Exam Questions CISM

Certified Information Security Manager

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

NEW QUESTION 1
Of the following, whose input is of GREATEST importance in the development of an information security strategy?

A. Process owners
B. End users
C. Security architects.
D. Corporate auditors

Answer: A

NEW QUESTION 2
Which of the following BEST enables an organization to transform its culture to support information security?

A. Periodic compliance audits
B. Strong management support
C. Robust technical security controls
D. Incentives for security incident reporting

Answer: B

Explanation:
While periodic compliance audits, robust technical security controls, and incentives for security incident reporting can all help to improve an organization's information security posture, strong management support is essential for enabling an organization to transform its culture to support information security. This means ensuring that security is given the necessary attention and resources, and that the security team is given the autonomy to implement the necessary policies, procedures, and controls.

NEW QUESTION 3
Which of the following will ensure confidentiality of content when accessing an email system over the Internet?

A. Multi-factor authentication
B. Digital encryption
C. Data masking
D. Digital signatures

Answer: B

NEW QUESTION 4
Which of the following is a PRIMARY benefit of managed security solutions?

A. Wider range of capabilities
B. Easier implementation across an organization
C. Greater ability to focus on core business operations
D. Lower cost of operations

Answer: D

NEW QUESTION 5
Which of the following events would MOST likely require a revision to the information security program?

A. An increase in industry threat level .
B. A significant increase in reported incidents
C. A change in IT management
D. A merger with another organization

Answer: D

Explanation:
A merger with another organization would likely require a revision to the information security program because it can result in significant changes to the structure, size, and information systems of the merged entity. This can affect the security requirements, risk tolerance, and governance policies of the organization. To ensure that the information security program remains effective, it is important to review and revise the security policies, standards, and procedures in light of the changes brought on by the merger. The information security program should align with the new organization's risk tolerance, security requirements, and governance policies. This information can be found in the ISACA's Certified Information Security Manager (CISM) Study Manual, Section 3.1.

NEW QUESTION 6
Which of the following security processes will BEST prevent the exploitation of system vulnerabilities?

A. Intrusion detection
B. Log monitoring
C. Patch management
D. Antivirus software

Answer: C

NEW QUESTION 7

Which of the following presents the GREATEST challenge to a security operations center's wna GY of potential security breaches?

A. IT system clocks are not synchronized with the centralized logging server.
B. Operating systems are no longer supported by the vendor.
C. The patch management system does not deploy patches in a timely manner.
D. An organization has a decentralized data center that uses cloud services.

Answer: A

NEW QUESTION 8
Which of the following is the BEST evidence of alignment between corporate and information security governance?

A. Security key performance indicators (KPIs)
B. Project resource optimization
C. Regular security policy reviews
D. Senior management sponsorship

Answer: D

NEW QUESTION 9
Which of the following BEST determines the allocation of resources during a security incident response?

A. Senior management commitment
B. A business continuity plan (BCP)
C. An established escalation process
D. Defined levels of severity

Answer: D

Explanation:
Defined levels of severity is the best determinant of the allocation of resources during a security incident response. Having defined levels of severity allows organizations to plan for and allocate resources for each level of incident, depending on the severity of the incident. This ensures that the right resources are allocated in a timely manner and that incidents are addressed appropriately.

NEW QUESTION 10
Which of the following is the BEST tool to monitor the effectiveness of information security governance?

A. Key performance indicators (KPIs)
B. Balanced scorecard
C. Business impact analysis (BIA)
D. Risk profile

Answer: B

Explanation:
The best tool to monitor the effectiveness of information security governance is a Balanced Scorecard. A Balanced Scorecard is a performance management tool used to measure the success of an organization's information security governance. It is a strategic planning and management system that helps organizations track and measure the progress of their security initiatives by using a set of metrics across four areas: financial, customer, internal, and learning and growth. This helps organizations to assess their progress and adjust their security strategies to ensure they are meeting their desired objectives.

NEW QUESTION 10
Which of the following is MOST important when conducting a forensic investigation?

A. Analyzing system memory
B. Documenting analysis steps
C. Capturing full system images
D. Maintaining a chain of custody

Answer: D

NEW QUESTION 13
Security administration efforts will be greatly reduced following the deployment of which of the following techniques?

A. Discretionary access control
B. Role-based access control
C. Access control lists
D. Distributed access control

Answer: B

NEW QUESTION 15
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 16
While classifying information assets an information security manager notices that several production databases do not have owners assigned to them What is the BEST way to address this situation?

A. Assign responsibility to the database administrator (DBA).
B. Review the databases for sensitive content.
C. Prepare a report of the databases for senior management.
D. Assign the highest classification level to those databases.

