Vendor: Isaca

Exam Code: CISM

Exam Name: Certified Information Security Manager (CISM)

Version: DEMO

QUESTION 1
An information security risk analysis BEST assists an organization in ensuring that:

A. the infrastructure has the appropriate level of access control.
B. cost-effective decisions are made with regard to which assets need protection
C. an appropriate level of funding is applied to security processes.
D. the organization implements appropriate security technologies

Answer: B
Explanation:
The risk analyst studies different event scenarios and determines the impact of each. This may be expressed in quantitative terms (dollars or other currency) or qualitative terms (high/medium/low or a numeric scale of 1 to 5 or of 1 to 10).

QUESTION 2
In a multinational organization, local security regulations should be implemented over global security policy because:

A. business objectives are defined by local business unit managers.
B. deploying awareness of local regulations is more practical than of global policy.
C. global security policies include unnecessary controls for local businesses.
D. requirements of local regulations take precedence.

Answer: D
Explanation:
In a multinational organization, local security regulations should take precedence because different countries may have specific laws and regulations regarding information security and data protection. Adhering to local regulations is crucial to ensure compliance with the legal requirements of each region in which the organization operates. This helps avoid legal and regulatory issues and ensures that the organization's security practices align with local laws.

QUESTION 3
To gain a clear understanding of the impact that a new regulatory requirement will have on an organization's information security controls, an information security manager should FIRST:

A. conduct a cost-benefit analysis.
B. conduct a risk assessment.
C. interview senior management.
D. perform a gap analysis.

Answer: B
Explanation:
A gap analysis is a method of assessing the performance of a business unit to determine whether business requirements or objectives are being met and, if not, what steps should be taken to meet them.

QUESTION 4
When management changes the enterprise business strategy, which of the following processes should be used to evaluate the existing information security controls as well as to select new information security controls?

A. Access control management
B. Change management
C. Configuration management
D. Risk management

Answer: D
Explanation:
Risk management is the process of identifying, assessing, and prioritizing risks to an organization, including the evaluation of existing controls and the selection of new controls based on changes in the business strategy. When the business strategy changes, it may introduce new risks or alter the significance of existing risks. Risk management allows organizations to adapt their information security controls to align with the evolving risk landscape.

QUESTION 5
Which of the following is the BEST way to build a risk-aware culture?

A. Periodically change risk awareness messages.
B. Ensure that threats are communicated organization-wide in a timely manner.
C. Periodically test compliance with security controls and post results.
D. Establish incentives and a channel for staff to report risks.

Answer: D

QUESTION 6
What would be an information security manager's BEST recommendation upon learning that an existing contract with a third party does not clearly identify requirements for safeguarding the organization's critical data?

A. Cancel the outsourcing contract.
B. Transfer the risk to the provider.
C. Create an addendum to the existing contract.
D. Initiate an external audit of the provider's data center.

Answer: C
Explanation:
The Definition of an addendum is an item of additional material added at the end of a book or document, typically in order to correct, clarify, or supplement something.

QUESTION 7
An organization has purchased a security information and event management (SIEM) tool. Which of the following is MOST important to consider before implementation?

A. Controls to be monitored
B. Reporting capabilities
C. The contract with the SIEM vendor
D. Available technical support

Answer: A

QUESTION 8
Which of the following is MOST likely to be included in an enterprise security policy?

A. Definitions of responsibilities
B. Retention schedules
C. System access specifications
D. Organizational risk

Answer: A

QUESTION 9
Which of the following should an information security manager do FIRST when a legacy application is not compliant with a regulatory requirement, but the business unit does not have the budget for remediation?

A. Develop a business case for funding remediation efforts.
B. Advise senior management to accept the risk of noncompliance.
C. Notify legal and internal audit of the noncompliant legacy application.
D. Assess the consequences of noncompliance against the cost of remediation.

Answer: D

QUESTION 10
Which of the following is the MOST effective way to address an organization's security concerns during contract negotiations with a third party?

A. Review the third-party contract with the organization's legal department.
B. Communicate security policy with the third-party vendor.
C. Ensure security is involved in the procurement process.
D. Conduct an information security audit on the third-party vendor.

Answer: C
Explanation:
Ensuring security is involved in the procurement process is the most effective way to address an organization's security concerns during contract negotiations with a third party. Involving security personnel in the procurement process allows the organization to identify and address potential security risks early on, before a contract is signed. This helps ensure that security requirements are included in the contract and that the third-party vendor is aware of and committed to meeting the organization's security standards. By having security involved in the procurement process, the organization can also ensure that the third-party vendor has adequate security controls in place to protect sensitive information and critical assets. This can include reviewing the vendor's security policies, conducting security assessments, and verifying that the vendor is in compliance with relevant laws and regulations.

