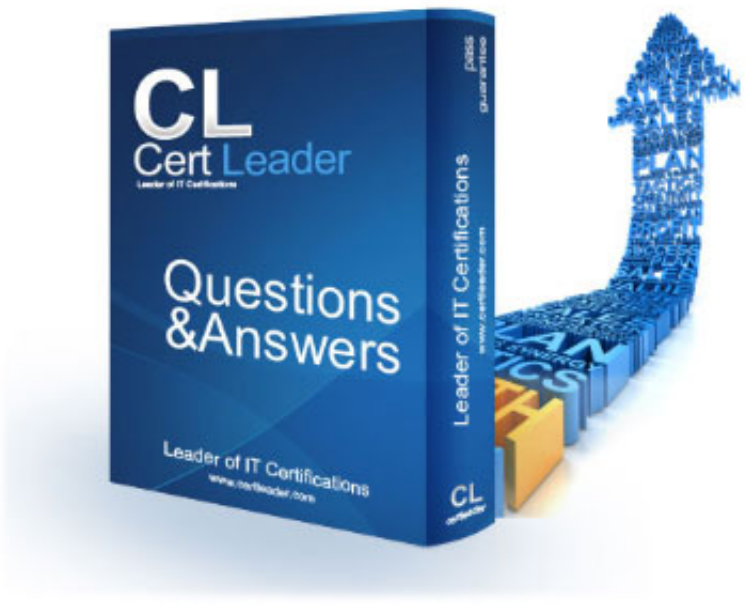
CISM Dumps

Certified Information Security Manager

https://www.certleader.com/CISM-dumps.html



NEW QUESTION 1
Which of the following is the BEST way to ensure the capability to restore clean data after a ransomware attack?

A. Purchase cyber insurance
B. Encrypt sensitive production data
C. Perform Integrity checks on backups
D. Maintain multiple offline backups

Answer: D

Explanation:
Maintaining multiple offline backups is the best way to ensure the capability to restore clean data after a ransomware attack. This is because offline backups are not connected to the network and thus cannot be compromised by the ransomware. Additionally, performing integrity checks on backups will help to ensure that any backups that have been potentially corrupted by the ransomware can be identified and discarded. Encrypting sensitive production data and purchasing cyber insurance can help to protect against a ransomware attack, but are not the best way to ensure the capability to restore clean data after an attack.

NEW QUESTION 2
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 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 MOST effective in monitoring an organization's existing risk?

A. Periodic updates to risk register
B. Risk management dashboards
C. Security information and event management (SIEM) systems
D. Vulnerability assessment results

Answer: B

NEW QUESTION 5
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 6
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 7
Data entry functions for a web-based application have been outsourced to a third-party service provider who will work from a remote site Which of the following issues would be of GREATEST concern to an information security manager?

A. The application does not use a secure communications protocol
B. The application is configured with restrictive access controls
C. The business process has only one level of error checking
D. Server-based malware protection is not enforced

Answer: B

Explanation:
The greatest concern for an information security manager in this situation would be the security of the data that is being processed by the third-party service provider working from a remote site. This could be a concern because the data may not be adequately protected from unauthorized access, manipulation, or theft. A secure communications protocol should be used to ensure the confidentiality and integrity of the data in transit. Additionally, the information security manager should ensure that the third-party service provider has appropriate security controls in place to protect the data, such as access controls, error checking, and malware protection. This information can be found in the ISACA's Certified Information Security Manager (CISM) Study Manual, Section 5.2.

NEW QUESTION 8
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 9
Which of the following is the GREATEST benefit of including incident classification criteria within an incident response plan?

A. Ability to monitor and control incident management costs
B. More visibility to the impact of disruptions
C. Effective protection of information assets
D. Optimized allocation of recovery resources

Answer: D

Explanation:
The explanation given in the manual is:
Incident classification criteria enable an organization to prioritize incidents based on their impact and urgency. This allows for an optimized allocation of recovery resources to minimize business disruption and ensure timely restoration of normal operations. The other choices are benefits of incident management but not directly related to incident classification criteria.

NEW QUESTION 10
To help ensure that an information security training program is MOST effective its contents should be

A. focused on information security policy.
B. aligned to business processes
C. based on employees' roles
D. based on recent incidents

Answer: C

Explanation:
“An information security training program should be tailored to the specific roles and responsibilities of employees. This will help them understand how their actions affect information security and what they need to do to protect it. A generic training program that is focused on policy, business processes or recent incidents may not be relevant or effective for all employees.”

