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)
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: C

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)
An organization is planning to engage a cloud-based service provider for some of its data-intensive business processes. Which of the following is MOST important to help define the IT risk associated with this outsourcing activity?

A. Service level agreement

B. Customer service reviews
C. Scope of services provided
D. Right to audit the provider

Answer: D

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 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 10
- (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 11
- (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 12
- (Exam Topic 1)

Malware has recently affected an organization, The MOST effective way to resolve this situation and define a comprehensive risk treatment plan would be to perform:

A. a gap analysis
B. a root cause analysis.
C. an impact assessment.
D. a vulnerability assessment.

Answer: C

NEW QUESTION 17
- (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 19
- (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 22
- (Exam Topic 1)
Which of the following is of GREATEST concern when uncontrolled changes are made to the control environment?

A. A decrease in control layering effectiveness
B. An increase in inherent risk
C. An increase in control vulnerabilities
D. An increase in the level of residual risk

Answer: D

NEW QUESTION 25
- (Exam Topic 1)
Which of the following should be the risk practitioner s PRIMARY focus when determining whether controls are adequate to mitigate risk?

A. Sensitivity analysis
B. Level of residual risk
C. Cost-benefit analysis
D. Risk appetite

Answer: C

NEW QUESTION 27
- (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 32
- (Exam Topic 1)
The analysis of which of the following will BEST help validate whether suspicious network activity is malicious?

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

Answer: B

NEW QUESTION 34
- (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 36
- (Exam Topic 1)
Which of the following is the MOST important data source for monitoring key risk indicators (KRIs)?

A. Directives from legal and regulatory authorities
B. Audit reports from internal information systems audits
C. Automated logs collected from different systems
D. Trend analysis of external risk factors

Answer: C

NEW QUESTION 38
- (Exam Topic 1)
The MOST important characteristic of an organization s policies is to reflect the organization's:

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

Answer: B

NEW QUESTION 42
- (Exam Topic 1)
A risk practitioner is organizing a training session lo communicate risk assessment methodologies to ensure a consistent risk view within the organization Which of the following i< the MOST important topic to cover in this training?

A. Applying risk appetite
B. Applying risk factors
C. Referencing risk event data
D. Understanding risk culture

Answer: D

NEW QUESTION 47
- (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 49
- (Exam Topic 1)
A risk assessment has identified that an organization may not be in compliance with industry regulations. The BEST course of action would be to:

A. conduct a gap analysis against compliance criteria.
B. identify necessary controls to ensure compliance.
C. modify internal assurance activities to include control validation.
D. collaborate with management to meet compliance requirements.

Answer: A

NEW QUESTION 50
- (Exam Topic 1)
Risk mitigation procedures should include:

A. buying an insurance policy.
B. acceptance of exposures
C. deployment of counter measures.
D. enterprise architecture implementation.

Answer: C

NEW QUESTION 51
- (Exam Topic 1)
An organization has outsourced its IT security operations to a third party. Who is ULTIMATELY accountable for the risk associated with the outsourced operations?

A. The third party s management
B. The organization's management
C. The control operators at the third party
D. The organization's vendor management office

Answer: B

NEW QUESTION 53
- (Exam Topic 1)
Which of the following would be MOST helpful when estimating the likelihood of negative events?

A. Business impact analysis
B. Threat analysis
C. Risk response analysis
D. Cost-benefit analysis

Answer: B

NEW QUESTION 54
- (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 59
- (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 63
- (Exam Topic 1)
The MOST effective way to increase the likelihood that risk responses will be implemented is to:

A. create an action plan
B. assign ownership
C. review progress reports
D. perform regular audits.

Answer: B

NEW QUESTION 65
- (Exam Topic 1)
A risk practitioner has observed that there is an increasing trend of users sending sensitive information by email without using encryption. Which of the following would be the MOST effective approach to mitigate the risk associated with data loss?

A. Implement a tool to create and distribute violation reports
B. Raise awareness of encryption requirements for sensitive data.
C. Block unencrypted outgoing emails which contain sensitive data.
D. Implement a progressive disciplinary process for email violations.

