for documenting the performance of controls?

A. Obtaining management sign-off
B. Demonstrating effective risk mitigation
C. Justifying return on investment
D. Providing accurate risk reporting

Answer: D

NEW QUESTION 120
- (Exam Topic 1)
Which of the following attributes of a key risk indicator (KRI) is MOST important?

A. Repeatable
B. Automated
C. Quantitative
D. Qualitative

Answer: A

NEW QUESTION 124

- (Exam Topic 1)
A risk practitioner is organizing risk awareness training for senior management. Which of the following is the MOST important topic to cover in the training session?

A. The organization's strategic risk management projects
B. Senior management roles and responsibilities
C. The organizations risk appetite and tolerance
D. Senior management allocation of risk management resources

Answer: B

NEW QUESTION 127
- (Exam Topic 1)
While evaluating control costs, management discovers that the annual cost exceeds the annual loss expectancy (ALE) of the risk. This indicates the:

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

Answer: B

NEW QUESTION 128
- (Exam Topic 1)
Which of the following is the MOST critical element to maximize the potential for a successful security implementation?

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

Answer: C

NEW QUESTION 129
- (Exam Topic 1)
Which of the following is the MOST important consideration for a risk practitioner when making a system implementation go-live recommendation?

A. Completeness of system documentation
B. Results of end user acceptance testing
C. Variances between planned and actual cost
D. availability of in-house resources

Answer: B

NEW QUESTION 132
- (Exam Topic 1)
Which of the following is the GREATEST benefit of analyzing logs collected from different systems?

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

Answer: C

NEW QUESTION 134
- (Exam Topic 1)
During testing, a risk practitioner finds the IT department's recovery time objective (RTO) for a key system does not align with the enterprise's business continuity plan (BCP). Which of the following should be done NEXT?

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

Answer: A

NEW QUESTION 139
- (Exam Topic 1)
In an organization with a mature risk management program, which of the following would provide the BEST evidence that the IT risk profile is up to date?

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

Answer: B

NEW QUESTION 142
- (Exam Topic 1)
Which of the following is MOST useful when communicating risk to management?

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

Answer: A

NEW QUESTION 145
- (Exam Topic 1)
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 150
- (Exam Topic 1)
Which of the following should be the PRIMARY input when designing IT controls?

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

Answer: B

NEW QUESTION 155
- (Exam Topic 1)
The risk associated with an asset before controls are applied can be expressed as:

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

Answer: C

NEW QUESTION 160
- (Exam Topic 1)
A data processing center operates in a jurisdiction where new regulations have significantly increased penalties for data breaches. Which of the following elements of the risk register is MOST important to update to reflect this change?

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

Answer: A

NEW QUESTION 164
- (Exam Topic 1)
When updating the risk register after a risk assessment, which of the following is MOST important to include?

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

Answer: C

NEW QUESTION 168
- (Exam Topic 1)
Which of the following is MOST effective against external threats to an organizations confidential information?

A. Single sign-on
B. Data integrity checking
C. Strong authentication
D. Intrusion detection system

Answer:

C

NEW QUESTION 170
- (Exam Topic 1)
A newly hired risk practitioner finds that the risk register has not been updated in the past year. What is the risk practitioner's BEST course of action?

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

Answer: A

NEW QUESTION 172
- (Exam Topic 1)
Which of the following would be the BEST key performance indicator (KPI) for monitoring the effectiveness of the IT asset management process?

A. Percentage of unpatched IT assets
B. Percentage of IT assets without ownership
C. The number of IT assets securely disposed during the past year
D. The number of IT assets procured during the previous month

Answer: B

NEW QUESTION 177
- (Exam Topic 1)
Which of the following would be a risk practitioner'$ BEST recommendation to help ensure cyber risk is assessed and reflected in the enterprise-level risk profile?

A. Manage cyber risk according to the organization's risk management framework.
B. Define cyber roles and responsibilities across the organization
C. Conduct cyber risk awareness training tailored specifically for senior management
D. Implement a cyber risk program based on industry best practices

Answer: B

NEW QUESTION 181
- (Exam Topic 1)
Which of the following tools is MOST effective in identifying trends in the IT risk profile?