NEW QUESTION 10
Which of the following Is MOST useful to an information security manager when conducting a post-incident review of an attack?

A. Cost of the attack to the organization
B. Location of the attacker
C. Method of operation used by the attacker
D. Details from intrusion detection system (IDS) logs

Answer: C

NEW QUESTION 12
ACISO learns that a third-party service provider did not notify the organization of a data breach that affected the service provider's data center. Which of the following should the CISO do FIRST?

A. Recommend canceling the outsourcing contract.
B. Request an independent review of the provider's data center.
C. Notify affected customers of the data breach.
D. Determine the extent of the impact to the organization.

Answer: D

NEW QUESTION 15
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 18
When performing a business impact analysis (BIA), who should be responsible for determining the initial recovery time objective (RTO)?

A. External consultant
B. Information owners
C. Information security manager
D. Business continuity coordinator

Answer: D

Explanation:
When performing a business impact analysis (BIA), it is the responsibility of the business continuity coordinator to determine the initial recovery time objective (RTO). The RTO is a critical component of the
BIA and should be determined in cooperation with the information owners. The RTO should reflect the maximum tolerable period of disruption (MTPD) and should be used to guide the development of the recovery strategy.

NEW QUESTION 19
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 22
An organization's marketing department wants to use an online collaboration service, which is not in compliance with the information security policy, A risk assessment is performed, and risk acceptance is being pursued. Approval of risk acceptance should be provided by:

A. the chief risk officer (CRO).
B. business senior management.
C. the information security manager.
D. the compliance officer.

Answer: B

NEW QUESTION 26
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 31
An information security manager determines there are a significant number of exceptions to a newly released industry-required security standard. Which of the following should be done NEXT?

A. Document risk acceptances.
B. Revise the organization's security policy.
C. Assess the consequences of noncompliance.
D. Conduct an information security audit.

Answer: C

NEW QUESTION 32
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 36
Which of the following would be MOST helpful to identify worst-case disruption scenarios?

A. Business impact analysis (BIA)
B. Business process analysis
C. SWOT analysis
D. Cast-benefit analysis

Answer: A

NEW QUESTION 37
Due to specific application requirements, a project team has been granted administrative ponieon GR: is the PRIMARY reason for ensuring clearly defined roles and responsibilities are communicated to these users?

A. Clearer segregation of duties
B. Increased user productivity
C. Increased accountability
D. Fewer security incidents

Answer: C

NEW QUESTION 42
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 43
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 45
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 48
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 52
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 57
Management decisions concerning information security investments will be MOST effective when they are based on:

A. a process for identifying and analyzing threats and vulnerabilities.
B. an annual loss expectancy (ALE) determined from the history of security events,
C. the reporting of consistent and periodic assessments of risks.
D. the formalized acceptance of risk analysis by management,

Answer: C

NEW QUESTION 61
Which of the following should be the PRIMARY objective of the information security incident response process?

A. Conducting incident triage
B. Communicating with internal and external parties
C. Minimizing negative impact to critical operations
D. Classifying incidents

Answer: C

NEW QUESTION 62
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 64
Who is BEST suited to determine how the information in a database should be classified?

A. Database analyst
B. Database administrator (DBA)
C. Information security analyst
D. Data owner

Answer: D

NEW QUESTION 69
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 70
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 72
An organization's main product is a customer-facing application delivered using Software as a Service (SaaS). The lead security engineer has just identified a major security vulnerability at the primary cloud provider. Within the organization, who is PRIMARILY accountable for the associated task?

A. The information security manager
B. The data owner
C. The application owner
D. The security engineer

Answer: B

NEW QUESTION 73
A penetration test was conducted by an accredited third party Which of the following should be the information security manager's FIRST course of action?

A. Ensure a risk assessment is performed to evaluate the findings
B. Ensure vulnerabilities found are resolved within acceptable timeframes
C. Request funding needed to resolve the top vulnerabilities
D. Report findings to senior management

Answer: D

NEW QUESTION 76
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 79
Which of the following BEST demonstrates the added value of an information security program?