Answer: A

Explanation:
The best way to address this situation is to assign responsibility to the database administrator (DBA). The DBA should review the databases for sensitive content and assign the appropriate classification level to each database. This should be done in accordance with the organization's information security policies, which should outline the rules and guidelines for classifying information assets. Additionally, the information security manager should prepare a report of the databases for senior management, noting the databases that do not have owners assigned to them, as well as any other relevant information. This will help to ensure that the organization is properly managing its information assets and that any risks associated with the lack of owners are identified and addressed. This information can be found in the ISACA's Certified Information Security Manager (CISM) Study Manual, Section 5.3.

NEW QUESTION 18
An information security manager has been notified about a compromised endpoint device Which of the following is the BEST course of action to prevent further damage?

A. Wipe and reset the endpoint device.
B. Isolate the endpoint device.
C. Power off the endpoint device.
D. Run a virus scan on the endpoint device.

Answer: B

Explanation:
The best course of action to prevent further damage is to isolate the endpoint device. Isolating the endpoint device will prevent the compromised system from connecting to other systems on the network and spreading the infection. Other possible courses of action include wiping and resetting the endpoint device, running a virus scan, and powering off the endpoint device. However, these actions will not prevent the compromised system from continuing to spread the infection.

NEW QUESTION 22
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 26
Penetration testing is MOST appropriate when a:

A. new system is about to go live.
B. new system is being designed.
C. security policy is being developed.
D. security incident has occurred,

Answer: A

NEW QUESTION 31
When choosing the best controls to mitigate risk to acceptable levels, the information security manager's decision should be MAINLY driven by:

A. best practices.
B. control framework
C. regulatory requirements.
D. cost-benefit analysis,

Answer: C

NEW QUESTION 33
To overcome the perception that security is a hindrance to business activities, it is important for an information security manager to:

A. rely on senior management to enforce security.
B. promote the relevance and contribution of security.

C. focus on compliance.
D. reiterate the necessity of security.

Answer: B

Explanation:
To overcome the perception that security is a hindrance to business activities, it is important for an information security manager to promote the relevance and contribution of security. By demonstrating the value that security brings to the organization, including protecting assets and supporting business objectives, the information security manager can help to change the perception of security from a hindrance to a critical component of business success.
Relying on senior management to enforce security, focusing on compliance, and reiterating the necessity of security are all important elements of a comprehensive security program, but they do not directly address the perception that security is a hindrance to business activities. By promoting the relevance and contribution of security, the information security manager can help to align security with the overall goals and objectives of the organization, and foster a culture that values and supports security initiatives.

NEW QUESTION 38
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 42
Which of the following is the MOST important reason for obtaining input from risk owners when implementing controls?

A. To reduce risk mitigation costs
B. To resolve vulnerabilities in enterprise architecture (EA)
C. To manage the risk to an acceptable level
D. To eliminate threats impacting the business

Answer: C

Explanation:
According to the Certified Information Security Manager (CISM) Study Manual, risk owners are responsible for managing a risk, including taking corrective action to reduce the risk to an acceptable level. When implementing controls, it is essential to obtain input from risk owners to ensure that the controls are effective in managing the risk to an acceptable level.
By obtaining input from risk owners, the organization can ensure that the controls are tailored to the specific
risks and are effective in reducing the risk to an acceptable level. This can help to minimize the impact of the risk on the organization and reduce the potential for financial or reputational damage.

NEW QUESTION 44
Which of the following is the PRIMARY objective of incident triage?

A. Coordination of communications
B. Mitigation of vulnerabilities
C. Categorization of events
D. Containment of threats

Answer: C

Explanation:
Incident triage is the process of quickly assessing an incident and determining its severity in order to prioritize the response. This involves categorizing the events based on their potential impact, which helps to determine the right response and the most effective use of resources. It also helps to identify potential threats and vulnerabilities, and to coordinate communications and response activities.

NEW QUESTION 49
Which of the following is the MOST important reason to ensure information security is aligned with the organization's strategy?

A. To identify the organization's risk tolerance
B. To improve security processes
C. To align security roles and responsibilities
D. To optimize security risk management

Answer: D

NEW QUESTION 53

An organization has received complaints from users that some of their files have been encrypted. These users are receiving demands for money to decrypt the files. Which of the following would be the BEST course of action?

A. Conduct an impact assessment.
B. Isolate the affected systems.
C. Rebuild the affected systems.
D. Initiate incident response.

Answer: B

NEW QUESTION 54
Which of the following is the GREATEST inherent risk when performing a disaster recovery plan (DRP) test?

