Isaca

Exam Questions CISM

Certified Information Security Manager

NEW QUESTION 1
Which of the following BEST facilitates an information security manager's efforts to obtain senior management commitment for an information security program?

A. Presenting evidence of inherent risk
B. Reporting the security maturity level
C. Presenting compliance requirements
D. Communicating the residual risk

Answer: C

NEW QUESTION 2
An organization needs to comply with new security incident response requirements. Which of the following should the information security manager do FIRST?

A. Create a business case for a new incident response plan.
B. Revise the existing incident response plan.
C. Conduct a gap analysis.
D. Assess the impact to the budget,

Answer: C

NEW QUESTION 3
Which of the following BEST indicates that an organization has effectively tested its business continuity and disaster recovery plans within the stated recovery time objectives (RTOs)?

A. Regulatory requirements are being met.
B. Internal compliance requirements are being met.
C. Risk management objectives are being met.
D. Business needs are being met.

Answer: D

NEW QUESTION 4
Which of the following is the responsibility of a risk owner?

A. Performing risk assessments to direct risk response
B. Determining the organization's risk appetite
C. Ensuring control effectiveness is monitored
D. Implementing controls to mitigate the risk

Answer: D

Explanation:
A risk owner is a person or entity that is responsible for ensuring that risk is managed effectively. One of the primary responsibilities of a risk owner is to implement controls that will help mitigate or manage the risk. While risk assessments, determining the organization's risk appetite, and monitoring control effectiveness are all important aspects of managing risk, it is the responsibility of the risk owner to take the necessary actions to manage the risk.

NEW QUESTION 5
An information security manager learns that IT personnel are not adhering to the information security policy because it creates process inefficiencies. What should the information security manager do FIRST?

A. Conduct user awareness training within the IT function.
B. Propose that IT update information security policies and procedures.
C. Determine the risk related to noncompliance with the policy.
D. Request that internal audit conduct a review of the policy development process,

Answer: C

NEW QUESTION 6
Which of the following risk scenarios is MOST likely to emerge from a supply chain attack?

A. Compromise of critical assets via third-party resources
B. Unavailability of services provided by a supplier
C. Loss of customers due to unavailability of products
D. Unreliable delivery of hardware and software resources by a supplier

Answer: C

NEW QUESTION 7
Which of the following is the BEST approach to make strategic information security decisions?

A. Establish regular information security status reporting.
B. Establish an information security steering committee.
C. Establish business unit security working groups.
D. Establish periodic senior management meetings.

Answer: B

Explanation:
An Information Security Steering Committee is a group of stakeholders responsible for providing governance and guidance to the organization on all matters related to information security. The committee provides oversight and guidance on security policies, strategies, and technology implementation. It also ensures that the organization is in compliance with relevant laws and regulations. Additionally, it serves as a forum for discussing security-related issues and ensures that security is taken into account when making strategic decisions.

NEW QUESTION 8
When developing an asset classification program, which of the following steps should be completed FIRST?

A. Categorize each asset.
B. Create an inventor
C. &
D. Create a business case for a digital rights management tool.
E. Implement a data loss prevention (OLP) system.

Answer: B

NEW QUESTION 9
Which of the following is the MOST effective way to demonstrate alignment of information security strategy with business objectives?

A. Balanced scorecard
B. Risk matrix
C. Benchmarking
D. Heat map

Answer: A

Explanation:
The balanced scorecard is a management tool that can be used to demonstrate the alignment of information security strategy with business objectives. The balanced scorecard provides a comprehensive view of an organization's performance by considering multiple dimensions, including financial performance, customer satisfaction, internal processes, and learning and growth.
By integrating information security objectives and metrics into the balanced scorecard, organizations can demonstrate how their information security investments support and align with their overall business objectives. This can help to gain the support and commitment of senior management and other stakeholders, as well as ensure that information security investments are effectively managed and optimized to deliver maximum value to the organization.
While other tools, such as risk matrices, benchmarking, and heat maps, can also provide valuable information, the balanced scorecard provides a more holistic and integrated view of organizational performance and the alignment of information security with business objectives.

NEW QUESTION 10
Which of the following is the sole responsibility of the client organization when adopting a Software as a Service (SaaS) model?

A. Host patching
B. Penetration testing
C. Infrastructure hardening
D. Data classification

Answer: D

NEW QUESTION 10
An information security manager is reporting on open items from the risk register to senior management. Which of the following is MOST important to communicate with regard to these risks?

