



Vendor: Isaca

Exam Code: CRISC

Exam Name: Certified in Risk and Information Systems
Control

Version: DEMO

QUESTION 1

Which of the following is the BEST recommendation of a risk practitioner for an organization that recently changed its organizational structure?

- A. Communicate the new risk profile.
- B. Implement a new risk assessment process.
- C. Revalidate the corporate risk appetite.
- D. Review and adjust key risk indicators (KRIs).

Answer: A

Explanation:

Communicating the new risk profile is the best recommendation for a risk practitioner for an organization that recently changed its organizational structure, because it helps to inform and align the stakeholders on the current state of risks and their implications for the organization's objectives and strategy. A risk profile is a summary of the key risks that an organization faces, along with their likelihood, impact, and response strategies. An organizational structure is the way that an organization arranges its people, roles, and responsibilities to achieve its goals and deliver its value proposition. A change in the organizational structure may affect the risk profile, as it may introduce new sources or types of risk, or alter the existing risk levels or responses. Therefore, communicating the new risk profile is the best recommendation, as it helps to ensure that the stakeholders are aware of and prepared for the changes and challenges that the new organizational structure may bring. Implementing a new risk assessment process, revalidating the corporate risk appetite, and reviewing and adjusting key risk indicators (KRIs) are all important tasks to perform after communicating the new risk profile, but they are not the best recommendation, as they depend on the communication and understanding of the new risk profile.

QUESTION 2

Which of the following is the BEST key performance indicator (KPI) to measure the effectiveness of a vulnerability management process?

- A. Percentage of vulnerabilities remediated within the agreed service level
- B. Number of vulnerabilities identified during the period
- C. Number of vulnerabilities re-opened during the period
- D. Percentage of vulnerabilities escalated to senior management

Answer: A

Explanation:

A vulnerability management process is a process that identifies, analyzes, prioritizes, and remediates the vulnerabilities in the IT systems and applications. The effectiveness of a vulnerability management process can be measured by the key performance indicators (KPIs) that reflect the achievement of the process objectives and the alignment with the enterprise's risk appetite and tolerance. The best KPI to measure the effectiveness of a vulnerability management process is the percentage of vulnerabilities remediated within the agreed service level. This KPI indicates how well the process is able to address the vulnerabilities in a timely and efficient manner, and reduce the exposure and impact of the risks associated with the vulnerabilities.

QUESTION 3

When a high-risk security breach occurs, which of the following would be MOST important to the person responsible for managing the incident?

- A. An analysis of the security logs that illustrate the sequence of events

- B. An analysis of the impact of similar attacks in other organizations
- C. A business case for implementing stronger logical access controls
- D. A justification of corrective action taken

Answer: A

Explanation:

An analysis of the security logs that illustrate the sequence of events is the most important information for the person responsible for managing the incident, as it can help to identify the source, scope, and impact of the security breach, and to determine the appropriate response actions. An analysis of the security logs can also provide evidence for forensic investigation and legal action, and help to prevent or mitigate future incidents by identifying the root causes and vulnerabilities.

QUESTION 4

A hospital recently implemented a new technology to allow virtual patient appointments. Which of the following should be the risk practitioner's FIRST course of action?

- A. Reassess the risk profile.
- B. Modify the risk taxonomy.
- C. Increase the risk tolerance.
- D. Review the risk culture.

Answer: A

Explanation:

Reassessing the risk profile is the first course of action that a risk practitioner should take after a hospital recently implemented a new technology to allow virtual patient appointments. This is because reassessing the risk profile can help identify, analyze, and evaluate the new or changed risks that the new technology may introduce or affect, such as data privacy, security, quality, reliability, or compliance risks. Reassessing the risk profile can also help determine the appropriate risk response and mitigation strategies, as well as monitor and report the risk performance and outcomes. According to the CRISC Review Manual 2022, reassessing the risk profile is one of the key steps in the IT risk management process. According to the web search results, reassessing the risk profile is a common and recommended practice for addressing the risks of virtual patient appointments.

QUESTION 5

Which of the following provides the MOST mitigation value for an organization implementing new Internet of Things (IoT) devices?