A. Poor documentation of results and lessons learned
B. Lack of communication to affected users
C. Disruption to the production environment
D. Lack of coordination among departments

Answer: C

Explanation:
The greatest inherent risk when performing a disaster recovery plan (DRP) test is disruption to the production environment. A DRP test involves simulating a disaster scenario to ensure that the organization's plans are effective and that it is able to recover from an incident. However, this involves running tests on the production environment, which has the potential to disrupt the normal operations of the organization. This inherent risk can be mitigated by running tests on a non-production environment or by running tests at times when disruption will be minimized.

NEW QUESTION 55
The effectiveness of an information security governance framework will BEST be enhanced if:

A. consultants review the information security governance framework.
B. a culture of legal and regulatory compliance is promoted by management.
C. risk management is built into operational and strategic activities.
D. IS auditors are empowered to evaluate governance activities

Answer: B

NEW QUESTION 58
What should be the FIRST step when an Internet of Things (loT) device in an organization's network is confirmed to have been hacked?

A. Monitor the network.
B. Perform forensic analysis.
C. Disconnect the device from the network,
D. Escalate to the incident response team

Answer: C

NEW QUESTION 63
Which of the following is MOST important to include in a report to key stakeholders regarding the effectiveness of an information security program?

A. Security metrics
B. Security baselines
C. Security incident details
D. Security risk exposure

Answer: A

Explanation:
Security metrics are the most important to include in a report to key stakeholders regarding the effectiveness of an information security program because they provide objective and measurable evidence of security performance and progress. Security metrics can include measures such as the number and severity of security incidents, the level of compliance with security policies and standards, the effectiveness of security controls, and the return on investment (ROI) of security initiatives. The other choices may also be included in a security report, but security metrics are the most important.
An information security program is a set of policies, procedures, standards, guidelines, and tools that aim to protect an organization’s information assets from threats and ensure compliance with laws and regulations. The effectiveness of an information security program depends on various factors, such as the organization’s risk appetite, business objectives, resources, culture, and external environment. Regular reporting to key stakeholders, such as senior management, the board of directors, and business partners, is critical to maintaining their support and buy-in for the program. The report should provide clear and concise information on the program’s status, achievements, challenges, and future plans, and it should be tailored to the audience’s needs and expectations.

NEW QUESTION 64
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 66
Which of the following is MOST important to include in an incident response plan to ensure incidents are responded to by the appropriate individuals?

A. Skills required for the incident response team
B. A list of external resources to assist with incidents
C. Service level agreements (SLAs)
D. A detailed incident notification process

Answer: D

Explanation:
An incident response plan is a critical component of an organization's overall security strategy, as it provides a framework for responding to security incidents in a timely and effective manner. To ensure that incidents are responded to by the appropriate individuals, it is essential to have a detailed incident notification process that clearly outlines who is responsible for responding to different types of incidents, how incidents should be reported and escalated, and who should be notified in the event of an incident. This helps to ensure that incidents are addressed promptly and effectively, and that the right resources are brought to bear to resolve the issue. Other important elements to include in an incident response plan include a clear definition of roles and responsibilities, a list of external resources to assist with incidents, and incident response procedures, such as steps to contain, assess, and recover from incidents.

NEW QUESTION 67
A multinational organization is required to follow governmental regulations with different security requirements at each of its operating locations. The chief information security officer (CISO) should be MOST concerned with:

A. developing a security program that meets global and regional requirements.
B. ensuring effective communication with local regulatory bodies.
C. using industry best practice to meet local legal regulatory requirements.
D. monitoring compliance with defined security policies and standards.

Answer: A

Explanation:
In this scenario, the chief information security officer (CISO) should be most concerned with developing a security program that meets the global and regional requirements of the organization. This includes considering the different legal and regulatory requirements of each operating location, and designing a security program that meets all of these requirements. The CISO should also ensure effective communication with local regulatory bodies to ensure compliance and understanding of the security program. Additionally, the CISO should use industry best practices and defined security policies and standards to ensure the program meets all applicable requirements.

NEW QUESTION 68
A recovery point objective (RPO) is required in which of the following?

A. Disaster recovery plan (DRP)
B. Information security plan
C. Incident response plan
D. Business continuity plan (BCP)

Answer: A

NEW QUESTION 73
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 75
Implementing the principle of least privilege PRIMARILY requires the identification of:

A. job duties
B. data owners
C. primary risk factors.
D. authentication controls

Answer: A

Explanation:
Implementing the principle of least privilege primarily requires the identification of job duties. This principle states that users should only be given the minimum level of access necessary to perform their job duties. By identifying the specific job duties of each user, an organization can determine the minimum level of access needed, and restrict access to any unnecessary resources. This helps to minimize the potential damage that can be caused by a malicious or compromised user.