A. Responsible entities
B. Key risk indicators (KRIS)
C. Compensating controls
D. Potential business impact

Answer: D

NEW QUESTION 12
The PRIMARY benefit of introducing a single point of administration in network monitoring is that it:

A. reduces unauthorized access to systems.
B. promotes efficiency in control of the environment.
C. prevents inconsistencies in information in the distributed environment.
D. allows administrative staff to make management decisions.

Answer: D

NEW QUESTION 14
Which of the following is the BEST way to assess the risk associated with using a Software as a Service (SaaS) vendor?

A. Verify that information security requirements are included in the contract.
B. Request customer references from the vendor.
C. Require vendors to complete information security questionnaires.

D. Review the results of the vendor's independent control reports.

Answer: A

NEW QUESTION 18
An organization's HR department requires that employee account privileges be removed from all corporate IT systems within three days of termination to comply with a government regulation However, the systems all have different user directories, and it currently takes up to four weeks to remove the privileges Which of the following would BEST enable regulatory compliance?

A. Multi-factor authentication (MFA) system
B. Identity and access management (IAM) system
C. Privileged access management (PAM) system
D. Governance, risk, and compliance (GRC) system

Answer: C

Explanation:
The best option for enabling regulatory compliance in this situation is a Privileged Access Management (PAM) system. A PAM system allows organizations to centrally manage user access and privileges across different systems, making it easier to remove user privileges within the required timeframe. Additionally, a PAM system can also help to ensure that user access remains secure, reducing the risk of unauthorized access and ensuring regulatory compliance.

NEW QUESTION 22
The MOST important reason for having an information security manager serve on the change management committee is to:

A. identify changes to the information security policy.
B. ensure that changes are tested.
C. ensure changes are properly documented.
D. advise on change-related risk.

Answer: D

NEW QUESTION 24
Which of the following is MOST helpful for determining which information security policies should be implemented by an organization?

A. Risk assessment
B. Business impact analysis (BIA)
C. Vulnerability assessment
D. Industry best practices

Answer: A

NEW QUESTION 29
In order to understand an organization's security posture, it is MOST important for an organization's senior leadership to:

A. evaluate results of the most recent incident response test.
B. review the number of reported security incidents.
C. ensure established security metrics are reported.
D. assess progress of risk mitigation efforts.

Answer: C

NEW QUESTION 30
An organization finds it necessary to quickly shift to a work-fromhome model with an increased need for remote access security.
Which of the following should be given immediate focus?

A. Moving to a zero trust access model
B. Enabling network-level authentication
C. Enhancing cyber response capability
D. Strengthening endpoint security

Answer: D

NEW QUESTION 35
Which of the following is the BEST way to reduce the risk associated with a bring your own device (BYOD) program?

A. Provide employee training on secure mobile device practices
B. Implement a mobile device management (MDM) solution.
C. Require employees to install an effective anti-malware app.
D. Implement a mobile device policy and standard.

Answer: B

Explanation:
The best way to reduce the risk associated with a bring your own device (BYOD) program is to implement a mobile device policy and standard. This policy should include guidelines and rules regarding the use of mobile devices, such as acceptable use guidelines and restrictions on the types of data that can be stored or accessed on the device. Additionally, it should also include requirements for secure mobile device practices, such as the use of strong passwords, encryption, and

regular patching. A mobile device management (MDM) solution can also be implemented to help ensure mobile devices meet the organizational security requirements. However, it is not enough to simply implement the policy and MDM solution; employees must also be trained on the secure mobile device practices to ensure the policy is followed.

NEW QUESTION 36
A balanced scorecard MOST effectively enables information security:

A. risk management
B. project management
C. governance
D. performance

Answer: C

Explanation:
A balanced scorecard enables information security governance by providing a framework for aligning security objectives with business goals and measuring performance against them. The other choices are not directly related to governance but may be supported by it.
A balanced scorecard is a strategic management tool that describes the cause-and-effect linkages between four high-level perspectives of strategy and execution: financial, customer, internal process, and learning and growth2. It helps organizations communicate and monitor their vision and strategy across different levels and functions2.