A. Risk self-assessment
B. Risk register
C. Risk dashboard
D. Risk map

Answer: C

NEW QUESTION 182
- (Exam Topic 1)
An unauthorized individual has socially engineered entry into an organization's secured physical premises. Which of the following is the BEST way to prevent future occurrences?

A. Employ security guards.
B. Conduct security awareness training.
C. Install security cameras.
D. Require security access badges.

Answer: B

NEW QUESTION 187
- (Exam Topic 1)
Which of the following roles would provide the MOST important input when identifying IT risk scenarios?

A. Information security managers
B. Internal auditors
C. Business process owners
D. Operational risk managers

Answer: C

NEW QUESTION 192
- (Exam Topic 1)
An organization that has been the subject of multiple social engineering attacks is developing a risk awareness program. The PRIMARY goal of this program should be to:

A. reduce the risk to an acceptable level.
B. communicate the consequences for violations.

C. implement industry best practices.
D. reduce the organization's risk appetite

Answer: B

NEW QUESTION 194
- (Exam Topic 1)
Which of the following is the MOST important consideration when sharing risk management updates with executive management?

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

Answer: B

NEW QUESTION 197
- (Exam Topic 1)
IT management has asked for a consolidated view into the organization's risk profile to enable project prioritization and resource allocation. Which of the following materials would
be MOST helpful?

A. IT risk register
B. List of key risk indicators
C. Internal audit reports
D. List of approved projects

Answer: A

NEW QUESTION 199
- (Exam Topic 1)
An organization has allowed its cyber risk insurance to lapse while seeking a new insurance provider. The risk practitioner should report to management that the risk has been:

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

Answer: C

NEW QUESTION 201
- (Exam Topic 1)
The BEST key performance indicator (KPI) to measure the effectiveness of a backup process would be the number of:

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

Answer: D

NEW QUESTION 204
- (Exam Topic 1)
An organization has procured a managed hosting service and just discovered the location is likely to be flooded every 20 years. Of the following, who should be notified of this new information FIRST.

A. The risk owner who also owns the business service enabled by this infrastructure
B. The data center manager who is also employed under the managed hosting services contract
C. The site manager who is required to provide annual risk assessments under the contract
D. The chief information officer (CIO) who is responsible for the hosted services

Answer: A

NEW QUESTION 206
- (Exam Topic 1)
Which of the following would be MOST important for a risk practitioner to provide to the internal audit department during the audit planning process?

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

Answer: A

NEW QUESTION 209

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

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

Answer: B

NEW QUESTION 213
- (Exam Topic 1)
Which of the following will BEST mitigate the risk associated with IT and business misalignment?

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

Answer: D

NEW QUESTION 218
- (Exam Topic 1)
After the review of a risk record, internal audit questioned why the risk was lowered from medium to low. Which of the following is the BEST course of action in responding to this inquiry?

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

Answer: B

NEW QUESTION 220
- (Exam Topic 1)
Which of the following would be considered a vulnerability?

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

Answer: A

NEW QUESTION 222
- (Exam Topic 1)
An organization has determined a risk scenario is outside the defined risk tolerance level. What should be the NEXT course of action?

A. Develop a compensating control.
B. Allocate remediation resources.
C. Perform a cost-benefit analysis.
D. Identify risk responses

Answer: D

NEW QUESTION 224
- (Exam Topic 1)
Which of the following would BEST help to ensure that identified risk is efficiently managed?

A. Reviewing the maturity of the control environment
B. Regularly monitoring the project plan
C. Maintaining a key risk indicator for each asset in the risk register
D. Periodically reviewing controls per the risk treatment plan

Answer: D

NEW QUESTION 225
- (Exam Topic 1)
A risk assessment has identified that departments have installed their own WiFi access points on the enterprise network. Which of the following would be MOST important to include in a report to senior management?

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

Answer: B

NEW QUESTION 226
- (Exam Topic 1)
During a routine check, a system administrator identifies unusual activity indicating an intruder within a firewall. Which of the following controls has MOST likely been compromised?

A. Data validation
B. Identification
C. Authentication
D. Data integrity

Answer: C

NEW QUESTION 230
- (Exam Topic 1)
Which of the following should be the PRIMARY focus of a risk owner once a decision is made to mitigate a risk?