NEW QUESTION 78
Which of the following has the GREATEST influence on an organization's information security strategy?

A. The organization's risk tolerance
B. The organizational structure
C. Industry security standards
D. Information security awareness

Answer: A

Explanation:
An organization's information security strategy should be aligned with its risk tolerance, which is the level of risk that an organization is willing to accept in pursuit of its objectives. The strategy should aim to balance the cost of security controls with the potential impact of security incidents on the organization's objectives. Therefore, an organization's risk tolerance has the greatest influence on its information security strategy.
The organization’s risk tolerance has the greatest influence on its information security strategy because it determines how much risk the organization is willing to accept and how much resources it will allocate to mitigate or transfer risk. The organizational structure, industry security standards, and information security awareness are important factors that affect the implementation and effectiveness of an information security strategy but not as much as the organization’s risk tolerance.
An information security strategy is a high-level plan that defines how an organization will achieve its information security objectives and address its information security risks. An information security strategy should align with the organization’s business strategy and reflect its mission, vision, values, and culture. An information security strategy should also consider the external and internal factors that influence the organization’s information security environment such as laws, regulations, competitors, customers, suppliers, partners, stakeholders, employees etc.

NEW QUESTION 81
When properly implemented, secure transmission protocols protect transactions:

A. from eavesdropping.
B. from denial of service (DoS) attacks.
C. on the client desktop.
D. in the server's database.

Answer: A

NEW QUESTION 82
Which of the following BEST supports the incident management process for attacks on an organization's supply chain?

A. Including service level agreements (SLAs) in vendor contracts
B. Establishing communication paths with vendors
C. Requiring security awareness training for vendor staff
D. Performing integration testing with vendor systems

Answer: B

NEW QUESTION 84
Reverse lookups can be used to prevent successful:

A. denial of service (DoS) attacks
B. session hacking
C. phishing attacks
D. Internet protocol (IP) spoofing

Answer: D

Explanation:
Reverse lookups can be used to prevent successful IP spoofing. IP spoofing is a type of attack in which an attacker sends packets with a false source IP address in order to disguise their identity or impersonate another system. By performing reverse lookups on the source IP address of incoming packets, the system can verify that the packets are coming from a trusted source, and any packets with an invalid or spoofed source IP can be discarded. This is an important measure for preventing IP spoofing, and can help to reduce the risk of other types of attacks, such as DoS attacks, session hacking, and phishing attacks.

NEW QUESTION 86
The PRIMARY advantage of single sign-on (SSO) is that it will:

A. increase efficiency of access management
B. increase the security of related applications.
C. strengthen user passwords.
D. support multiple authentication mechanisms.

Answer: A

Explanation:
The primary advantage of single sign-on (SSO) is that it increases the efficiency of access management. With SSO, users only need to remember one set of credentials to access all of their applications, rather than having to remember multiple usernames and passwords for each application. This simplifies the user experience and helps to reduce the amount of time spent managing access to multiple applications. Additionally, SSO can also increase the security of related applications, as users are not sharing the same credentials across multiple applications, and it can also support multiple authentication mechanisms, such as biometric authentication.

NEW QUESTION 90

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 95
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 96
Which of the following is the MOST critical factor for information security program success?

A. comprehensive risk assessment program for information security
B. The information security manager's knowledge of the business
C. Security staff with appropriate training and adequate resources
D. Ongoing audits and addressing open items

Answer: B

Explanation:
The explanation given in the manual is:
The information security manager’s knowledge of the business is the most critical factor for information security program success because it enables him or her to align security objectives with business goals and communicate effectively with senior management and other stakeholders. The other choices are important elements of an information security program but not as critical as the information security manager’s knowledge of the business.
An information security program is a set of policies, procedures, standards, guidelines, and tools that aim to protect an organization’s information assets from threats and ensure compliance with laws and regulations. An information security manager is a professional who oversees and coordinates the implementation and maintenance of an information security program. An information security manager should have a good understanding of the business environment, culture, strategy, processes, and needs of an organization to ensure that security supports its objectives.

NEW QUESTION 97
Which of the following is MOST important to ensuring information stored by an organization is protected appropriately?

A. Defining information stewardship roles
B. Defining security asset categorization
C. Assigning information asset ownership
D. Developing a records retention schedule

Answer: C

NEW QUESTION 102
Which of the following would BEST ensure that security is integrated during application development?

A. Employing global security standards during development processes
B. Providing training on secure development practices to programmers
C. Performing application security testing during acceptance testing
D. Introducing security requirements during the initiation phase

Answer: B

NEW QUESTION 105
In violation of a policy prohibiting the use of cameras at the office, employees have been issued smartphones and tablet computers with enabled web cameras.
Which of the following should be the information security manager's FIRST course of action?