NEW QUESTION 39
Which of the following change management procedures is MOST likely to cause concern to the information security manager?
A. Fallback processes are tested the weekend before changes are made
B. Users are not notified of scheduled system changes
C. A manual rather than an automated process is used to compare program versions.
D. The development manager migrates programs into production

Answer: D

Explanation:
According to the Certified Information Security Manager (CISM) Study Guide, one of the primary responsibilities of an information security manager is to ensure that changes to systems and processes are managed in a secure and controlled manner. The change management procedure that is most likely to cause concern for an information security manager is when the development manager migrates programs into production without proper oversight or control. This can increase the risk of unauthorized changes being made to systems and data, and can also increase the risk of configuration errors or other issues that can negatively impact the security and availability of systems. To mitigate these risks, it is important for the information security manager to work closely with the development team to establish and enforce change management procedures that ensure that all changes are properly approved, tested, and implemented in a controlled manner.

NEW QUESTION 42
Which of the following BEST indicates that information assets are classified accurately?

A. Appropriate prioritization of information risk treatment
B. Increased compliance with information security policy
C. Appropriate assignment of information asset owners
D. An accurate and complete information asset catalog

Answer: A

NEW QUESTION 43
An organization's quality process can BEST support security management by providing:
A. security configuration controls.
B. assurance that security requirements are met.
C. guidance for security strategy.
D. a repository for security systems documentation.

Answer: B

Explanation:
An organization's quality process can BEST support security management by providing assurance that security requirements are met. This means that the quality process can be used to ensure that security controls are being implemented as intended and that they are achieving the desired results. This helps to ensure that the organization is properly protected and that it is in compliance with security regulations and standards.

NEW QUESTION 48
Which of the following should be the PRIMARY consideration when developing an incident response plan?

A. The definition of an incident
B. Compliance with regulations
C. Management support
D. Previously reported incidents

Answer: B

NEW QUESTION 53
An organization plans to utilize Software as a Service (SaaS) and is in the process of selecting a vendor. What should the information security manager do FIRST

to support this initiative?

A. Review independent security assessment reports for each vendor.
B. Benchmark each vendor's services with industry best practices.
C. Analyze the risks and propose mitigating controls.
D. Define information security requirements and processes.

Answer: A

NEW QUESTION 55
Which of the following is the BEST way for an organization to ensure that incident response teams are properly prepared?

A. Providing training from third-party forensics firms
B. Obtaining industry certifications for the response team
C. Conducting tabletop exercises appropriate for the organization
D. Documenting multiple scenarios for the organization and response steps

Answer: C

Explanation:
The BEST way for an organization to ensure that incident response teams are properly prepared is by conducting tabletop exercises appropriate for the organization.
Tabletop exercises are an effective way to test and validate an organization's incident response plan (IRP) and the readiness of the incident response team. These exercises simulate different scenarios in a controlled environment and allow the team to practice their response procedures, identify gaps, and make improvements to the plan. By conducting regular tabletop exercises, the incident response team can stay current with changes in the threat landscape and ensure that they are prepared to respond to incidents effectively.
According to the Certified Information Security Manager (CISM) Study Manual, "Tabletop exercises are a valuable tool for testing and validating the effectiveness of the IRP and the readiness of the incident response team. These exercises simulate different scenarios in a controlled environment and allow the team to practice their response procedures, identify gaps, and make improvements to the plan."
While providing training from third-party forensics firms, obtaining industry certifications, and documenting multiple scenarios for the organization and response steps can all be useful in preparing incident response teams, they are not as effective as conducting tabletop exercises appropriate for the organization.

NEW QUESTION 59
Which of the following is the BEST indication of an effective information security awareness training program?

A. An increase in the frequency of phishing tests
B. An increase in positive user feedback
C. An increase in the speed of incident resolution
D. An increase in the identification rate during phishing simulations

Answer: D

NEW QUESTION 63
An organization plans to offer clients a new service that is subject to regulations. What should the organization do FIRST when developing a security strategy in support of this new service?

A. Determine security controls for the new service.
B. Establish a compliance program,
C. Perform a gap analysis against the current state
D. Hire new resources to support the service.

Answer: C

NEW QUESTION 64
When performing a business impact analysis (BIA), who should calculate the recovery time and cost estimates?

A. Business process owner
B. Business continuity coordinator
C. Senior management
D. Information security manager

Answer: A

NEW QUESTION 67
When remote access to confidential information is granted to a vendor for analytic purposes, which of the following is the MOST important security consideration?