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

Answer: A

NEW QUESTION 232
- (Exam Topic 1)
Which of the following would provide the BEST guidance when selecting an appropriate risk treatment plan?

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

Answer: B

NEW QUESTION 236
- (Exam Topic 1)
An audit reveals that several terminated employee accounts maintain access. Which of the following should be the FIRST step to address the risk?

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

Answer: B

NEW QUESTION 241
- (Exam Topic 1)
A risk practitioner has identified that the organization's secondary data center does not provide redundancy for a critical application. Who should have the authority to accept the associated risk?

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

Answer: C

NEW QUESTION 245
- (Exam Topic 1)
Which of the following is the BEST way to determine the ongoing efficiency of control processes?

A. Perform annual risk assessments.
B. Interview process owners.
C. Review the risk register.
D. Analyze key performance indicators (KPIs).

Answer: D

NEW QUESTION 248
- (Exam Topic 1)
Risk management strategies are PRIMARILY adopted to:

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

Answer: B

NEW QUESTION 250
- (Exam Topic 1)
When reviewing management's IT control self-assessments, a risk practitioner noted an ineffective control that links to several low residual risk scenarios. What should be the NEXT course of action?

A. Assess management's risk tolerance.
B. Recommend management accept the low risk scenarios.
C. Propose mitigating controls
D. Re-evaluate the risk scenarios associated with the control

Answer: D

NEW QUESTION 253
- (Exam Topic 1)
Which of the following is a PRIMARY benefit of engaging the risk owner during the risk assessment process?

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

Answer: D

NEW QUESTION 258
- (Exam Topic 1)
A PRIMARY advantage of involving business management in evaluating and managing risk is that management:

A. better understands the system architecture.
B. is more objective than risk management.
C. can balance technical and business risk.
D. can make better informed business decisions.

Answer: D

NEW QUESTION 261
- (Exam Topic 1)
Which of the following would BEST help to ensure that suspicious network activity is identified?

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

Answer: A

NEW QUESTION 262
- (Exam Topic 1)
Which of the following would BEST help minimize the risk associated with social engineering threats?

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

Answer: B

NEW QUESTION 267
- (Exam Topic 1)
Which of the following is the MOST important factor when deciding on a control to mitigate risk exposure?

A. Relevance to the business process
B. Regulatory compliance requirements
C. Cost-benefit analysis
D. Comparison against best practice

Answer: B

NEW QUESTION 272
- (Exam Topic 1)
A risk practitioners PRIMARY focus when validating a risk response action plan should be that risk response:

A. reduces risk to an acceptable level
B. quantifies risk impact

C. aligns with business strategy
D. advances business objectives.

Answer: A

NEW QUESTION 275
- (Exam Topic 1)
Which of the following techniques would be used during a risk assessment to demonstrate to stakeholders that all known alternatives were evaluated?

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

Answer: D

NEW QUESTION 277
- (Exam Topic 1)
Which of the following would be MOST useful when measuring the progress of a risk response action plan?

A. Percentage of mitigated risk scenarios
B. Annual loss expectancy (ALE) changes
C. Resource expenditure against budget
D. An up-to-date risk register

Answer: D

NEW QUESTION 278
- (Exam Topic 1)
During the risk assessment of an organization that processes credit cards, a number of existing controls have been found to be ineffective and do not meet industry standards. The overall control environment may still be effective if:

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

Answer: A

NEW QUESTION 279
- (Exam Topic 1)
Which of the following should be the PRIMARY consideration when implementing controls for monitoring user activity logs?

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

Answer: C

NEW QUESTION 281
- (Exam Topic 1)
What is the PRIMARY reason to periodically review key performance indicators (KPIs)?

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

Answer: B

NEW QUESTION 283
- (Exam Topic 1)
After undertaking a risk assessment of a production system, the MOST appropriate action is for the risk manager to:

A. recommend a program that minimizes the concerns of that production system.
B. inform the development team of the concerns, and together formulate risk reduction measures.
C. inform the process owner of the concerns and propose measures to reduce them
D. inform the IT manager of the concerns and propose measures to reduce them.