A. Revise the policy.
B. Perform a root cause analysis.
C. Conduct a risk assessment,
D. Communicate the acceptable use policy.

Answer: C

NEW QUESTION 109
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 113
An organization's disaster recovery plan (DRP) is documented and kept at a disaster recovery site. Which of the following is the BEST way to ensure the plan can be carried out in an emergency?

A. Store disaster recovery documentation in a public cloud.
B. Maintain an outsourced contact center in another country.
C. Require disaster recovery documentation be stored with all key decision makers.
D. Provide annual disaster recovery training to appropriate staff.

Answer: C

NEW QUESTION 114
The MAIN reason for having senior management review and approve an information security strategic plan is to ensure:

A. the organization has the required funds to implement the plan.
B. compliance with legal and regulatory requirements.
C. staff participation in information security efforts.
D. the plan aligns with corporate governance.

Answer: D

Explanation:
Senior management review and approval of an information security strategic plan is important to ensure that the plan is aligned with the organization's overall corporate governance objectives. It is also important to ensure that the plan takes into account any legal and regulatory requirements, as well as the resources and staff needed to properly implement the plan.

NEW QUESTION 119
Which of the following defines the triggers within a business continuity plan (BCP)? @

A. Needs of the organization
B. Disaster recovery plan (DRP)
C. Information security policy
D. Gap analysis

Answer: B

NEW QUESTION 122
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 125
Which of the following is the BEST approach when creating a security policy for a global organization subject to varying laws and regulations?

A. Incorporate policy statements derived from third-party standards and benchmarks.
B. Adhere to a unique corporate privacy and security standard
C. Establish baseline standards for all locations and add supplemental standards as required
D. Require that all locations comply with a generally accepted set of industry

Answer: C

Explanation:
When creating a security policy for a global organization subject to varying laws and regulations, it is important to consider the unique legal and cultural requirements of each location. The best approach is to establish baseline standards for all locations and then add supplemental standards as required to meet local laws and regulations. This approach ensures that the organization is in compliance with all relevant laws and regulations, while also maintaining a consistent and unified approach to security across all locations. Additionally, by establishing baseline standards, the organization can ensure that its security policies are aligned with its overall security strategy and objectives.

NEW QUESTION 128

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 132
Network isolation techniques are immediately implemented after a security breach to:

A. preserve evidence as required for forensics
B. reduce the extent of further damage.
C. allow time for key stakeholder decision making.
D. enforce zero trust architecture principles.

Answer: B

NEW QUESTION 136
Which of the following is MOST important for building 4 robust information security culture within an organization?

A. Mature information security awareness training across the organization
B. Strict enforcement of employee compliance with organizational security policies
C. Security controls embedded within the development and operation of the IT environment
D. Senior management approval of information security policies

Answer: D

NEW QUESTION 137
Which of the following parties should be responsible for determining access levels to an application that processes client information?

A. The business client
B. The information security tear
C. The identity and access management team
D. Business unit management

Answer: D

NEW QUESTION 139
To confirm that a third-party provider complies with an organization's information security requirements, it is MOST important to ensure:

A. security metrics are included in the service level agreement (SLA).
B. contract clauses comply with the organization's information security policy.
C. the information security policy of the third-party service provider is reviewed.
D. right to audit is included in the service level agreement (SLA).

Answer: D

NEW QUESTION 142
Which of the following is MOST important for an information security manager to verify before conducting full-functional continuity testing?

A. Risk acceptance by the business has been documented
B. Teams and individuals responsible for recovery have been identified
C. Copies of recovery and incident response plans are kept offsite
D. Incident response and recovery plans are documented in simple language

Answer: B

Explanation:
Before conducting full-functional continuity testing, an information security manager should verify that teams and individuals responsible for recovery have been identified and trained on their roles and responsibilities. This will ensure that the testing can be executed effectively and efficiently, as well as identify any gaps or issues in the recovery process. Risk acceptance by the business, copies of plans kept offsite and plans documented in simple language are all good practices for continuity management, but they are not as important as having clear roles and responsibilities defined before testing.

NEW QUESTION 145
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 149
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 153
Which of the following is MOST important to consider when aligning a security awareness program with the organization's business strategy?

A. Regulations and standards
B. People and culture
C. Executive and board directives
D. Processes and technology

Answer: B

NEW QUESTION 156
Which of the following MUST be defined in order for an information security manager to evaluate the appropriateness of controls currently in place?

A. Security policy
B. Risk management framework
C. Risk appetite
D. Security standards

Answer: A

NEW QUESTION 157
An information security manager believes that information has been classified inappropriately, = the risk of a breach. Which of the following is the information security manager's BEST action?