QUESTION 11
Which of the following is the BEST method to protect consumer private information for an online public website?

A. Apply strong authentication to online accounts
B. Encrypt consumer data in transit and at rest

C. Use secure encrypted transport layer
D. Apply a masking policy to the consumer data

Answer: B
Explanation:
Encrypting consumer data in transit (as it travels over the internet) and at rest (when stored on servers or databases) is a fundamental and effective security measure. This helps safeguard the confidentiality of the information even if unauthorized access occurs. Encryption ensures that even if data is intercepted or accessed by unauthorized parties, it remains unreadable and secure.

QUESTION 12
Which of the following is the MOST important consideration in a bring your own device (BYOD) program to protect company data in the event of a loss?

A. The ability to remotely locate devices
B. The ability to centrally manage devices
C. The ability to restrict unapproved applications
D. The ability to classify types of devices

Answer: B

QUESTION 13
An information security manager has been asked to determine whether an information security initiative has reduced risk to an acceptable level. Which of the following activities would provide the BEST information for the information security manager to draw a conclusion?

A. Initiating a cost-benefit analysis of the implemented controls
B. Performing a risk assessment
C. Reviewing the risk register
D. Conducting a business impact analysis (BIA)

Answer: B
Explanation:
A cost-benefit analysis in my opinion is done in order to take a decission whether implementing a mitigation control would be profitable to reduce the rist to an acceptable level. In this case the decision has alread been taken and controls have been implemented, so to actually evaluate whether the implemented controls were indeed effective to reduce the rist to an acceptable level is to do a risk assessment to evaluate the current risk.

QUESTION 14
An organization that uses external cloud services extensively is concerned with risk monitoring and timely response. The BEST way to address this concern is to ensure:

A. the availability of continuous technical support.
B. appropriate service level agreements (SLAs) are in place.
C. a right-to-audit clause is included in contracts.
D. internal security standards are in place.

Answer: B

QUESTION 15
Which of the following is the BEST way to ensure that organizational security policies comply with data security regulatory requirements?

A. Obtain annual sign-off from executive management.
B. Align the policies to the most stringent global regulations.
C. Send the policies to stakeholders for review.
D. Outsource compliance activities.

Answer: B

QUESTION 16
The PRIMARY reason for defining the information security roles and responsibilities of staff throughout an organization is to:

A. comply with security policy.
B. increase corporate accountability.
C. enforce individual accountability.
D. reinforce the need for training.

Answer: C
Explanation:
Individual accountability ensures that individuals are held responsible for their actions related to information security, which promotes adherence to policy, procedures and guidelines. Defining roles and responsibilities helps make clear what is expected of each staff member, which in turn makes it possible to hold individuals accountable for fulfilling those expectations. This encourages behavior that supports the organization’s information security objectives.

QUESTION 17
Threat and vulnerability assessments are important PRIMARILY because they are:

A. used to establish security investments.
B. needed to estimate risk.
C. the basis for setting control objectives.
D. elements of the organization's security posture.

Answer: B

QUESTION 18
Which of the following should be an information security managers PRIMARY focus during the development of a critical system storing highly confidential data?

A. Ensuring the amount of residual risk is acceptable
B. Reducing the number of vulnerabilities detected
C. Avoiding identified system threats
D. Complying with regulatory requirements

Answer: D

QUESTION 19
When evaluating vendors for sensitive data processing, which of the following should be the FIRST step to ensure the correct level of information security is provided?

A. Develop metrics for vendor performance.
B. Include information security criteria as part of vendor selection.
C. Review third-party reports of potential vendors.
D. Include information security clauses in the vendor contract.

Answer: B

QUESTION 20
An information security team is investigating an alleged breach of an organization's network. Which of the following would be the BEST single source of evidence to review?

A. File integrity monitoring (FIM) software
B. Security information and event management (SIEM) tool
C. Intrusion detection system (IDS)
D. Antivirus software

Answer: B
Explanation:
The BEST single source of evidence to review when investigating an alleged breach of an organization's network is the Security Information and Event Management (SIEM) tool. The SIEM tool collects and aggregates log data from various sources throughout the network, such as firewalls, intrusion detection systems, and servers. The data is then analyzed and correlated to identify potential security incidents or breaches.

QUESTION 21
Over the last year, an information security manager has performed risk assessments on multiple third-party vendors. Which of the following criteria would be MOST helpful in determining the associated level of risk applied to each vendor?

A. Compliance requirements associated with the regulation
B. Criticality of the service to the organization
C. Corresponding breaches associated with each vendor
D. Compensating controls in place to protect information security

Answer: B

QUESTION 22
Which of the following is the MOST important security consideration when developing an incident response strategy with a cloud provider?