Answer: A

NEW QUESTION 288
- (Exam Topic 1)
In addition to the risk register, what should a risk practitioner review to develop an understanding of the organization's risk profile?

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

Answer: C

NEW QUESTION 289
- (Exam Topic 1)
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: D

NEW QUESTION 293
- (Exam Topic 1)
Which of the following is the MOST important factor affecting risk management in an organization?

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

Answer: B

NEW QUESTION 298
- (Exam Topic 1)
When determining which control deficiencies are most significant, which of the following would provide the MOST useful information?

A. Risk analysis results
B. Exception handling policy
C. Vulnerability assessment results
D. Benchmarking assessments

Answer: C

NEW QUESTION 301
- (Exam Topic 1)
A review of an organization s controls has determined its data loss prevention {DLP) system is currently failing to detect outgoing emails containing credit card data. Which of the following would be MOST impacted?

A. Key risk indicators (KRIs)
B. Inherent risk
C. Residual risk
D. Risk appetite

Answer: C

NEW QUESTION 305
- (Exam Topic 1)
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 306
- (Exam Topic 1)
Who is the MOST appropriate owner for newly identified IT risk?

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

Answer: B

NEW QUESTION 309

- (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 311
- (Exam Topic 2)
The PRIMARY objective for requiring an independent review of an organization's IT risk management process should be to:

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

Answer: A

NEW QUESTION 315
- (Exam Topic 2)
The PRIMARY reason for establishing various Threshold levels for a set of key risk indicators (KRIs) is to:

A. highlight trends of developing risk.
B. ensure accurate and reliable monitoring.
C. take appropriate actions in a timely manner.
D. set different triggers for each stakeholder.

Answer: B

NEW QUESTION 317
- (Exam Topic 2)
Which of the following can be used to assign a monetary value to risk?

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

Answer: A

NEW QUESTION 320
- (Exam Topic 2)
Which of the following should be of GREATEST concern to a risk practitioner when determining the effectiveness of IT controls?

A. Configuration updates do not follow formal change control.
B. Operational staff perform control self-assessments.
C. Controls are selected without a formal cost-benefit
D. analysis-Management reviews security policies once every two years.

Answer: A

NEW QUESTION 324
- (Exam Topic 2)
Which of the following is the BEST evidence that risk management is driving business decisions in an organization?

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

Answer: D

NEW QUESTION 328
- (Exam Topic 2)
An organizations chief technology officer (CTO) has decided to accept the risk associated with the potential loss from a denial-of-service (DoS) attack. In this situation, the risk practitioner's BEST course of action is to:

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

Answer: A

NEW QUESTION 330
- (Exam Topic 2)
A large organization is replacing its enterprise resource planning (ERP) system and has decided not to deploy the payroll module of the new system. Instead, the current payroll system will continue to be
used. Of the following, who should own the risk if the ERP and payroll system fail to operate as expected?

A. The business owner
B. The ERP administrator
C. The project steering committee
D. The IT project manager

Answer: A

NEW QUESTION 332
- (Exam Topic 2)
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 333
- (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 335
- (Exam Topic 2)
Which of the following is MOST helpful in aligning IT risk with business objectives?

A. Introducing an approved IT governance framework
B. Integrating the results of top-down risk scenario analyses
C. Performing a business impact analysis (BIA)
D. Implementing a risk classification system

Answer: A

NEW QUESTION 336
- (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 339
- (Exam Topic 2)
Which of the following is MOST important to review when determining whether a potential IT service provider s control environment is effective?

A. Independent audit report
B. Control self-assessment
C. Key performance indicators (KPIs)
D. Service level agreements (SLAs)

Answer: A

NEW QUESTION 342
- (Exam Topic 2)
A bank wants to send a critical payment order via email to one of its offshore branches. Which of the following is the BEST way to ensure the message reaches the intended recipient without alteration?

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

D. Add a secret key

Answer: C

NEW QUESTION 345
- (Exam Topic 2)
Which of the following would be a weakness in procedures for controlling the migration of changes to production libraries?