A. Refer the issue to internal audit for a recommendation.
B. Re-classify the data and increase the security level to meet business risk.
C. Instruct the relevant system owners to reclassify the data.
D. Complete a risk assessment and refer the results to the data owners.

Answer: D

NEW QUESTION 160
Which of the following is the BEST indication ofa successful information security culture?

A. Penetration testing is done regularly and findings remediated.
B. End users know how to identify and report incidents.
C. Individuals are given roles based on job functions.
D. The budget allocated for information security is sufficient.

Answer: B

NEW QUESTION 163
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 164
Which of the following BEST enables the integration of information security governance into corporate governance?

A. Well-decumented information security policies and standards
B. An information security steering committee with business representation
C. Clear lines of authority across the organization
D. Senior management approval of the information security strategy

Answer: B

NEW QUESTION 166
Which of the following is the MOST important consideration when establishing an organization's information security governance committee?

A. Members have knowledge of information security controls.
B. Members are business risk owners.
C. Members are rotated periodically.
D. Members represent functions across the organization.

Answer: D

NEW QUESTION 167
Which of the following BEST supports information security management in the event of organizational changes in security personnel?

A. Formalizing a security strategy and program
B. Developing an awareness program for staff
C. Ensuring current documentation of security processes
D. Establishing processes within the security operations team

Answer: C

NEW QUESTION 172
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 173
Which of the following BEST indicates that information security governance and corporate governance are integrated?

A. The information security team is aware of business goals.
B. The board is regularly informed of information security key performance indicators (KPIs),
C. The information security steering committee is composed of business leaders.
D. A cost-benefit analysis is conducted on all information security initiatives.

Answer: C

NEW QUESTION 174
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 177
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 181
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 186
An organization is planning to outsource the execution of its disaster recovery activities. Which of the following would be MOST important to include in the outsourcing agreement?

A. Definition of when a disaster should be declared
B. Requirements for regularly testing backups
C. Recovery time objectives (RTOs)
D. The disaster recovery communication plan

Answer: D

NEW QUESTION 190
Which of the following is MOST critical when creating an incident response plan?

A. Identifying vulnerable data assets
B. Identifying what constitutes an incident
C. Decumenting incident notification and escalation processes
D. Aligning with the risk assessment process

Answer: B

NEW QUESTION 193
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 198
Reevaluation of risk is MOST critical when there is:

A. resistance to the implementation of mitigating controls.
B. a management request for updated security reports.
C. a change in security policy.
D. a change in the threat landscape.

Answer: D

NEW QUESTION 202
Which of the following is the BEST course of action if the business activity residual risk is lower than the acceptable risk level?

A. Monitor the effectiveness of controls
B. Update the risk assessment framework
C. Review the inherent risk level
D. Review the risk probability and impact

Answer: A

Explanation:
If the residual risk of the business activity is lower than the acceptable risk level, it means that the existing controls are effectively mitigating the identified risks. In this case, the best course of action is to monitor the effectiveness of the controls and ensure they remain effective. The information security manager should review and test the controls periodically to ensure that they continue to provide adequate protection. It is also essential to update the risk assessment framework to reflect changes in the business environment or risk landscape.

NEW QUESTION 205
Which of the following BEST enables staff acceptance of information security policies?

A. Strong senior management support
B. Gomputer-based training
C. Arobust incident response program

D. Adequate security funding

Answer: A

NEW QUESTION 208
Which of the following would be MOST effective in gaining senior management approval of security investments in network infrastructure?

A. Performing penetration tests against the network to demonstrate business vulnerability
B. Highlighting competitor performance regarding network best security practices
C. Demonstrating that targeted security controls tie to business objectives
D. Presenting comparable security implementation estimates from several vendors

Answer: C

Explanation:
The most effective way to gain senior management approval of security investments in network infrastructure is by demonstrating that targeted security controls tie to business objectives.
Security investments should be tied to business objectives and should support the overall goals of the organization. By demonstrating that the security controls will directly support the organization's business objectives, senior management will be more likely to approve the investment.
According to the Certified Information Security Manager (CISM) Study Manual, "To gain senior
management's approval for investments in security, it is essential to show how the security controls tie to business objectives and are in support of the overall goals of the organization."
While performing penetration tests against the network, highlighting competitor performance, and presenting comparable security implementation estimates from vendors are all useful in presenting the value of security investments, they are not as effective as demonstrating how the security controls will support the organization's business objectives.

NEW QUESTION 210
Which of the following will result in the MOST accurate controls assessment?

A. Mature change management processes
B. Senior management support
C. Well-defined security policies
D. Unannounced testing

Answer: B

NEW QUESTION 211
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 215
Due to changes in an organization's environment, security controls may no longer be adequate. What is the information security manager's BEST course of action?