Answer: C

NEW QUESTION 66
- (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 71
- (Exam Topic 1)
The PRIMARY reason a risk practitioner would be interested in an internal audit report is to:

A. plan awareness programs for business managers.
B. evaluate maturity of the risk management process.
C. assist in the development of a risk profile.
D. maintain a risk register based on noncompliances.

Answer: C

NEW QUESTION 73
- (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 76
- (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 80
- (Exam Topic 1)
Numerous media reports indicate a recently discovered technical vulnerability is being actively exploited. Which of the following would be the BEST response to this scenario?

A. Assess the vulnerability management process.
B. Conduct a control serf-assessment.
C. Conduct a vulnerability assessment.
D. Reassess the inherent risk of the target.

Answer: C

NEW QUESTION 83
- (Exam Topic 1)
Which of the following is the MOST important characteristic of an effective risk management program?

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

Answer: D

NEW QUESTION 86
- (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 89
- (Exam Topic 1)
Which of the following IT controls is MOST useful in mitigating the risk associated with inaccurate data?

A. Encrypted storage of data
B. Links to source data
C. Audit trails for updates and deletions
D. Check totals on data records and data fields

Answer: C

NEW QUESTION 91
- (Exam Topic 1)
An organization operates in an environment where reduced time-to-market for new software products is a top business priority. Which of the following should be the risk practitioner's GREATEST concern?

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

Answer: A

NEW QUESTION 92
- (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 94
- (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 96
- (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 101
- (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 105
- (Exam Topic 1)
Which of the following would be- MOST helpful to understand the impact of a new technology system on an organization's current risk profile?

A. Hire consultants specializing m the new technology.
B. Review existing risk mitigation controls.
C. Conduct a gap analysis.
D. Perform a risk assessment.

Answer: D

NEW QUESTION 110

- (Exam Topic 1)
The MAIN purpose of conducting a control self-assessment (CSA) is to:

A. gain a better understanding of the control effectiveness in the organization
B. gain a better understanding of the risk in the organization
C. adjust the controls prior to an external audit
D. reduce the dependency on external audits

Answer: A

NEW QUESTION 111
- (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 112
- (Exam Topic 1)
Who should be accountable for ensuring effective cybersecurity controls are established?

A. Risk owner
B. Security management function
C. IT management
D. Enterprise risk function

Answer: B

NEW QUESTION 114
- (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 119
- (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 123
- (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 125
- (Exam Topic 1)
Which of the following BEST describes the role of the IT risk profile in strategic IT-related decisions?

A. It compares performance levels of IT assets to value delivered.
B. It facilitates the alignment of strategic IT objectives to business objectives.
C. It provides input to business managers when preparing a business case for new IT projects.
D. It helps assess the effects of IT decisions on risk exposure

Answer: D

NEW QUESTION 129
- (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 134
- (Exam Topic 1)
Which of the following helps ensure compliance with a nonrepudiation policy requirement for electronic transactions?

A. Digital signatures
B. Encrypted passwords
C. One-time passwords
D. Digital certificates

Answer: A

NEW QUESTION 138
- (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 141
- (Exam Topic 1)
The BEST reason to classify IT assets during a risk assessment is to determine the:

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

Answer: D

NEW QUESTION 145
- (Exam Topic 1)
Which of the following issues should be of GREATEST concern when evaluating existing controls during a risk assessment?

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

Answer: D

NEW QUESTION 150
- (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 155
- (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 160
- (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 165
- (Exam Topic 1)
Senior management has asked a risk practitioner to develop technical risk scenarios related to a recently developed enterprise resource planning (ERP) system. These scenarios will be owned by the system manager. Which of the following would be the BEST method to use when developing the scenarios?

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

Answer: A

NEW QUESTION 168
- (Exam Topic 1)
Which of the following is the MOST important foundational element of an effective three lines of defense model for an organization?

A. A robust risk aggregation tool set
B. Clearly defined roles and responsibilities
C. A well-established risk management committee
D. Well-documented and communicated escalation procedures

Answer: B

NEW QUESTION 172
- (Exam Topic 1)
Which of the following is MOST critical when designing controls?

A. Involvement of internal audit
B. Involvement of process owner
C. Quantitative impact of the risk
D. Identification of key risk indicators

Answer: B

NEW QUESTION 174
- (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 176
- (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 181
- (Exam Topic 1)
Which of the following is the BEST method for assessing control effectiveness?