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

Answer: D

NEW QUESTION 349
- (Exam Topic 2)
The GREATEST concern when maintaining a risk register is that:

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

Answer: D

NEW QUESTION 350
- (Exam Topic 2)
As part of an overall IT risk management plan, an IT risk register BEST helps management:

A. align IT processes with business objectives.
B. communicate the enterprise risk management policy.
C. stay current with existing control status.
D. understand the organizational risk profile.

Answer: D

NEW QUESTION 351
- (Exam Topic 2)
A third-party vendor has offered to perform user access provisioning and termination. Which of the following control accountabilities is BEST retained within the organization?

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

Answer: B

NEW QUESTION 352
- (Exam Topic 2)
Which of the following BEST helps to identify significant events that could impact an organization? Vulnerability analysis

A. Control analysis
B. Scenario analysis
C. Heat map analysis

Answer: C

NEW QUESTION 355
- (Exam Topic 2)
Which of the following would require updates to an organization's IT risk register?

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

Answer: A

NEW QUESTION 360
- (Exam Topic 2)
A PRIMARY function of the risk register is to provide supporting information for the development of an organization's risk:

A. strategy.

B. profile.
C. process.
D. map.

Answer: A

NEW QUESTION 363
- (Exam Topic 2)
The BEST key performance indicator (KPI) for monitoring adherence to an organization's user accounts provisioning practices is the percentage of:

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

Answer: A

NEW QUESTION 367
- (Exam Topic 2)
A key risk indicator (KRI) indicates a reduction in the percentage of appropriately patched servers. Which of the following is the risk practitioner's BEST course of action?

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

Answer: C

NEW QUESTION 370
- (Exam Topic 2)
Which of the following is the FIRST step in risk assessment?

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

Answer: B

NEW QUESTION 373
- (Exam Topic 2)
Which of the following is MOST important to the integrity of a security log?

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

Answer: A

NEW QUESTION 377
- (Exam Topic 2)
An IT license audit has revealed that there are several unlicensed copies of co be to:

A. immediately uninstall the unlicensed software from the laptops
B. centralize administration rights on laptops so that installations are controlled
C. report the issue to management so appropriate action can be taken.
D. procure the requisite licenses for the software to minimize business impact.

Answer: B

NEW QUESTION 382
- (Exam Topic 2)
Which of the following is MOST important to have in place to ensure the effectiveness of risk and security metrics reporting?

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

Answer: C

NEW QUESTION 387
- (Exam Topic 2)

Implementing which of the following will BEST help ensure that systems comply with an established baseline before deployment?

A. Vulnerability scanning
B. Continuous monitoring and alerting
C. Configuration management
D. Access controls and active logging

Answer: C

NEW QUESTION 388
- (Exam Topic 2)
IT stakeholders have asked a risk practitioner for IT risk profile reports associated with specific departments to allocate resources for risk mitigation. The BEST way to address this request would be to use:

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

Answer: D

NEW QUESTION 393
- (Exam Topic 2)
The design of procedures to prevent fraudulent transactions within an enterprise resource planning (ERP) system should be based on:

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

Answer: D

NEW QUESTION 394
- (Exam Topic 2)
Which of the following is the BEST evidence that a user account has been properly authorized?

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

Answer: C

NEW QUESTION 396
- (Exam Topic 2)
Which of the following would provide executive management with the BEST information to make risk decisions as a result of a risk assessment?

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

Answer: D

NEW QUESTION 400
- (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: D

NEW QUESTION 403
- (Exam Topic 2)
Which of the following would be MOST helpful to a risk owner when making risk-aware decisions?

A. Risk exposure expressed in business terms
B. Recommendations for risk response options
C. Resource requirements for risk responses
D. List of business areas affected by the risk

Answer: A

NEW QUESTION 404
- (Exam Topic 2)
Which of the following is the BEST indicator of the effectiveness of IT risk management processes?

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

Answer: C

NEW QUESTION 409
- (Exam Topic 2)
Which of the following is the BEST way for a risk practitioner to verify that management has addressed control issues identified during a previous external audit?

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

Answer: B

NEW QUESTION 410
- (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 411
- (Exam Topic 2)
What should be the PRIMARY objective for a risk practitioner performing a post-implementation review of an IT risk mitigation project?

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

Answer: A

NEW QUESTION 414
- (Exam Topic 2)
An internal audit report reveals that not all IT application databases have encryption in place. Which of the following information would be MOST important for assessing the risk impact?