A. Review the previous risk assessment and countermeasures.
B. Perform a new risk assessment,
C. Evaluate countermeasures to mitigate new risks.
D. Transfer the new risk to a third party.

Answer: C

NEW QUESTION 218
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 219
Which of the following is MOST important to consider when determining asset valuation?

A. Asset recovery cost
B. Asset classification level
C. Cost of insurance premiums
D. Potential business loss

Answer: D

NEW QUESTION 221
Which of the following is MOST important to include in a post-incident review following a data breach?

A. An evaluation of the effectiveness of the information security strategy
B. Evaluations of the adequacy of existing controls
C. Documentation of regulatory reporting requirements
D. A review of the forensics chain of custom

Answer: B

NEW QUESTION 223
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 225
What is the PRIMARY benefit to an organization when information security program requirements are aligned with employment and staffing processes?

A. Security incident reporting procedures are followed.
B. Security staff turnover is reduced.
C. Information assets are classified appropriately.
D. Access is granted based on task requirements.

Answer: D

NEW QUESTION 230
Which of the following is the BEST way to help ensure an organization's risk appetite will be considered as part of the risk treatment process?

A. Establish key risk indicators (KRIs).
B. Use quantitative risk assessment methods.
C. Provide regular reporting on risk treatment to senior management
D. Require steering committee approval of risk treatment plans.

Answer: D

NEW QUESTION 235
A user reports a stolen personal mobile device that stores sensitive corporate data. Which of the following will BEST minimize the risk of data exposure?

A. Prevent the user from using personal mobile devices.
B. Report the incident to the police.
C. Wipe the device remotely.
D. Remove user's access to corporate data.

Answer: C

NEW QUESTION 239
Which of the following would be MOST useful to a newly hired information security manager who has been tasked with developing and implementing an information security strategy?

A. The capabilities and expertise of the information security team
B. The organization's mission statement and roadmap
C. A prior successful information security strategy
D. The organization's information technology (IT) strategy

Answer: B

NEW QUESTION 242
Which of the following is the BEST approach to incident response for an organization migrating to a cloud-based solution?

A. Adopt the cloud provider's incident response procedures.
B. Transfer responsibility for incident response to the cloud provider.
C. Continue using the existing incident response procedures.
D. Revise incident response procedures to encompass the cloud environment.

Answer: D

NEW QUESTION 243
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 248
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 250
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. After an incident has occurred, the post-incident review process involves gathering and analyzing evidence to determine the cause of the incident. This analysis will help to identify both the underlying vulnerability that allowed the incident to occur, as well as any control improvements that should be implemented to prevent similar incidents from occurring in the future. Additionally, the post-incident review process can also be used to re-evaluate the impact of the incident, as well as any potential implications for the organization.

NEW QUESTION 254
Which of the following BEST enables an information security manager to determine the comprehensiveness of an organization's information security strategy?

A. Internal security audit
B. External security audit
C. Organizational risk appetite
D. Business impact analysis (BIA)

Answer: A

NEW QUESTION 256
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 258
Which of the following is the MOST important detail to capture in an organization's risk register?

A. Risk appetite
B. Risk severity level
C. Risk acceptance criteria

D. Risk ownership

Answer: D

Explanation:
Risk ownership is the most important detail to capture in an organization's risk register. Risk ownership is the responsibility for managing a risk, including taking corrective action, and should be assigned to a specific individual or team. It is important to note that the risk owner is not necessarily the same as the risk acceptor, who is the individual or team who makes the final decision to accept a risk. Capturing risk ownership in the risk register is important to ensure that risks are actively managed and that the responsible parties are held accountable.

NEW QUESTION 259
Which of the following sources is MOST useful when planning a business-aligned information security program?

A. Security risk register
B. Information security policy
C. Business impact analysis (BIA)
D. Enterprise architecture (EA)

Answer: C

Explanation:
The most useful source when planning a business-aligned information security program is a Business Impact Analysis (BIA). A BIA is a process of identifying and evaluating the potential effects of disruptions to an organization's operations, and helps to identify the security controls and measures that should be implemented to reduce the impact of those disruptions. The BIA should include an assessment of the organization's information security posture, including its security policies, risk register, and enterprise architecture. With this information, organizations can develop an information security program that is aligned to the organization's business objectives.

NEW QUESTION 261
When collecting admissible evidence, which of the following is the MOST important requirement?

A. Need to know
B. Preserving audit logs
C. Due diligence
D. Chain of custody

Answer: D

Explanation:
The most important requirement when collecting admissible evidence is the chain of custody. The chain of
custody is a documented record of who had control of the evidence at any given time, from the point of collection until the evidence is presented in court. This is important in order to ensure the evidence can be authenticated and is not subject to tampering or any other form of interference. Other important considerations include need to know, preserving audit logs, and due diligence.