- A. Performing a vulnerability assessment on the IoT devices
- B. Designing IoT architecture with IT security controls from the start
- C. Implementing key risk indicators (KRIs) for IoT devices
- D. To ensure risk trend data is collected and reported

Answer: B

QUESTION 6

Which of the following is the BEST method of creating risk awareness in an organization?

- A. Marking the risk register available to project stakeholders
- B. Ensuring senior management commitment to risk training

- C. Providing regular communication to risk managers
- D. Appointing the risk manager from the business units

Answer: B

Explanation:

The best method of creating risk awareness in an organization is to ensure senior management commitment to risk training. Senior management plays a vital role in setting the tone and direction of the risk culture and governance in the organization. By demonstrating their support and participation in risk training, they can influence and motivate the employees to follow the risk policies and procedures, and to enhance their risk knowledge and skills. Marking the risk register available to project stakeholders, providing regular communication to risk managers, and appointing the risk manager from the business units are other methods of creating risk awareness, but they are not as effective as ensuring senior management commitment to risk training.

QUESTION 7

Which of the following proposed benefits is MOST likely to influence senior management approval to reallocate budget for a new security initiative?

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

Answer: C

Explanation:

The proposed benefit that is most likely to influence senior management approval to reallocate budget for a new security initiative is the reduction in residual risk, as it indicates the expected value and outcome of the initiative in terms of reducing the risk exposure and impact to the level that is aligned with the risk tolerance and appetite of the organization.

QUESTION 8

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

Explanation:

Annual loss expectancy (ALE) is a method to assign a monetary value to risk by multiplying the probability of a risk event by the potential loss associated with that event. ALE can be used to compare the costs and benefits of different risk mitigation options and to determine the optimal level of investment in risk management. Business impact analysis (BIA) is a process to identify and evaluate the potential effects of a disruption on the critical functions and processes of an organization. BIA can help to forecast the impacts of a risk event, but it does not assign a monetary value to the risk itself. Cost-benefit analysis (CBA) is a technique to compare the costs and benefits of a project, decision, or action. CBA can help to evaluate the feasibility and profitability of a risk mitigation option, but it does not assign a monetary value to the risk itself. Inherent vulnerabilities are the weaknesses or flaws in a system, process, or asset that expose it to potential threats. Inherent vulnerabilities can increase the likelihood or impact of a risk event,

but they do not assign a monetary value to the risk itself.

QUESTION 9

Which of the following scenarios represents a threat?

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

Answer: D

Explanation:

A virus transmitted on a USB thumb drive is a scenario that represents a threat, as it involves a malicious or harmful event that could compromise the confidentiality, integrity, or availability of an information system. A virus is a type of malware that can infect and damage files, programs, or devices by replicating itself and spreading to other systems or networks. A USB thumb drive is a portable storage device that can be used to transfer data between computers or devices. A virus transmitted on a USB thumb drive can occur when a user inserts an infected USB thumb drive into a computer or device, or when a user downloads or copies an infected file from a USB thumb drive to a computer or device. A virus transmitted on a USB thumb drive can pose a serious risk to the information system, as it can corrupt or delete data, disrupt or degrade performance, steal or leak information, or allow unauthorized access or control.

QUESTION 10

A risk practitioner is performing a risk assessment of recent external advancements in quantum computing. Which of the following would pose the GREATEST concern for the risk practitioner?

- A. The organization has incorporated blockchain technology in its operations.
- B. The organization has not reviewed its encryption standards.
- C. The organization has implemented heuristics on its network firewall.
- D. The organization has not adopted Infrastructure as a Service (IaaS) for its operations.

Answer: B

QUESTION 11

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

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

Answer: B

Explanation:

The business process owner is the stakeholder who is responsible for the business process that is supported by the IT system, such as the CRM system. The business process owner has the authority and accountability to manage the risk and its response associated with the business process and the IT system. The business process owner should own the risk of customer data leakage caused by insufficient IT security controls for the new system, as it directly affects the

performance, functionality, and compliance of the business process.

QUESTION 12

A recent regulatory requirement has the potential to affect an organization's use of a third party to supply outsourced business services. Which of the following is the BEST course of action?