A. Security baselines
B. A gap analysis
C. A SWOT analysis
D. A balanced scorecard

Answer: D

Explanation:
A balanced scorecard is a tool that can be used to demonstrate the added value of an information security program by measuring and reporting on key performance indicators (KPIs) and key risk indicators (KRIs) aligned with strategic objectives. Security baselines, a gap analysis and a SWOT analysis are all useful for assessing and improving security posture, but they do not necessarily show how security contributes to business value.

NEW QUESTION 82
Which of the following would BEST justify continued investment in an information security program?

A. Reduction in residual risk
B. Security framework alignment
C. Speed of implementation
D. Industry peer benchmarking

Answer:

A

Explanation:
Residual risk is the remaining risk after all security controls have been implemented. It is important to measure the residual risk of an organization in order to determine the effectiveness of the security program and to justify continued investment in the program. A reduction in residual risk is an indication that the security program is effective and that continued investment is warranted.

NEW QUESTION 85
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 87
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 92
What should be the FIRST step when an Internet of Things (IoT) 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 95
Measuring which of the following is the MOST accurate way to determine the alignment of an information security strategy with organizational goals?

A. Number of blocked intrusion attempts
B. Number of business cases reviewed by senior management
C. Trends in the number of identified threats to the business
D. Percentage of controls integrated into business processes

Answer: D

NEW QUESTION 100
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 101
An information security manager finds that a soon-to-be deployed online application will increase risk beyond acceptable levels, and necessary controls have not been included. Which of the following is the BEST course of action for the information security manager?

A. Instruct IT to deploy controls based on urgent business needs.
B. Present a business case for additional controls to senior management.
C. Solicit bids for compensating control products.
D. Recommend a different application.

Answer: B

NEW QUESTION 106
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 109
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 112
Which of the following activities is designed to handle a control failure that leads to a breach?

A. Risk assessment
B. Incident management
C. Root cause analysis
D. Vulnerability management

Answer: B

NEW QUESTION 113
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 114
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 115
Which of the following is the MOST effective way to prevent information security incidents?

A. Implementing a security information and event management (SIEM) tool
B. Implementing a security awareness training program for employees
C. Deploying a consistent incident response approach
D. Deploying intrusion detection tools in the network environment

Answer: B

Explanation:
The most effective way to prevent information security incidents is to implement a security awareness training program for employees. Security awareness training provides employees with the knowledge and skills they need to identify potential security threats and protect their systems from unauthorized access and malicious activity. Security awareness training also helps to ensure that employees understand their roles and responsibilities when it comes to information security, and can

help to reduce the risk of information security incidents by making employees more aware of potential risks. Additionally, implementing a security information and event management (SIEM) tool, deploying a consistent incident response approach, and deploying intrusion detection tools in the network environment can also help to reduce the risk of security incidents

NEW QUESTION 117
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 118
Which of the following should be an information security manager's FIRST course of action when a newly introduced privacy regulation affects the business?

A. Consult with IT staff and assess the risk based on their recommendations
B. Update the security policy based on the regulatory requirements
C. Propose relevant controls to ensure the business complies with the regulation
D. Identify and assess the risk in the context of business objectives

Answer: D

Explanation:
Identify and assess the risk in the context of business objectives. Before making any changes to the security policy or introducing any new controls, the information security manager should first identify and assess the risk that the new privacy regulation poses to the business. This should be done in the context of the overall business objectives so that the security measures introduced are tailored to meet the specific needs of the organization.

NEW QUESTION 119
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 123
Which of the following is the PRIMARY reason to monitor key risk indicators (KRIs) related to information security?

A. To alert on unacceptable risk
B. To identify residual risk
C. To reassess risk appetite
D. To benchmark control performance

Answer: D

NEW QUESTION 128
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 129
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 134
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 135
An organization is close to going live with the implementation of a cloud-based application. Independent penetration test results have been received that show a high-rated vulnerability. Which of the following would be the BEST way to proceed?

A. Implement the application and request the cloud service provider to fix the vulnerability.
B. Assess whether the vulnerability is within the organization's risk tolerance levels.
C. Commission further penetration tests to validate initial test results,
D. Postpone the implementation until the vulnerability has been fixed.

Answer: D

NEW QUESTION 140
Which of the following should be the MOST important consideration of business continuity management?