A. Ad hoc control reporting

B. Control self-assessment
C. Continuous monitoring
D. Predictive analytics

Answer: C

NEW QUESTION 186
- (Exam Topic 1)
Which of the following activities would BEST contribute to promoting an organization-wide risk-aware culture?

A. Performing a benchmark analysis and evaluating gaps
B. Conducting risk assessments and implementing controls
C. Communicating components of risk and their acceptable levels
D. Participating in peer reviews and implementing best practices

Answer: C

NEW QUESTION 189
- (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 191
- (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 193
- (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 197
- (Exam Topic 1)
Which of the following is MOST helpful to ensure effective security controls for a cloud service provider?

A. A control self-assessment
B. A third-party security assessment report
C. Internal audit reports from the vendor
D. Service level agreement monitoring

Answer: B

NEW QUESTION 201
- (Exam Topic 1)
Management has noticed storage costs have increased exponentially over the last 10 years because most users do not delete their emails. Which of the following can BEST alleviate this issue while not sacrificing security?

A. Implementing record retention tools and techniques
B. Establishing e-discovery and data loss prevention (DLP)
C. Sending notifications when near storage quota
D. Implementing a bring your own device 1BVOD) policy

Answer: A

NEW QUESTION 205
- (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 208
- (Exam Topic 2)
Which of the following is MOST important when discussing risk within an organization?

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

Answer: A

NEW QUESTION 210
- (Exam Topic 2)
To mitigate the risk of using a spreadsheet to analyze financial data, IT has engaged a third-party vendor to deploy a standard application to automate the process. Which of the following parties should own the risk associated with calculation errors?

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

Answer: D

NEW QUESTION 212
- (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 214
- (Exam Topic 2)
When reviewing a risk response strategy, senior management's PRIMARY focus should be placed on the:

A. cost-benefit analysis.
B. investment portfolio.
C. key performance indicators (KPIs).
D. alignment with risk appetite.

Answer: A

NEW QUESTION 216
- (Exam Topic 2)
Whose risk tolerance matters MOST when making a risk decision?

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

Answer: C

NEW QUESTION 218
- (Exam Topic 2)
Who is PRIMARILY accountable for risk treatment decisions?

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

Answer: B

NEW QUESTION 222
- (Exam Topic 2)
Which of the following is the PRIMARY responsibility of the first line of defense related to computer-enabled fraud?

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

Answer: C

NEW QUESTION 225
- (Exam Topic 2)
Which of the following will BEST help an organization evaluate the control environment of several third-party vendors?

A. Review vendors' internal risk assessments covering key risk and controls.
B. Obtain independent control reports from high-risk vendors.
C. Review vendors performance metrics on quality and delivery of processes.
D. Obtain vendor references from third parties.

Answer: B

NEW QUESTION 229
- (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 233
- (Exam Topic 2)
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: A

NEW QUESTION 234
- (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 237
- (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 238
- (Exam Topic 2)
Quantifying the value of a single asset helps the organization to understand the:

A. overall effectiveness of risk management
B. consequences of risk materializing
C. necessity of developing a risk strategy,
D. organization s risk threshold.

Answer: B

NEW QUESTION 243
- (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 248
- (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 249
- (Exam Topic 2)
Mapping open risk issues to an enterprise risk heat map BEST facilitates:

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

Answer: D

NEW QUESTION 252
- (Exam Topic 2)
Which of the following should be a risk practitioner's NEXT action after identifying a high probability of data loss in a system?

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

Answer: D

NEW QUESTION 254
- (Exam Topic 2)
An organization has decided to implement an emerging technology and incorporate the new capabilities into its strategic business plan. Business operations for the technology will be outsourced. What will be the risk practitioner's PRIMARY role during the change?

A. Managing third-party risk
B. Developing risk scenarios
C. Managing the threat landscape
D. Updating risk appetite

Answer: B

NEW QUESTION 256
- (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 257
- (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 258
- (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 259
- (Exam Topic 2)
When a high-risk security breach occurs, which of the following would be MOST important to the person responsible for managing the incident?