- A. Conduct a gap analysis.
- B. Terminate the outsourcing agreement.
- C. Identify compensating controls.
- D. Transfer risk to the third party.

Answer: A

Explanation:

The best course of action when a recent regulatory requirement has the potential to affect an organization's use of a third party to supply outsourced business services is to conduct a gap analysis, as it involves comparing the current and desired states of compliance, and identifying any gaps or discrepancies that need to be addressed. Terminating the outsourcing agreement, identifying compensating controls, and transferring risk to the third party are not the best courses of action, as they may not be feasible, effective, or appropriate, respectively, and may require the prior knowledge of the compliance gaps and risks.

QUESTION 13

The PRIMARY advantage of involving end users in continuity planning is that they:

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

Answer: A

Explanation:

Continuity planning is the process of developing strategies and plans to ensure the continuity of critical business functions and processes in the event of a disruption or disaster. Continuity planning involves identifying the risks, impacts, and recovery options for various scenarios, as well as testing and updating the plans regularly. The primary advantage of involving end users in continuity planning is that they have a better understanding of specific business needs, such as the operational requirements, the customer expectations, and the dependencies and interdependencies of the business processes. End users can provide valuable input and feedback on the continuity plans, as well as participate in the testing and validation of the plans. End users can also help to ensure the alignment of the continuity plans with the business objectives and priorities, as well as the compliance with the relevant standards and regulations.

QUESTION 14

A user has contacted the risk practitioner regarding malware spreading laterally across the organization's corporate network. Which of the following is the risk practitioner's BEST course of action?

- A. Review all log files generated during the period of malicious activity.
- B. Perform a root cause analysis.
- C. Notify the cybersecurity incident response team.
- D. Update the risk register.

Answer: C

Explanation:

Notifying the incident response team ensures immediate action to contain and remediate the malware spread, limiting further impact. This aligns with Incident Response and Containment protocols under risk management.

QUESTION 15

After the implementation of internal of Things (IoT) devices, new risk scenarios were identified. What is the PRIMARY reason to report this information to risk owners?

- A. To reevaluate continued use to IoT devices
- B. The add new controls to mitigate the risk
- C. The recommend changes to the IoT policy
- D. To confirm the impact to the risk profile

Answer: D

Explanation:

The primary reason to report the information about the new risk scenarios identified after the implementation of Internet of Things (IoT) devices to risk owners is to confirm the impact to the risk profile. The risk profile is a summary of the level and nature of the risks that the organization faces or may face in the future. The risk profile reflects the risk appetite, tolerance, and capacity of the organization, and guides the risk management decisions and actions. The implementation of IoT devices may introduce new risks or increase the likelihood or impact of existing risks, such as data privacy, security, or interoperability issues. Therefore, the information about the new risk scenarios should be reported to the risk owners, who have the authority and responsibility for managing the risks and their responses, to confirm the impact to the risk profile and to determine the appropriate risk treatment plans.

QUESTION 16

The percentage of unpatched systems is a:

- A. threat vector.
- B. critical success factor (CSF).
- C. key performance indicator (KPI).
- D. key risk indicator (KRI).

Answer: D

Explanation:

The percentage of unpatched systems is best classified as a Key Risk Indicator (KRI). KRIs are metrics used by organizations to provide an early signal of increasing risk exposures in various areas of the business. Here's a

Understanding KRIs:

Definition: KRIs are specific metrics that provide insights into the risk level of an organization. They help in identifying potential risks that could impact the business negatively if not addressed promptly.

Purpose: KRIs are used to monitor the effectiveness of risk management strategies and to provide an early warning system for emerging risks.

Percentage of Unpatched Systems as a KRI:

Indicator of Vulnerability: The percentage of unpatched systems directly indicates how vulnerable an organization is to cyber threats. Unpatched systems are a common entry point for attackers, making this metric critical for assessing the organization's exposure to cyber risks.

Impact on Security Posture: A high percentage of unpatched systems can significantly increase

the likelihood of security incidents, making it a valuable metric for risk management.

Proactive Risk Management: By monitoring this KRI, organizations can take proactive measures to address vulnerabilities before they are exploited.