A. Ensuring human safety
B. Identifying critical business processes
C. Ensuring the reliability of backup data
D. Securing critical information assets

Answer: A

NEW QUESTION 145
An online bank identifies a successful network attack in progress. The bank should FIRST:

A. isolate the affected network segment.
B. report the root cause to the board of directors.
C. assess whether personally identifiable information (Pll) is compromised.
D. shut down the entire network.

Answer: A

NEW QUESTION 148
Which of the following should be done FIRST when establishing a new data protection program that must comply with applicable data privacy regulations?

A. Evaluate privacy technologies required for data protection.
B. Encrypt all personal data stored on systems and networks.
C. Update disciplinary processes to address privacy violations.
D. Create an inventory of systems where personal data is stored.

Answer: D

NEW QUESTION 152
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 157
Which of the following provides the BEST assurance that security policies are applied across business operations?

A. Organizational standards are included in awareness training.

B. Organizational standards are enforced by technical controls.
C. Organizational standards are required to be formally accepted.
D. Organizational standards are documented in operational procedures.

Answer: D

NEW QUESTION 162
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 163
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 167
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 168
Which of the following will provide the MOST guidance when deciding the level of protection for an information asset?

A. Impact on information security program
B. Cost of controls
C. Impact to business function
D. Cost to replace

Answer: C

Explanation:
When deciding the level of protection for an information asset, the most important factor to consider is the impact to the business function. The value of the asset should be evaluated in terms of its importance to the organization's operations and how its security posture affects the organization's overall security posture. Additionally, the cost of implementing controls, the potential impact on the information security program, and the cost to replace the asset should be taken into account when determining the appropriate level of protection for the asset.

NEW QUESTION 170
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 175
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 177
Which of the following is the FIRST step to establishing an effective information security program?

A. Conduct a compliance review.
B. Assign accountability.
C. Perform a business impact analysis (BIA).
D. Create a business case.

Answer: D

NEW QUESTION 181
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 182
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 186
Which of the following should be the PRIMARY area of focus when mitigating security risks associated with emerging technologies?

A. Compatibility with legacy systems
B. Application of corporate hardening standards
C. Integration with existing access controls
D. Unknown vulnerabilities

Answer: D

NEW QUESTION 189
Which of the following is the BEST way to ensure the organization's security objectives are embedded in business operations?

A. Publish adopted information security standards.
B. Perform annual information security compliance reviews.
C. Implement an information security governance framework.
D. Define penalties for information security noncompliance.

Answer: C

NEW QUESTION 193
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 198
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 202
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 207
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 209
When deciding to move to a cloud-based model, the FIRST consideration should be:

A. storage in a shared environment.
B. availability of the data.
C. data classification.
D. physical location of the data.

Answer: C

NEW QUESTION 213
Which of the following should be considered FIRST when recovering a compromised system that needs a complete rebuild?

A. Patch management files
B. Network system logs
C. Configuration management files
D. Intrusion detection system (IDS) logs

Answer: C

Explanation:
When recovering a compromised system that needs a complete rebuild, the first step should be to restore configuration management files. Configuration management files are critical for identifying the system's original state and the changes that were made to it, and restoring them can help ensure that the system is rebuilt to its original state.
According to the Certified Information Security Manager (CISM) Study Manual, "The initial phase of the recovery process requires that configuration management files be restored. These files represent the foundation of the system and provide insight into the original state of the system, which is important for identifying changes that were made to the system as well as ensuring the recovery process can return the system to its original state."
Patch management files, network system logs, and intrusion detection system (IDS) logs are also important in the recovery process, but they should be addressed after configuration management files have been restored.

NEW QUESTION 216
Prior to conducting a forensic examination, an information security manager should:

A. boot the original hard disk on a clean system.
B. create an image of the original data on new media.
C. duplicate data from the backup media.
D. shut down and relocate the server.

Answer: B

Explanation:
Prior to conducting a forensic examination, an information security manager should create an image of the original data on new media. This is done in order to preserve the evidence, as making changes to the original data could potentially alter or destroy the evidence. Creating an image of the data also helps to ensure that the data remains intact and free from any interference or tampering.

NEW QUESTION 221
The MOST appropriate time to conduct a disaster recovery test would be after:

A. major business processes have been redesigned.
B. the business continuity plan (BCP) has been updated.
C. the security risk profile has been reviewed
D. noncompliance incidents have been filed.