A. Data is encrypted in transit and at rest at the vendor site.
B. Data is subject to regular access log review.
C. The vendor must be able to amend data.
D. The vendor must agree to the organization's information security policy,

Answer: D

NEW QUESTION 70
Which of the following should be the MOST important consideration when establishing information security policies for an organization?

A. Job descriptions include requirements to read security policies.

B. The policies are updated annually.
C. Senior management supports the policies.
D. The policies are aligned to industry best practices.

Answer: C

NEW QUESTION 75
Which of the following BEST ensures information security governance is aligned with corporate governance?

A. A security steering committee including IT representation
B. A consistent risk management approach
C. An information security risk register
D. Integration of security reporting into corporate reporting

Answer: D

NEW QUESTION 78
Which of the following is PRIMARILY determined by asset classification?

A. Insurance coverage required for assets
B. Level of protection required for assets
C. Priority for asset replacement
D. Replacement cost of assets

Answer: B

NEW QUESTION 80
Which of the following is MOST important to convey to employees in building a security risk-aware culture?

A. Personal information requires different security controls than sensitive information.
B. Employee access should be based on the principle of least privilege.
C. Understanding an information asset's value is critical to risk management.
D. The responsibility for security rests with all employees.

Answer: D

Explanation:
In building a security risk-aware culture, it is most important to convey to employees that the responsibility for security rests with all employees. Every employee plays a role in ensuring the security of the organization's information assets, and it is essential that they understand their role and take security seriously. This means not only following security policies and procedures but also being vigilant in identifying and reporting potential security incidents.
The other items listed (personal information requiring different security controls than sensitive information, employee access should be based on the principle of least privilege, and understanding an information asset's value is critical to risk management) are all important elements of a comprehensive security program, but they are secondary to the fundamental message that security is a shared responsibility. By emphasizing this message and empowering employees to take an active role in security, organizations can build a stronger, more effective security risk-aware culture.

NEW QUESTION 83
Which of the following is MOST effective for communicating forward-looking trends within security reporting?

A. Key control indicator (KCIs)
B. Key risk indicators (KRIs)
C. Key performance indicators (KPIs)
D. Key goal indicators (KGIs)

Answer: C

Explanation:
Key performance indicators (KPIs) are the most effective for communicating forward-looking trends within security reporting. KPIs are metrics used to measure progress towards a specific goal or objective, and can provide insight into the current state of security and any potential issues or risks that may arise in the future. Key control indicators (KCIs), key risk indicators (KRIs), and key goal indicators (KGIs) are all important for measuring security performance and identifying areas for improvement, but KPIs are the most effective for communicating forward-looking trends.
References that support this statement include:

- "Key Performance Indicators (KPIs) for IT Security" by ISACA. This resource states that KPIs "can be used to measure the performance of security controls and identify trends in security risks."
- "Measuring and Managing Information Risk: A FAIR Approach" by The Open Group. This guide states that "KPIs are used to track progress over time and to identify areas where improvements may be needed."
- "Key Performance Indicators (KPIs) for Cyber Security" by SANS Institute. This resource states that "KPIs can be used to identify potential risks and measure the effectiveness of security controls.

NEW QUESTION 85
Which of the following tasks should be performed once a disaster recovery plan (DRP) has been developed?

A. Develop the test plan.
B. Analyze the business impact.
C. Define response team roles.
D. Identify recovery time objectives (RTOs).

Answer: A

NEW QUESTION 90
Which of the following has The GREATEST positive impact on The ability to execute a disaster recovery plan (DRP)?

A. Storing the plan at an offsite location
B. Communicating the plan to all stakeholders
C. Updating the plan periodically
D. Conducting a walk-through of the plan

Answer: C

Explanation:
Updating the plan periodically has the greatest positive impact on the ability to execute a disaster recovery plan (DRP). This is because an up-to-date plan is more likely to reflect the current environment, and any potential risks or issues can be addressed before an emergency arises. Storing the plan at an offsite location, communicating the plan to all stakeholders, and conducting a walk-through of the plan are all important steps, but they do not have the same impact as regularly updating the DRP.

NEW QUESTION 95
Which of the following is the PRIMARY benefit of implementing a vulnerability assessment process?

A. Threat management is enhanced.
B. Compliance status is improved.
C. Security metrics are enhanced.
D. Proactive risk management is facilitated.