A. Security audit reports
B. Recovery time objective (RTO)
C. Technological capabilities
D. Escalation processes

Answer: D
Explanation:
Incident response strategies need to have clear and well-defined escalation processes. This is especially true when dealing with cloud providers where the client company may have little or no control over the actual infrastructure where their data is stored and processed. If an incident occurs, it is vital that the cloud provider can be quickly and effectively alerted, and that there is a clearly defined process for how the cloud provider will respond to and communicate during such incidents. The escalation process needs to clearly outline who should be contacted, how they should be contacted, what information should be provided, and what the next steps are in the incident response process.

QUESTION 23
Executive leadership has decided to engage a consulting firm to develop and implement a comprehensive security framework for the organization to allow senior management to remain focused on business priorities. Which of the following poses the GREATEST challenge to the successful implementation of the new security governance framework?

A. Executive leadership becomes involved in decisions about information security governance.
B. Executive leadership views information security governance primarily as a concern of the information security management team
C. Information security staff has little or no experience with the practice of information security governance.
D. Information security management does not fully accept the responsibility for information security governance.

Answer: B

QUESTION 24
Risk scenarios simplify the risk assessment process by:

A. covering the full range of possible risk.
B. ensuring business risk is mitigated.
C. reducing the need for subsequent risk evaluation.
D. focusing on important and relevant risk.

Answer: D
Explanation:
Risk scenarios allow professionals to focus on specific/relevant risks rather than looking at everything.

QUESTION 25
Which of the following is the MOST important consideration when developing information security objectives?

A. They are regularly reassessed and reported to stakeholders
B. They are approved by the IT governance function
C. They are clear and can be understood by stakeholders
D. They are identified using global security frameworks and standards

Answer: C

QUESTION 26
A legacy application does not comply with new regulatory requirements to encrypt sensitive data at rest, and remediating this issue would require significant investment. What should the information security manager do FIRST?

A. Assess the business impact to the organization.
B. Present the noncompliance risk to senior management.
C. Investigate alternative options to remediate the noncompliance.
D. Determine the cost to remediate the noncompliance.

Answer: A

QUESTION 27
Which of the following BEST enables effective information security governance?

A. Security-aware corporate culture
B. Advanced security technologies
C. Periodic vulnerability assessments
D. Established information security metrics

Answer: A
Explanation:
Metrics serve only one purpose: to provide the information neceessary for making decisions.

QUESTION 28
Application data integrity risk is MOST directly addressed by a design that includes.

A. strict application of an authorized data dictionary.
B. reconciliation routines such as checksums, hash totals, and record counts.
C. application log requirements such as field-level audit trails and user activity logs.
D. access control technologies such as role-based entitlements.

Answer: B
Explanation:
Reconciliation routines like checksums, hash totals, and record counts are used to detect any changes or modifications to the data. These routines enable organizations to verify the integrity of their data by comparing the stored data to the original data. This helps to ensure that the data has not been tampered with or altered in any way, which is the primary concern when addressing data integrity risks.

QUESTION 29
Deciding the level of protection a particular asset should be given is BEST determined by:

A. the corporate risk appetite.
B. a risk analysis.
C. a threat assessment.
D. a vulnerability assessment.

Answer: A

Explanation:
Risk Analysis facilitates prioritization of risks, but does not tell you the level of protection needed. Risk Appetite on the other hand tells you whether a risk is under-controlled or over-controlled by determining the risk levels after applying the controls if they are within acceptable levels or not.

QUESTION 30
What should be an information security manager's FIRST step when developing a business case for a new intrusion detection system (IDS) solution?

A. Calculate the total cost of ownership (TCO).
B. Define the issues to be addressed.
C. Perform a cost-benefit analysis.
D. Conduct a feasibility study.

Answer: B

QUESTION 31
Which of the following is the MOST important incident management consideration for an organization subscribing to a cloud service?

A. Decision on the classification of cloud-hosted data
B. Expertise of personnel providing incident response
C. Implementation of a SIEM in the organization
D. An agreement on the definition of a security incident

Answer: D
Explanation:
An agreement on the definition of a security incident is the MOST important incident management consideration for an organization subscribing to a cloud service, according to ISACA. Having a clear and agreed upon definition of a security incident is crucial for effective incident management and response.

QUESTION 32
Which of the following is the BEST way for an organization to determine the maturity level of its information security program?

A. Review the results of information security awareness testing.
B. Validate the effectiveness of implemented security controls.
C. Benchmark the information security policy against industry standards.
D. Track the trending of information security incidents.

Answer: B

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

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

10% Discount Coupon Code: ASTR14