Answer: A

NEW QUESTION 226
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 231
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 234
What should be an information security manager's MOST important consideration when developing a multi-year plan?

A. Ensuring contingency plans are in place for potential information security risks
B. Ensuring alignment with the plans of other business units
C. Allowing the information security program to expand its capabilities
D. Demonstrating projected budget increases year after year

Answer: B

NEW QUESTION 235
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 237
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 241
Which of the following is an example of risk mitigation?

A. Purchasing insurance
B. Discontinuing the activity associated with the risk
C. Improving security controls
D. Performing a cost-benefit analysis

Answer: C

Explanation:
Risk mitigation refers to the processes and strategies that organizations use to reduce the likelihood or impact of potential risks. Improving security controls is a classic example of risk mitigation. By implementing or enhancing security controls, organizations can reduce the risk of security incidents or breaches, such as data theft or unauthorized access. For example, implementing strong passwords, regularly updating software and systems, and training employees on security best practices are all ways to improve security controls and mitigate risk. Other examples of risk mitigation include implementing disaster recovery and business continuity plans, conducting regular security assessments and audits, and purchasing insurance.

NEW QUESTION 244
Which of the following is the BEST approach to reduce unnecessary duplication of compliance activities?

A. Documentation of control procedures
B. Standardization of compliance requirements
C. Automation of controls
D. Integration of assurance efforts

Answer: B

NEW QUESTION 245
Which of the following BEST enables an organization to provide ongoing assurance that legal and regulatory compliance requirements can be met?

A. Embedding compliance requirements within operational processes
B. Engaging external experts to provide guidance on changes in compliance requirements
C. Performing periodic audits for compliance with legal and regulatory requirements
D. Assigning the operations manager accountability for meeting compliance requirements

Answer: A

Explanation:
Embedding compliance requirements within operational processes ensures that they are consistently followed and monitored as part of normal business activities. This provides ongoing assurance that legal and regulatory compliance requirements can be met. The other choices are not as effective as embedding compliance requirements within operational processes.
Regulatory compliance involves following external legal mandates set forth by state, federal, or international government2. Compliance requirements may vary depending on the industry, location, and nature of the organization2. Compliance helps organizations avoid legal penalties, protect their reputation, and ensure ethical conduct2.

NEW QUESTION 247
An information security manager learns of a new standard related to an emerging technology the organization wants to implement. Which of the following should the information security manager recommend be done FIRST?

A. Determine whether the organization can benefit from adopting the new standard.
B. Obtain legal counsel's opinion on the standard's applicability to regulations,
C. Perform a risk assessment on the new technology.
D. Review industry specialists' analyses of the new standard.

Answer: C

NEW QUESTION 250
An incident management team is alerted to a suspected security event. Before classifying the suspected event as a security incident, it is MOST important for the security manager to:

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

Answer: C

NEW QUESTION 255
Recovery time objectives (RTOs) are BEST determined by:

A. business managers
B. business continuity officers
C. executive management
D. database administrators (DBAs).

Answer: B

Explanation:
Recovery time objectives (RTOs) are best determined by business continuity officers, who are responsible for ensuring that the organization is prepared for any type of disruption. Business managers, executive management, and database administrators (DBAs) all have important roles to play in the preparation and implementation of a disaster recovery plan, but they are not the ones who should determine the RTOs.
References that support this statement include:

- "Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP)" by ISACA (Information Systems Audit and Control Association). This resource states that "BCP and DRP teams are responsible for determining the RTOs for critical processes and systems."
- "Business Continuity Planning" by the Federal Emergency Management Agency (FEMA). This guide states that "RTOs are determined by the organization and are based on the criticality of the business function and the maximum acceptable outage for that function."
- "Business Continuity Planning: The Process" by Continuity Central. This resource states that "The BCP team should determine the RTOs for the organization's critical functions, processes and systems."

Please note that while Business Continuity Officer is responsible for determining RTOs, it is important to consider input from other stakeholders such as executive management, IT, and other department heads to ensure that RTOs align with the overall goals and priorities of the organization.

NEW QUESTION 258
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 262
Following a successful attack, an information security manager should be confident the malware @ continued to spread at the completion of which incident response phase?