Answer: A

NEW QUESTION 96
Which of the following has the MOST influence on the inherent risk of an information asset?

A. Risk tolerance
B. Net present value (NPV)
C. Return on investment (ROI)
D. Business criticality

Answer: D

Explanation:
Business criticality is the degree to which an asset is essential to the success of the business and the extent to which its loss or compromise could have a significant impact on the business. Business criticality is one of the main factors that help to determine the inherent risk of an asset, as assets that are more critical to the business tend to have a higher inherent risk.

NEW QUESTION 98
Which of the following should be given the HIGHEST priority during an information security post-incident review?

A. Documenting actions taken in sufficient detail
B. Updating key risk indicators (KRIs)
C. Evaluating the performance of incident response team members
D. Evaluating incident response effectiveness

Answer: D

Explanation:
During post-incident reviews, the highest priority should be given to evaluating the effectiveness of the incident response effort. This includes assessing the accuracy of the response to the incident, the timeliness of the response, and the efficiency of the response. It is important to assess the effectiveness of the response in order to identify areas for improvement and ensure that future responses can be more effective. Documenting the actions taken in sufficient detail, updating key risk indicators (KRIs), and evaluating the performance of incident response team members are all important components of a post-incident review, but evaluating incident response effectiveness should be given the highest priority.

NEW QUESTION 102
Which of the following is the BEST course of action when an online company discovers a network attack in progress?

A. Dump all event logs to removable media
B. Isolate the affected network segment
C. Enable trace logging on ail events
D. Shut off all network access points

Answer: B

Explanation:
The BEST course of action when an online company discovers a network attack in progress is to isolate the affected network segment. This prevents the attacker from gaining further access to the network and limits the scope of the attack. Dumping event logs to removable media and enabling trace logging may be useful for forensic purposes, but should not be the first course of action in the midst of an active attack. Shutting off all network access points would be too drastic and would prevent legitimate traffic from accessing the network.

NEW QUESTION 104
Which of the following service offerings in a typical Infrastructure as a Service (laaS) model will BEST enable a cloud service provider to assist customers when

recovering from a security incident?

A. Availability of web application firewall logs.
B. Capability of online virtual machine analysis
C. Availability of current infrastructure documentation
D. Capability to take a snapshot of virtual machines

Answer: D

NEW QUESTION 105
Which of the following provides an information security manager with the MOST accurate indication of the organization's ability to respond to a cyber attack?

A. Walk-through of the incident response plan
B. Black box penetration test
C. Simulated phishing exercise
D. Red team exercise

Answer: D

NEW QUESTION 106
Which of the following is MOST helpful in determining an organization's current capacity to mitigate risks?

A. Capability maturity model
B. Vulnerability assessment
C. IT security risk and exposure
D. Business impact analysis (BIA)

Answer: A

NEW QUESTION 109
Which of the following is MOST important in increasing the effectiveness of incident responders?

A. Communicating with the management team
B. Integrating staff with the IT department
C. Testing response scenarios
D. Reviewing the incident response plan annually

Answer: C

NEW QUESTION 113
Which of the following is the MOST important requirement for a successful security program?

A. Mapping security processes to baseline security standards
B. Penetration testing on key systems
C. Management decision on asset value
D. Nondisclosure agreements (NDA) with employees

Answer: C

Explanation:
“A successful security program requires management support and involvement. One of the key aspects of management support is to decide on the value of assets and the acceptable level of risk for them. This will help define the security objectives and priorities for the program. The other options are possible activities within a security program, but they are not as important as management decision on asset value.”

NEW QUESTION 118
Of the following, who is in the BEST position to evaluate business impacts?

A. Senior management
B. Information security manager
C. IT manager
D. Process manager

Answer: D

NEW QUESTION 119
An intrusion has been detected and contained. Which of the following steps represents the BEST practice for ensuring the integrity of the recovered system?

A. Install the OS, patches, and application from the original source.
B. Restore the OS, patches, and application from a backup.
C. Restore the application and data from a forensic copy.
D. Remove all signs of the intrusion from the OS and application.

Answer: B

Explanation:
The BEST practice for ensuring the integrity of the recovered system after an intrusion is to restore the OS, patches, and application from a backup. This will

ensure that the system is in a known good state, without any potential residual malicious code or changes from the intrusion. Restoring from a backup also enables the organization to revert to a previous configuration that has been tested and known to be secure. This step should be taken prior to conducting a thorough investigation and forensic analysis to determine the cause and extent of the intrusion.