NEW QUESTION 263
Which of the following is the PRIMARY role of an information security manager in a software development project?

A. To enhance awareness for secure software design
B. To assess and approve the security application architecture
C. To identify noncompliance in the early design stage
D. To identify software security weaknesses

Answer: A

NEW QUESTION 266
Which of the following is the MOST important consideration when defining a recovery strategy in a business continuity plan (BCP)?

A. Legal and regulatory requirements
B. Likelihood of a disaster
C. Organizational tolerance to service interruption
D. Geographical location of the backup site

Answer: C

NEW QUESTION 267
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 268
Which of the following is the MOST important reason to conduct interviews as part of the business impact analysis (BIA) process?

A. To facilitate a qualitative risk assessment following the BIA
B. To increase awareness of information security among key stakeholders
C. To ensure the stakeholders providing input own the related risk
D. To obtain input from as many relevant stakeholders as possible

Answer: C

NEW QUESTION 270
The PRIMARY objective of a post-incident review of an information security incident is to:

A. update the risk profile
B. minimize impact
C. prevent recurrence.
D. determine the impact

Answer: C

Explanation:
The primary objective of a post-incident review of an information security incident is to identify the root cause of the incident and determine what can be done to prevent a similar incident from happening in the future. This process helps organizations to learn from past incidents and make improvements to their security posture to reduce the risk of future incidents. By conducting a thorough post-incident review, organizations can identify areas for improvement in their security controls, policies, and procedures, and implement changes to prevent similar incidents from happening in the future. Other important objectives of a post-incident review may include updating the risk profile, minimizing impact, and determining the impact of the incident, but the main focus should be on identifying ways to prevent recurrence.

NEW QUESTION 273
An anomaly-based intrusion detection system (IDS) operates by gathering data on:

A. normal network behavior and using it as a baseline lor measuring abnormal activity
B. abnormal network behavior and issuing instructions to the firewall to drop rogue connections
C. abnormal network behavior and using it as a baseline for measuring normal activity
D. attack pattern signatures from historical data

Answer: A

Explanation:
An anomaly-based intrusion detection system (IDS) operates by gathering data on normal network behavior and using it as a baseline for measuring abnormal activity. This is important because it allows the IDS to detect any activity that is outside of the normal range of usage for the network, which can help to identify potential malicious activity or security threats. Additionally, the IDS will monitor for any changes in the baseline behavior and alert the administrator if any irregularities are detected. By contrast, signature-based IDSs operate by gathering attack pattern signatures from historical data and comparing them against incoming traffic in order to identify malicious activity.

NEW QUESTION 277
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 278
Which of the following roles is BEST able to influence the security culture within an organization?

A. Chief information security officer (CISO)
B. Chief information officer (CIO)
C. Chief executive officer (CEO)
D. Chief operating officer (COO)

Answer: A

Explanation:
The Chief Information Security Officer (CISO) is responsible for leading and coordinating an organization's information security program, and as such, is in a prime position to influence the security culture within the organization. The CISO is responsible for setting policies and standards, educating employees about security risks and best practices, and ensuring that the organization is taking appropriate measures to mitigate security risks. By demonstrating a strong commitment to information security, the CISO can help to create a security-aware culture within the organization.

NEW QUESTION 281
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 282
An organization is in the process of acquiring a new company Which of the following would be the BEST approach to determine how to protect newly acquired data assets prior to integration?

A. Include security requirements in the contract
B. Assess security controls.
C. Perform a risk assessment
D. Review data architecture.

Answer: C

Explanation:
The best approach to determine how to protect newly acquired data assets prior to integration is to perform a risk assessment. A risk assessment will identify the various threats and vulnerabilities associated with the data assets and help the organization develop an appropriate security strategy. This risk assessment should include an assessment of the security controls in place to protect the data, a review of the data architecture, and a review of any contractual requirements related to security.

NEW QUESTION 286
During the initiation phase of the system development life cycle (SDLC) for a software project, information security activities should address:

A. baseline security controls.
B. benchmarking security metrics.
C. security objectives.
D. cost-benefit analyses.

Answer: A

NEW QUESTION 288
Which of the following is the MOST effective way to help staff members understand their responsibilities for information security?

A. Communicate disciplinary processes for policy violations.
B. Require staff to participate in information security awareness training.
C. Require staff to sign confidentiality agreements.
D. Include information security responsibilities in job descriptions.

Answer: B

NEW QUESTION 291
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

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

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

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

Money Back Guarantee

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