A. Containment
B. Recovery
C. Eradication
D. Identification

Answer: A

NEW QUESTION 264
Which of the following is the PRIMARY reason to perform regular reviews of the cybersecurity threat landscape?

A. To compare emerging trends with the existing organizational security posture
B. To communicate worst-case scenarios to senior management
C. To train information security professionals to mitigate new threats
D. To determine opportunities for expanding organizational information security

Answer: A

NEW QUESTION 266
In a business proposal, a potential vendor promotes being certified for international security standards as a measure of its security capability.
Before relying on this certification, it is MOST important that the information security manager confirms that the:

A. current international standard was used to assess security processes.
B. certification will remain current through the life of the contract.
C. certification scope is relevant to the service being offered.
D. certification can be extended to cover the client's business.

Answer: C

NEW QUESTION 268
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 272
Which of the following is the PRIMARY reason for granting a security exception?

A. The risk is justified by the cost to the business.
B. The risk is justified by the benefit to security.
C. The risk is justified by the cost to security.
D. The risk is justified by the benefit to the business.

Answer: D

NEW QUESTION 274
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 279
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 283
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 288
Relationships between critical systems are BEST understood by

A. evaluating key performance indicators (KPIs)
B. performing a business impact analysis (BIA)
C. developing a system classification scheme
D. evaluating the recovery time objectives (RTOs)

Answer: B

Explanation:
The explanation given is: “A BIA is a process that identifies and evaluates the potential effects of natural and man-made events on business operations. It helps to understand how critical systems are interrelated and what their dependencies are. A BIA also helps to determine the RTOs for each system. The other options are not directly related to understanding the relationships between critical systems.”

NEW QUESTION 289
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 291
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 293
A cloud application used by an organization is found to have a serious vulnerability. After assessing the risk, which of the following would be the information

security manager's BEST course of action?

A. Instruct the vendor to conduct penetration testing.
B. Suspend the connection to the application in the firewall
C. Report the situation to the business owner of the application.
D. Initiate the organization's incident response process.

Answer: C

NEW QUESTION 298
Which of the following is the BEST method to protect against emerging advanced persistent threat (APT) actors?

A. Providing ongoing training to the incident response team
B. Implementing proactive systems monitoring
C. Implementing a honeypot environment
D. Updating information security awareness materials

Answer: B

NEW QUESTION 302
Which of the following is the BEST indicator of an organization's information security status?

A. Intrusion detection log analysis
B. Controls audit
C. Threat analysis
D. Penetration test

Answer: B

NEW QUESTION 304
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 308
Which of the following is MOST important to have in place as a basis for developing an effective information security program that supports the organization's business goals?

A. Metrics to drive the information security program
B. Information security policies
C. A defined security organizational structure
D. An information security strategy

Answer: D

NEW QUESTION 311
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 312
What is the PRIMARY benefit to an organization that maintains an information security governance framework?

A. Resources are prioritized to maximize return on investment (ROI)
B. Information security guidelines are communicated across the enterprise_
C. The organization remains compliant with regulatory requirements.
D. Business risks are managed to an acceptable level.

Answer: D

Explanation:
According to the Certified Information Security Manager (CISM) Study Manual, a mature information security culture is one in which staff members regularly consider risk in their decisions. This means that they are aware of the risks associated with their actions and take preventative steps to reduce the likelihood of negative outcomes. Other indicators of a mature information security culture include mandatory information security training for all staff, documented and communicated information security policies, and regular interaction between the CISO and the board.
Maintaining an information security governance framework enables an organization to identify, assess, and manage its information security risks. By establishing policies, procedures, and controls that are aligned with the organization's objectives and risk tolerance, an information security governance framework helps ensure that information security risks are managed to an acceptable level.
According to the Certified Information Security Manager (CISM) Study Manual, "Information security governance provides a framework for managing and controlling information security practices and technologies at an enterprise level. Its primary objective is to manage and reduce risk through a process of identification, assessment, and management of those risks."
While the other options listed (prioritizing resources, communicating guidelines, and remaining compliant with regulations) are also important benefits of maintaining an information security governance framework, they are all secondary to the primary benefit of managing business risks to an acceptable level.

NEW QUESTION 315
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 317
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 319
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 322
Which of the following is the BEST justification for making a revision to a password policy?