NEW QUESTION 120
An organization is creating a risk mitigation plan that considers redundant power supplies to reduce the business risk associated with critical system outages. Which type of control is being considered?

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

Answer: A

NEW QUESTION 124
To support effective risk decision making, which of the following is MOST important to have in place?

A. Established risk domains
B. Risk reporting procedures
C. An audit committee consisting of mid-level management
D. Well-defined and approved controls

Answer: A

Explanation:
Established risk domains are important for effective risk decision making because they provide a basis for categorizing risks and assessing their impact on the organization. Risk domains are also used to assign risk ownership and prioritize risk management activities. Having established risk domains in place helps ensure that risks are properly identified and addressed, and enables organizations to make informed and effective decisions about risk. Risk reporting procedures, an audit committee consisting of mid-level management, and well-defined and approved controls are all important components of an effective risk management program, but established risk domains are the most important for effective risk decision making.

NEW QUESTION 125
Which of the following is a desired outcome of information security governance?

A. Penetration test
B. Improved risk management
C. Business agility
D. A maturity model

Answer: B

NEW QUESTION 130
A PRIMARY purpose of creating security policies is to:

A. define allowable security boundaries.
B. communicate management's security expectations.
C. establish the way security tasks should be executed.
D. implement management's security governance strategy.

Answer: B

NEW QUESTION 131
Which of the following messages would be MOST effective in obtaining senior management's commitment to information security management?

A. Effective security eliminates risk to the business.
B. Adopt a recognized framework with metrics.
C. Security is a business product and not a process.
D. Security supports and protects the business.

Answer: D

NEW QUESTION 135
In which cloud model does the cloud service buyer assume the MOST security responsibility?

A. Disaster Recovery as a Service (DRaaS)
B. Infrastructure as a Service (IaaS)
C. Platform as a Service (PaaS)
D. Software as a Service (SaaS)

Answer: B

NEW QUESTION 138
Which of the following is the BEST approach for governing noncompliance with security requirements?

A. Base mandatory review and exception approvals on residual risk,
B. Require users to acknowledge the acceptable use policy.
C. Require the steering committee to review exception requests.
D. Base mandatory review and exception approvals on inherent risk.

Answer: C

NEW QUESTION 141
The BEST way to identify the risk associated with a social engineering attack is to:

A. monitor the intrusion detection system (IDS),
B. review single sign-on (SSO) authentication lags.
C. test user knowledge of information security practices.
D. perform a business risk assessment of the email filtering system.

Answer: C

NEW QUESTION 142
An incident management team is alerted ta a suspected security event. Before classifying the suspected event as a security incident, it is MOST important for the security manager to:

A. notify the business process owner.
B. follow the business continuity plan (BCP).
C. conduct an incident forensic analysis.
D. follow the incident response plan.

Answer: A

NEW QUESTION 147
The PRIMARY objective of performing a post-incident review is to:

A. re-evaluate the impact of incidents.
B. identify vulnerabilities.
C. identify control improvements.
D. identify the root cause.

Answer: D

Explanation:
The primary objective of performing a post-incident review is to identify the root cause of the incident. This information is used to develop and implement corrective actions to prevent similar incidents from occurring in the future. The post-incident review process may also include a re-evaluation of the impact of the incidents, the identification of vulnerabilities, and the identification of control improvements, but the primary objective is to determine the root cause of the incident. By understanding the root cause, the organization can take proactive steps to prevent similar incidents from occurring in the future and improve the overall security posture of the organization.

NEW QUESTION 149
A post-incident review identified that user error resulted in a major breach. Which of the following is MOST important to determine during the review?

A. The time and location that the breach occurred
B. Evidence of previous incidents caused by the user
C. The underlying reason for the user error
D. Appropriate disciplinary procedures for user error

Answer: C

NEW QUESTION 152
Which of the following is MOST important to ensure when developing escalation procedures for an incident response plan?

A. Each process is assigned to a responsible party.
B. The contact list is regularly updated.
C. Minimum regulatory requirements are maintained.
D. Senior management approval has been documented.

Answer: B

NEW QUESTION 155
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

CISM Practice Exam Features:

* CISM Questions and Answers Updated Frequently

* CISM Practice Questions Verified by Expert Senior Certified Staff

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

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