QUESTION 17

Which of the following is the BEST course of action when an organization wants to reduce likelihood in order to reduce a risk level?

- A. Monitor riskcontrols.
- B. Implement preventive measures.
- C. Implement detective controls.
- D. Transfer the risk.

Answer: B

Explanation:

The best course of action when an organization wants to reduce likelihood in order to reduce a risk level is to implement preventive measures. Likelihood is the probability or chance of a risk occurring, and risk level is the combination of likelihood and impact of a risk. Preventive measures are controls that are designed to prevent or deter the occurrence of a risk, such as policies, standards, procedures, guidelines, etc. Implementing preventive measures is the best course of action, because it helps to reduce the likelihood of a risk, and consequently, the risk level. Implementing preventive measures also helps to protect and enhance the organization's objectives, performance, and improvement.

QUESTION 18

Which of the following is the BEST way to manage the risk associated with malicious activities performed by database administrators (DBAs)?

- A. Activity logging and monitoring
- B. Periodic access review
- C. Two-factor authentication
- D. Awareness training and background checks

Answer: A

Explanation:

According to the CRISC Review Manual, activity logging and monitoring is the best way to manage the risk associated with malicious activities performed by database administrators (DBAs), because it enables the detection and prevention of unauthorized or inappropriate actions on the database. Activity logging and monitoring involves capturing and reviewing the activities of the DBAs, such as the commands executed, the data accessed or modified, the privileges used, and the time and duration of the sessions. Activity logging and monitoring can also provide an audit trail for accountability and forensic purposes.

QUESTION 19

To help identify high-risk situations, an organization should:

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

Answer: A

Explanation:

To help identify high-risk situations, an organization should continuously monitor the environment, as it can help to detect and respond to any changes or emerging risks that may affect the organization's objectives and strategy. Continuous monitoring can also provide timely and relevant feedback and information to the decision-makers and stakeholders, and enable them to adjust the risk strategy and response actions accordingly. Continuous monitoring can also help to ensure that the risk management process is aligned with the organization's risk appetite and tolerance, and supports the achievement of the organization's goals and value creation.

QUESTION 20

Which of the following offers the SIMPLEST overview of changes in an organization's risk profile?

- A. A risk roadmap
- B. A balanced scorecard
- C. A heat map
- D. The risk register

Answer: C

Explanation:

A heat map is a graphical representation of the organization's risk profile that shows the relative level of risk for each risk category or event. A heat map uses colors, shapes, or symbols to indicate the magnitude and likelihood of each risk, as well as its trend and status. A heat map offers the simplest overview of changes in the organization's risk profile, as it allows the risk decision-makers to quickly identify the most significant risks, the areas of improvement or deterioration, and the gaps or overlaps in risk management. A heat map can also be used to communicate the risk profile to senior management and other stakeholders in a clear and concise manner.

QUESTION 21

Which of the following key performance indicators (KPIs) would BEST measure the risk of a service outage when using a Software as a Service (SaaS) vendors

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

Answer: C

Explanation:

Software as a Service (SaaS) is a cloud computing model that provides software applications over the internet, without requiring the users to install or maintain them on their own devices. SaaS vendors are responsible for hosting, managing, and updating the software applications, and providing technical support and security to the users. The key performance indicator (KPI) that would best measure the risk of a service outage when using a SaaS vendor is the frequency and duration of unplanned downtime, which is the amount and length of time that the software applications are unavailable or inaccessible due to unexpected events, such as network failures, server crashes, power outages, cyberattacks, etc. The frequency and duration of unplanned downtime indicate the reliability and availability of the SaaS vendor, and the potential impact of the service outage on the users' business operations and productivity.

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

- ★ More than **99,900** Satisfied Customers Worldwide.
- ★ Average **99.9%** Success Rate.
- ★ **Free Update** to match latest and real exam scenarios.
- ★ **Instant Download** Access! No Setup required.
- ★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.
- ★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.
- ★ **100%** Guaranteed Success or **100%** Money Back Guarantee.
- ★ **Fast**, helpful support **24x7**.



View list of all certification exams: <http://www.lead2pass.com/all-products.html>



10% Discount Coupon Code: ASTR14