A. Industry best practice
B. A risk assessment
C. Audit recommendation
D. Vendor recommendation

Answer: B

Explanation:
A risk assessment should be conducted in order to identify the potential risks associated with a particular system or process, and to determine the best way to mitigate those risks. Making a revision to a password policy based on the results of a risk assessment is the best way to ensure that the policy is effective and secure.
According to the Certified Information Security Manager (CISM) Study manual, the BEST justification for making a revision to a password policy is a risk assessment. A risk assessment enables an organization to identify and evaluate the risks to its information assets and determine the appropriate measures to mitigate those risks, including password policies. Password policies should be based on the risks to the organization's information assets and the level of protection needed.

NEW QUESTION 327

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 331
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 332
Which of the following presents the GREATEST challenge to the recovery of critical systems and data following a ransomware incident?

A. Lack of encryption for backup data in transit
B. Undefined or undocumented backup retention policies
C. Ineffective alert configurations for backup operations
D. Unavailable or corrupt data backups

Answer: D

Explanation:
According to the Certified Information Security Manager (CISM) Study Guide, the greatest challenge to the recovery of critical systems and data following a ransomware incident is the availability and integrity of backups. If the backups are unavailable or corrupt, it becomes much more difficult, if not impossible, to recover the systems and data. This highlights the importance of regularly testing and verifying the backup and recovery process to ensure that the backups are available and can be used in the event of an incident. Additionally, it is important to ensure that backups are stored securely and off-line to prevent them from being encrypted or deleted by an attacker.

NEW QUESTION 336
A common drawback of email software packages that provide native encryption of messages is that the encryption:

A. cannot encrypt attachments
B. cannot interoperate across product domains.
C. has an insufficient key length.
D. has no key-recovery mechanism.

Answer: B

Explanation:
A common drawback of email software packages that provide native encryption of messages is that the encryption cannot interoperate across product domains. This means that emails sent from one product cannot be read by another product, as the encryption keys used are not compatible. This can be a problem when sending emails to people who use different software packages, as the encrypted emails cannot be read.

NEW QUESTION 339
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 (laaS)
C. Platform as a Service (PaaS)
D. Software as a Service (SaaS)

Answer: B

NEW QUESTION 344
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 347
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 350
Which of the following will BEST facilitate the integration of information security governance into enterprise governance?

A. Developing an information security policy based on risk assessments
B. Establishing an information security steering committee
C. Documenting the information security governance framework
D. Implementing an information security awareness program

Answer: B

NEW QUESTION 352
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 356
An incident response team has been assembled from a group of experienced individuals, Which type of exercise would be MOST beneficial for the team at the first drill?

A. Red team exercise
B. Black box penetration test
C. Disaster recovery exercise
D. Tabletop exercise

Answer: D

NEW QUESTION 359
Which of the following is the BEST way to obtain support for a new organization-wide information security program?

A. Benchmark against similar industry organizations
B. Deliver an information security awareness campaign.
C. Publish an information security RACI chart.
D. Establish an information security strategy committee.

Answer: B

Explanation:
Deliver an information security awareness campaign is the BEST approach to obtain support for a new organization-wide information security program. An information security awareness campaign is a great way to raise awareness of the importance of information security and the impact it can have on an organization. It helps to ensure that all stakeholders understand the importance of information security and are aware of the risks associated with it. Additionally, an effective awareness campaign can help to ensure that everyone in the organization is aware of the cybersecurity policies, procedures, and best practices that must be followed.

NEW QUESTION 360
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 361
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 363
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 367
The PRIMARY reason to create and externally store the disk hash value when performing forensic data acquisition from a hard disk is to:

A. validate the confidentiality during analysis.
B. reinstate original data when accidental changes occur.
C. validate the integrity during analysis.
D. provide backup in case of media failure.

Answer: C

Explanation:
The main purpose of creating and storing an external disk hash value when performing forensic data acquisition from a hard disk is to validate the integrity of the data during the analysis. This is done by comparing the original hash value of the disk to the hash value created during the acquisition process, which can be used to ensure that the data has not been tampered with or corrupted in any way. Additionally, by creating a hash value of the disk, it can be used to quickly verify the integrity of any data that is accessed from the disk in the future.

NEW QUESTION 368
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 371
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 372
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your CISM Exam with Our Prep Materials Via below:

https://www.certleader.com/CISM-dumps.html