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

Answer: A

NEW QUESTION 260
- (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 264
- (Exam Topic 2)
Several network user accounts were recently created without the required management approvals. Which of the following would be the risk practitioner's BEST recommendation to address this situation?

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

Answer: C

NEW QUESTION 267
- (Exam Topic 2)
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: A

NEW QUESTION 270
- (Exam Topic 2)
Deviation from a mitigation action plan's completion date should be determined by which of the following?

A. Change management as determined by a change control board
B. Benchmarking analysis with similar completed projects
C. Project governance criteria as determined by the project office
D. The risk owner as determined by risk management processes

Answer: D

NEW QUESTION 271
- (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 272
- (Exam Topic 2)
An organization with a large number of applications wants to establish a security risk assessment program. Which of the following would provide the MOST useful information when determining the frequency of risk assessments?

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

Answer: D

NEW QUESTION 276
- (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 281
- (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 282
- (Exam Topic 2)
An upward trend in which of the following metrics should be of MOST concern?

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

Answer: C

NEW QUESTION 285
- (Exam Topic 2)
Which of the following is a detective control?

A. Limit check
B. Periodic access review
C. Access control software
D. Rerun procedures

Answer: B

NEW QUESTION 288
- (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 293
- (Exam Topic 2)
Which of the following BEST helps to balance the costs and benefits of managing IT risk?

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

Answer: A

NEW QUESTION 296
- (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: A

NEW QUESTION 297
- (Exam Topic 2)
Which of the following is a KEY responsibility of the second line of defense?

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

Answer: B

NEW QUESTION 299
- (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 304
- (Exam Topic 2)
Which of the following is MOST important to understand when developing key risk indicators (KRIs)?

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

Answer: A

NEW QUESTION 307
- (Exam Topic 2)
When updating a risk register with the results of an IT risk assessment, the risk practitioner should log:

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

Answer: D

NEW QUESTION 308
- (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 311
- (Exam Topic 2)
Which of the following should be included in a risk assessment report to BEST facilitate senior management's understanding of the results?

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

Answer: C

NEW QUESTION 313
- (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 316
- (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 319
- (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 323
- (Exam Topic 2)
An organization has decided to outsource a web application, and customer data will be stored in the vendor's public cloud. To protect customer data, it is MOST important to ensure which of the following?

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

Answer: D

NEW QUESTION 326
- (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 327
- (Exam Topic 2)
Which of the following BEST indicates the effectiveness of anti-malware software?

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

Answer: A

NEW QUESTION 329
- (Exam Topic 2)
A risk practitioner learns that the organization s industry is experiencing a trend of rising security incidents. Which of the following is the BEST course of action?

A. Evaluate the relevance of the evolving threats.
B. Review past internal audit results.
C. Respond to organizational security threats.
D. Research industry published studies.

Answer: A

NEW QUESTION 331
- (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 335
- (Exam Topic 2)
Following a significant change to a business process, a risk practitioner believes the associated risk has been reduced. The risk practitioner should advise the risk owner to FIRST

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

Answer: B

NEW QUESTION 340
- (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 344
- (Exam Topic 2)
An organization has completed a project to implement encryption on all databases that host customer data. Which of the following elements of the risk register should be updated the reflect this change?

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

Answer: B

NEW QUESTION 346
- (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 350
- (Exam Topic 2)
A risk practitioner is reviewing the status of an action plan to mitigate an emerging IT risk and finds the risk level has increased. The BEST course of action would be to:

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

Answer: D

NEW QUESTION 352
- (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 356
- (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 357
- (Exam Topic 2)
Which of the following is MOST important to ensure when continuously monitoring the performance of a client-facing application?

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

Answer: D

NEW QUESTION 358
- (Exam Topic 2)
Which of the following is the BEST way to support communication of emerging risk?

A. Update residual risk levels to reflect the expected risk impact.
B. Adjust inherent risk levels upward.
C. Include it on the next enterprise risk committee agenda.
D. Include it in the risk register for ongoing monitoring.

Answer: D

NEW QUESTION 359
- (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 363

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

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

Answer: D

NEW QUESTION 366
- (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 371
- (Exam Topic 2)
The MOST important reason to aggregate results from multiple risk assessments on interdependent information systems is to:

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

Answer: A

NEW QUESTION 372
.....

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