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

Answer: B

NEW QUESTION 416
- (Exam Topic 2)
The PRIMARY purpose of using control metrics is to evaluate the:

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

Answer: C

NEW QUESTION 418
- (Exam Topic 2)
What can be determined from the risk scenario chart?

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

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

Answer: A

NEW QUESTION 421
- (Exam Topic 2)
Which of The following is the PRIMARY consideration when establishing an organization's risk management methodology?

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

Answer: A

NEW QUESTION 425
- (Exam Topic 2)
Which of the following provides the MOST important information to facilitate a risk response decision?

A. Audit findings
B. Risk appetite
C. Key risk indicators
D. Industry best practices

Answer: B

NEW QUESTION 428
- (Exam Topic 2)
Sensitive data has been lost after an employee inadvertently removed a file from the premises, in violation of organizational policy. Which of the following controls MOST likely failed?

A. Background checks
B. Awareness training
C. User access
D. Policy management

Answer: C

NEW QUESTION 432
- (Exam Topic 2)
The BEST way to improve a risk register is to ensure the register:

A. is updated based upon significant events.
B. documents possible countermeasures.
C. contains the risk assessment completion date.
D. is regularly audited.

Answer: D

NEW QUESTION 435
- (Exam Topic 2)
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: C

NEW QUESTION 436
- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 439
- (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 440
- (Exam Topic 2)
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 442
- (Exam Topic 2)
Which of the following provides the MOST up-to-date information about the effectiveness of an organization's overall IT control environment?

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

Answer: A

NEW QUESTION 443
- (Exam Topic 2)
To help ensure all applicable risk scenarios are incorporated into the risk register, it is MOST important to review the:

A. risk mitigation approach
B. cost-benefit analysis.
C. risk assessment results.
D. vulnerability assessment results

Answer: C

NEW QUESTION 448
- (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: C

NEW QUESTION 450
- (Exam Topic 2)
A risk owner should be the person accountable for:

A. the risk management process
B. managing controls.
C. implementing actions.
D. the business process.

Answer: D

NEW QUESTION 454
- (Exam Topic 2)
Which of the following is the GREATEST risk associated with the use of data analytics?

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

Answer: C

NEW QUESTION 458
- (Exam Topic 2)
The BEST criteria when selecting a risk response is the:

A. capability to implement the response
B. importance of IT risk within the enterprise
C. effectiveness of risk response options
D. alignment of response to industry standards

Answer: C

NEW QUESTION 463
- (Exam Topic 2)
Which of the following provides the BEST evidence that risk mitigation plans have been implemented effectively?

A. Self-assessments by process owners
B. Mitigation plan progress reports
C. Risk owner attestation
D. Change in the level of residual risk

Answer: D

NEW QUESTION 468
- (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: A

NEW QUESTION 473
- (Exam Topic 2)
The BEST key performance indicator (KPI) to measure the effectiveness of a vendor risk management
program is the percentage of:

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

Answer: C

NEW QUESTION 478
- (Exam Topic 2)
During the control evaluation phase of a risk assessment, it is noted that multiple controls are ineffective. Which of the following should be the risk practitioner's
FIRST course of action?

A. Recommend risk remediation of the ineffective controls.
B. Compare the residual risk to the current risk appetite.
C. Determine the root cause of the control failures.
D. Escalate the control failures to senior management.

Answer: C

NEW QUESTION 479
- (Exam Topic 2)
Which of the following is the PRIMARY reason to have the risk management process reviewed by a third party?

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

Answer: A

NEW QUESTION 483
- (Exam Topic 2)
The PRIMARY purpose of IT control status reporting is to:

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

Answer: D

NEW QUESTION 484
- (Exam Topic 2)
Which of the following provides the MOST helpful reference point when communicating the results of a risk assessment to stakeholders?

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

Answer: A

NEW QUESTION 489
......

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual CRISC Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the CRISC Product From:

https://www.2passeasy.com/dumps/CRISC/

Money Back Guarantee

CRISC Practice Exam Features:

* CRISC Questions and Answers Updated Frequently

* CRISC Practice Questions Verified by Expert Senior Certified Staff

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

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